THE EVOLVING CYBERSECURITY LANDSCAPE

(117–32)

REMOTE HEARINGS

BEFORE THE

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

THURSDAY, NOVEMBER 4, 2021 and THURSDAY, DECEMBER 2, 2021

Printed for the use of the
Committee on Transportation and Infrastructure

Available online at: https://www.govinfo.gov/committee/house-transportation?path=/browsecommittee/chamber/house/committee/transportation

U.S. GOVERNMENT PUBLISHING OFFICE
47–568 PDF WASHINGTON : 2022

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

PETER A. DeFAZIO, Oregon, *Chair*

ELEANOR HOLMES NORTON,
District of Columbia
EDDIE BERNICE JOHNSON, Texas
RICK LARSEN, Washington
GRACE F. NAPOLITANO, California
STEVE COHEN, Tennessee
ALBIO SIRES, New Jersey
JOHN GARAMENDI, California
HENRY C. "HANK" JOHNSON, Jr., Georgia
ANDRÉ CARSON, Indiana
DINA TITUS, Nevada
SEAN PATRICK MALONEY, New York
JARED HUFFMAN, California
JULIA BROWNLEY, California
FREDERICA S. WILSON, Florida
DONALD M. PAYNE, Jr., New Jersey
ALAN S. LOWENTHAL, California
MARK DeSAULNIER, California
STEPHEN F. LYNCH, Massachusetts
SALUD O. CARBAJAL, California
ANTHONY G. BROWN, Maryland
TOM MALINOWSKI, New Jersey
GREG STANTON, Arizona
COLIN Z. ALLRED, Texas
SHARICE DAVIDS, Kansas, *Vice Chair*
JESÚS G. "CHUY" GARCÍA, Illinois
ANTONIO DELGADO, New York
CHRIS PAPPAS, New Hampshire
CONOR LAMB, Pennsylvania
SETH MOULTON, Massachusetts
JAKE AUCHINCLOSS, Massachusetts
CAROLYN BOURDEAUX, Georgia
KAIALI'I KAHELE, Hawaii
MARILYN STRICKLAND, Washington
NIKEMA WILLIAMS, Georgia
MARIE NEWMAN, Illinois
TROY A. CARTER, Louisiana

SAM GRAVES, Missouri
DON YOUNG, Alaska
ERIC A. "RICK" CRAWFORD, Arkansas
BOB GIBBS, Ohio
DANIEL WEBSTER, Florida
THOMAS MASSIE, Kentucky
SCOTT PERRY, Pennsylvania
RODNEY DAVIS, Illinois
JOHN KATKO, New York
BRIAN BABIN, Texas
GARRET GRAVES, Louisiana
DAVID ROUZER, North Carolina
MIKE BOST, Illinois
RANDY K. WEBER, Sr., Texas
DOUG LaMALFA, California
BRUCE WESTERMAN, Arkansas
BRIAN J. MAST, Florida
MIKE GALLAGHER, Wisconsin
BRIAN K. FITZPATRICK, Pennsylvania
JENNIFFER GONZÁLEZ-COLÓN,
Puerto Rico
TROY BALDERSON, Ohio
PETE STAUBER, Minnesota
TIM BURCHETT, Tennessee
DUSTY JOHNSON, South Dakota
JEFFERSON VAN DREW, New Jersey
MICHAEL GUEST, Mississippi
TROY E. NEHLS, Texas
NANCY MACE, South Carolina
NICOLE MALLIOTAKIS, New York
BETH VAN DUYNE, Texas
CARLOS A. GIMENEZ, Florida
MICHELLE STEEL, California

CONTENTS

STATEMENTS OF MEMBERS OF THE COMMITTEE

WITNESSES

APPENDIX

STATEMENTS OF MEMBERS OF THE COMMITTEE

WITNESSES

SUBMISSIONS FOR THE RECORD

APPENDIX

THE EVOLVING CYBERSECURITY LANDSCAPE: INDUSTRY PERSPECTIVES ON SECURING THE NATION'S INFRASTRUCTURE

THURSDAY, NOVEMBER 4, 2021

HOUSE OF REPRESENTATIVES,
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
WASHINGTON, DC.

The committee met, pursuant to call, at 10:05 in room 2167 Rayburn House Office Building and via Zoom, Hon. Peter A. DeFazio (Chair of the committee) presiding.

Members present in person: Mr. DeFazio, Ms. Norton, Mr. Larsen, Mr. Stanton, Mr. Auchincloss, Mr. Crawford, Mr. Webster, Mr. Perry, Mr. Rodney Davis, Dr. Babin, Mr. Rouzer, Mr. LaMalfa, Mr. Westerman, Mr. Mast, Mr. Stauber, and Mr. Burchett.

Members present remotely: Ms. Johnson of Texas, Mrs. Napolitano, Mr. Johnson of Georgia, Mr. Carson, Mr. Payne, Mr. DeSaulnier, Mr. Lynch, Mr. Carbajal, Mr. Malinowski, Ms. Davids of Kansas, Mr. García of Illinois, Mr. Delgado, Mr. Lamb, Ms. Bourdeaux, Mr. Kahele, Ms. Strickland, Ms. Williams of Georgia, Ms. Newman, Mr. Carter of Louisiana, Mr. Gibbs, Mr. Massie, Mr. Katko, Mr. Weber, Mr. Fitzpatrick, Mr. Balderson, Mr. Johnson of South Dakota, Mr. Guest, Mr. Nehls, Ms. Malliotakis, Ms. Van Duyne, and Mrs. Steel.

Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

Peter A. DeFazio
Chairman

Katherine W. Dedrick, Staff Director

Sam Graves
Ranking Member

Paul J. Sass, Republican Staff Director

NOVEMBER 1, 2021

SUMMARY OF SUBJECT MATTER

TO: Members, Committee on Transportation and Infrastructure
FROM: Staff, Committee on Transportation and Infrastructure
RE: Full Committee Hearing on "The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure"

PURPOSE

The Committee on Transportation and Infrastructure (T&I) will meet on Thursday, November 4, 2021, at 10:00 a.m. EDT in 2167 Rayburn House Office Building and via Zoom, to hold a hearing titled "The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure." The Committee will hear testimony from Scott Belcher on behalf of the Mineta Transportation Institute, Michael Stephens of the Tampa International Airport, Megan Samford of Schneider Electric, John Sullivan of the Boston Water and Sewer Commission on behalf of the Water Information Sharing and Analysis Center (WaterISAC), Gary Kessler of Gary Kessler Associates on behalf of The Atlantic Council, and Tom Farmer of the Association of American Railroads.

BACKGROUND

CYBERTHREATS TO U.S. INFRASTRUCTURE

Cyberattacks are a serious and evolving risk that affect transportation and infrastructure matters across T&I's jurisdiction. This hearing will focus on the needs of T&I stakeholders and the gaps in the nation's ability to prevent, prepare for, respond to, and recover from cyberattacks against infrastructure.

A common term that has sprung up for use within the government sector is "critical infrastructure," which according to Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, includes 16 sectors whose systems and networks, whether physical or virtual, "are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1] T&I's jurisdiction includes five of these sectors, including Transportation Systems, Government Facilities, Water and Wastewater Systems, Dams, and Emergency Services.[2]

The nation's critical infrastructure is comprised of both public and private sector assets.[3] However, within T&I's jurisdiction, cybersecurity requirements in the private sector are mainly voluntary. Like other industries and the federal government, the transportation sector is facing a critical shortage of cybersecurity personnel, which has impacted the ability to protect, detect, and respond to cyberattacks effec-

[1] The White House, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, (February 12, 2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[2] U.S. House of Representatives Committee on Transportation and Infrastructure, *Committee Rules 2021–2022*, (Adopted February 4, 2021), *available at* https://www.govinfo.gov/content/pkg/CPRT-117HPRT43188/pdf/CPRT-117HPRT43188.pdf.

[3] Cybersecurity and Infrastructure Security Agency (CISA), *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, (2013), *available at* https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

tively.[4] Simple steps regarding basic training, consistent cybersecurity hygiene, and periodic exercises could go a long way in protecting America's transportation infrastructure.[5] As the technology that enables America's infrastructure becomes ever more complex and increasingly integrated, cybersecurity threats and vulnerabilities will continue to multiply.

IMPACT OF CYBERATTACKS

Cyberattacks can result in tremendous financial damage, destruction of infrastructure assets, and even death. They impact governments, businesses, and individuals alike and have been growing in number and sophistication. Late last year, it was discovered that a Russian-backed cyber campaign had installed malware in software updates that were received by as many as 18,000 customers of an American firm, SolarWinds, which develops software for businesses and governments.[6] The Department of Homeland Security (DHS) released an updated alert on the SolarWinds hack in April 2021, warning that DHS "determined that this threat poses a grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations."[7]

Also, earlier this year, a ransomware attack on the Colonial Pipeline shut down the company's flow of fuel to the East Coast for nearly one week, causing fuel shortages and increasing fuel prices.[8] In April 2021, Chinese hackers reportedly penetrated New York City's Metropolitan Transit Agency, although no damage was reported.[9] In May 2021, the Washington Suburban Sanitary Commission, which provides water and wastewater service to 1.8 million people in two Maryland counties, was also the victim of a ransomware attack.[10]

COMPLEX JURISDICTIONAL LANDSCAPE

Cybersecurity efforts for the transportation sector are led jointly by the Department of Transportation (DOT), the Transportation Security Administration (TSA), and the U.S. Coast Guard.[11] In the water and wastewater sector, the Environmental Protection Agency (EPA) is designated as the lead agency, and its efforts are supported by the Cybersecurity and Infrastructure Security Agency (CISA).[12]

INCREASING VULNERABILITIES

Critical infrastructure sectors are facing more significant vulnerabilities for various reasons, including the proliferation of information technology and increasing digital access to computer networks.[13] Previously, critical infrastructure equipment

[4] The Washington Post, *The Cybersecurity 202: The government's facing a severe shortage of cyber workers when it needs them the most*, (August 2, 2021), *available at* https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/.

[5] Endpoint, *What is Cyber Hygiene and Why Does it Matter?*, (August 5, 2021), *available at* https://endpoint.tanium.com/what-is-cyber-hygiene-and-why-does-it-matter/.

[6] Bloomberg, *SolarWinds Hack Leaves Critical Infrastructure in the Dark on Risks*, (January 5, 2021), *available at* https://www.bloomberg.com/news/newsletters/2021-01-05/solarwinds-hack-leaves-critical-infrastructure-in-the-dark-on-risks.

[7] CISA, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, (released December 17, 2020, revised April 15, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

[8] Washington Post, *Panic buying strikes Southeastern United States as shuttered pipeline resumes operations*, (May 12, 2021), *available at* https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/.

[9] NBC 4 NYC, *MTA Hacked in April Cyberattack; Employee, Customer Info Was Not Compromised*, (June 2, 2021), *available at* https://www.nbcnewyork.com/news/local/mta-hacked-in-april-cyberattack-employee-customer-info-was-not-compromised/3086785/.

[10] WSSC Water, *WSSC Water Investigating Ransomware Cyberattack*, (June 25, 2021), *available at* https://www.wsscwater.com/news/2021/june/wssc-water-investigating-ransomware-cyberattack.

[11] CISA, *Transportation Systems Sector*, (accessed on October 22, 2021), *available at* https://www.cisa.gov/transportation-systems-sector and CISA, *Water and Wastewater Systems Sector*, (accessed on October 22, 2021), *available at* https://www.cisa.gov/water-and-wastewater-systems-sector.

[12] The White House, *PPD–21 Critical Infrastructure Security and Resilience* (Feb 12, 2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/.

[13] Government Accountability Office (GAO), *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, (May 28, 2004), *available at* https://www.gao.gov/products/gao-04-321.

was only accessible at its physical site.[14] To make any change to the system would require physically accessing the equipment.[15] Today, progress in technology, especially the Internet, has changed the risk landscape entirely with new and evolving ways to access systems which have made infrastructure assets more financially efficient and operationally effective while at the same time making them more vulnerable to cyber threats.[16] Demand for remote work, especially due to the COVID–19 pandemic, has dramatically increased vulnerabilities, with more employees needing remote access to systems.[17] However, making remote access to systems easier introduces significant vulnerabilities that bad actors can take advantage of to access those systems remotely.[18] Robust cybersecurity protocols can make remote access more secure. However, they can be time and work-intensive and not always possible depending on a facility's staffing and cybersecurity experience.[19] A vulnerability due to the use of a remote access program was how hackers were able to access a water treatment plant in Oldsmar, Florida earlier this year, for instance.[20]

The vulnerability of transportation infrastructure to cyberattacks will increase in the future as bad actors make greater use of emerging technologies, which create new vulnerabilities to exploit.[21] Cyberattacks that exploit an unknown vulnerability, known as a "zero-day" attack, provide no option or "zero days," to fix the issue before it is successfully used as part of a hack since the attack takes advantage of a new and previously unknown security flaw.[22] New technologies provide greater opportunities for zero-day attacks since they take advantage of technology that is new to cybersecurity professionals.[23] In addition, many emerging technologies in the transportation and infrastructure space will have various interconnected digital channels, providing multiple pathways for potential attackers.[24] Autonomous vehicles and unmanned aircraft systems are two key examples of emerging technologies that create multiple cybersecurity challenges for the future.[25]

High-Profile Cyberattacks Illustrate Range of Threats

Threats to infrastructure systems are increasing, as seen through several recent high-profile attacks against transportation infrastructure. Three such attacks include the recent ransomware attack on the Colonial Pipeline in May 2021,[26] the 2017 NotPetya malware attack that affected the Maersk shipping company,[27] and the February 2021 intrusion into the water treatment plant in Oldsmar, Florida.[28]

[14] George Brown College, *The Evolution of PLCs*, (July 21, 2021), *available at* https://www.plctechnician.com/news-blog/evolution-plcs.

[15] *Id.*

[16] Coolfire Core, *What Is the Difference Between IT and OT?*, (April 12, 2019), *available at* https://www.coolfiresolutions.com/blog/difference-between-it-ot/.

[17] McKinsey, *Building cyber resilience in national critical infrastructure*; U.S. News and World Report, *Remote Working Fueled by COVID Pandemic Gaining Popularity*, (September 25, 2021), *available at* https://www.usnews.com/news/best-states/minnesota/articles/2021-09-25/remote-working-fueled-by-covid-pandemic-gaining-popularity.

[18] Securicon, *The Difference Between IT and OT, and How They Are Converging*.

[19] Verve, *Securing OT Systems: Is Remote Access Here to Stay?*, (April 18, 2020), *available at* https://verveindustrial.com/resources/blog/securing-ot-systems-is-remote-access-here-to-stay/.

[20] Mass.gov, *Cybersecurity Advisory for Public Water Suppliers*, (accessed on October 13, 2021), *available at* https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers.

[21] AT&T, *Emerging Technologies and the Cyber Threat Landscape*, (December 13, 2017), *available at* https://cybersecurity.att.com/blogs/security-essentials/emerging-technologies-and-the-cyber-threat-landscape

[22] FireEye, *What is a Zero-Day Exploit?* (accessed on October 20, 2021), *available at* https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.

[23] *Id.*

[24] Boston Consulting Group, *Navigating Rising Cyber Risks in Transportation and Logistics*, (August 30, 2021), *available at* https://www.bcg.com/publications/2021/navigating-rising-cyber-risks-in-transportation-and-logistics

[25] ScienceDaily, *Need to safeguard drones and robotic cars against cyber attacks*, (November 27, 2019), *available at* https://www.sciencedaily.com/releases/2019/11/191127121302.htm

[26] Matt Egan and Clare Duffy, CNN, *Colonial Pipeline launches restart after six-day shutdown*, (May 12, 2021), *available at* https://www.cnn.com/2021/05/12/business/colonial-pipeline-restart/index.html.

[27] Jordan Novet, CNBC, *Shipping company Maersk says June cyberattack could cost it up to $300 million* (August 16, 2017) *available at* https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html.

[28] Colonial Pipeline, *Media Statement Update: Colonial Pipeline System Disruption*, (May 17, 2021), *available at* https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption; Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, (Aug 22, 2018), *available at* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Pinellas County Sheriff Department YouTube channel,

Each of these attacks were distinct and highlighted the risks facing vital infrastructure entities, as well as opportunities for improving both government and private sector coordination and oversight of these vulnerabilities.

Ransomware—Colonial Pipeline

On May 7, 2021, Colonial Pipeline, one of the nation's largest oil and gas pipelines, was the victim of a ransomware attack by DarkSide, a cyber-criminal group believed to operate out of Russia.[29] The attack was discovered when an employee found a digital ransom note on a system in the Colonial information technology (IT) network.[30] DarkSide encrypted all of Colonial's IT systems and demanded a financial payment in exchange for a key to unlock the impacted systems.[31] Though the attack did not directly affect Colonial's operational technology (OT)[32] network, which is used to control the pipeline equipment, company officials immediately halted operations throughout the pipeline. They did so to isolate and contain the damage and ensure the malware did not spread to the OT network.[33] The following day, Colonial made a $4.4 million ransom payment to DarkSide and received the information it needed to regain control of its IT systems.[34] Colonial began work immediately to restore pipeline operations with the assistance of the Pipeline and Hazardous Materials Safety Administration (PHMSA) at DOT, which provided guidance on temporary manual operations of the pipeline and its subsequent return to service.[35] On May 13, 2021, six days after the attack, it had fully restored service, though several more days passed before the fuel supply chain returned to normal.[36]

An investigation conducted by cybersecurity consulting firm FireEye-Mandiant (Mandiant) determined that the attackers used an employee's legacy username and password to log in to a virtual private network (VPN) device.[37] Several missteps helped enable DarkSide to access Colonial's network in this manner.[38] First, the employee's login information was no longer in use, but had not been deleted from the company's system.[39] Second, the legacy VPN profile did not require multi-factor authentication, such as the use of a one-time passcode, which CISA and the Federal Bureau of Investigation (FBI) recommend as a best practice.[40] Third, the employee

Treatment Plant Intrusion Press Conference, (February 8, 2021), *available at* https://www.youtube.com/watch?v=MkXDSOgLQ6M&t=1s.

[29] Hearing before the House Committee on Homeland Security, *Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure*, (June 9, 2021), *available at* https://www.govinfo.gov/content/pkg/CHRG-117hhrg45085/pdf/CHRG-117hhrg45085.pdf; Federal Bureau of Investigation, *FBI Deputy Director Paul M. Abbate's Remarks at Press Conference Regarding the Ransomware Attack on Colonial Pipeline*, (June 7, 2021), *available at* https://www.fbi.gov/news/pressrel/press-releases/fbi-deputy-director-paul-m-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline.

[30] House Committee on Homeland Security, *Cyber Threats in the Pipeline*.

[31] *Id.*

[32] Operational technology (OT) is equipment that handles machines and their physical operation. OT includes hardware and software that interacts with the physical environment, including monitoring and controlling industrial equipment, assets, processes, and events. Historically, IT and OT networks were entirely isolated from one another since they developed separately, with OT predating IT. OT used relatively simple systems that completed specific functions that were only accessible on-site and in-person. This provided physical isolation for OT networks, and when IT and the Internet were developed, that isolation prevented OT from being accessed remotely. This segmentation was good for security. However, there were business demands for remote visibility into industrial operations, leading businesses to move towards a more integrated system. An integrated system has productivity benefits, including reducing administrative burdens, streamlining work, and improving data to inform better decision-making. Unfortunately, it also creates and greatly expands a network's cyber vulnerabilities. A connection to an IT network can serve as a path to access OT networks. The safest version of an OT network is one that is completely separated and has no external connectivity with IT networks or the Internet, known as an air gap. An air gap is a security measure where a system is not connected to any other network or device and can only be accessed physically.

[33] House Committee on Homeland Security, *Cyber Threats in the Pipeline*.

[34] *Id.*

[35] U.S. DOT, PHMSA, *Remarks of Acting Administrator Tristan Brown at API's Midstream Committee Meeting*, (May 26, 2021), *available at* https://www.phmsa.dot.gov/news/remarks-tristan-brown-before-api-midstream-committee.

[36] Colonial Pipeline, *Media Statement Update: Colonial Pipeline System Disruption*, (May 17, 2021), *available at* https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

[37] House Committee on Homeland Security, *Cyber Threats in the Pipeline*.

[38] *Id.*

[39] *Id.*

[40] *Id.*; CISA, *Alert (AA21–131A): DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, (May 11, 2021), *available at* https://us-cert.cisa.gov/ncas/

Continued

had used the same password on a different website, from which the password had been stolen.[41] CISA recommends using unique passwords for each device or account.[42] The president and CEO of Colonial has said that his company has disabled the legacy VPN account, has instituted multi-factor authentication for network access, and is taking other steps to strengthen its cyber defenses.[43]

Colonial's pipelines transport nearly half of the East Coast's fuel, providing energy for more than 50 million Americans. The impact of the ransomware attack was felt throughout the eastern United States.[44] The shutdown resulted in massive fuel shortages and gasoline panic-buying.[45] At least 12,000 gas stations in 11 states reported being completely empty, and the price of gas surpassed $3 a gallon.[46] The day before Colonial fully resumed operations, 65 percent of gas stations in North Carolina reported being out of gas; in Georgia, South Carolina, and Virginia, more than 43 percent of gas stations reported being out of gas.[47] The governors of Florida, North Carolina, and Virginia all declared states of emergency to help alleviate the fuel shortages.[48]

The Colonial attack illustrated how intrusions into pipeline computer networks have the potential to negatively affect the nation's security, economy, and wellbeing.[49] The perpetrators of the attack also accessed personally identifiable information, such as names, birth dates, and Social Security numbers for more than 5,800 current and former Colonial employees, exposing these individuals to the risk of fraud and identity theft.[50]

In response to the attack, TSA—which oversees pipeline security[51]—issued security directives that require, among other things, pipeline owners and operators to take measures to protect against cyberattacks to their IT and OT systems and to develop and implement a cybersecurity contingency and recovery plan.[52] Although the Colonial attack was carried out on the company's IT network, it highlights the highly interconnected nature of OT operations that businesses must consider.[53] Experts say that actions like applying security patches and updates promptly and using multi-factor authentication can help protect against ransomware and other cyberattacks.[54]

alerts/aa21-131a and FBI, *OPS Cyber Awareness Guide*, (accessed on October 22, 2021), *available at* https://www.fbi.gov/file-repository/cyber-awareness-508.pdf/view.

[41] House Committee on Homeland Security, *Cyber Threats in the Pipeline*.

[42] CISA, *Security Tip (ST04–003): Good Security Habits*, (February 21, 2021), *available at* https://www.cisa.gov/tips/st04-003.

[43] Hearing before the Senate Committee on Homeland Security and Governmental Affairs, *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack, Testimony of Joseph Blount, President and Chief Executive Officer of the Colonial Pipeline Company*, (June 8, 2021), *available at* http://www.hsgac.senate.gov/download/testimony-blount-2021-06-08.

[44] See: Senate Committee on Homeland Security and Governmental Affairs, *Testimony of Joseph Blount* and House Committee on Homeland Security, *Cyber Threats in the Pipeline*.

[45] Washington Post, *New emergency cyber regulations lay out 'urgently needed' rules for pipelines but draw mixed reviews*, (October 3, 2021), *available at* https://www.washingtonpost.com/national-security/cybersecurity-energy-pipelines-ransomware/2021/10/03/6df9cab2-2157-11ec-8200-5e3fd4c49f5e__story.html.

[46] Washington Post, *Panic buying strikes Southeastern United States*.

[47] *Id.*

[48] New York Times, *Gas Pipeline Hack Leads to Panic Buying in the Southeast*, (May 11, 2021), *available at* https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html.

[49] TSA, *Written Testimony of David P. Pekoske, Administrator, Transportation Security Administration, U.S. Department of Homeland Security*, Hearing on Pipeline Security, Before the Committee on Commerce, Science, and Transportation, (July 27, 2021), *available at* https://www.commerce.senate.gov/services/files/3DFD1053-A11E-4B1A-9818-FE29C19AA06B.

[50] ZD Net, *Colonial Pipeline sends breach letters*.

[51] TSA also coordinates with PHMSA on pipeline security under a Memorandum of Understanding, *See: PHMSA, Annex to the Memorandum of Understanding Between the Department of Homeland Security and the Department of Transportation Concerning Transportation Security Administration and Pipeline and Hazardous Materials Safety Administration Cooperation on Pipeline Transportation Security and Safety*, Feb. 26, 2020, *available at*: https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/docs/regulatory-compliance/phmsa-guidance/73466/phmsa-tsa-mou-annexexecuted.pdf.

[52] *Id.*

[53] Dragos, *Recommendations Following the Colonial Pipeline Cyber Attack*, (May 11, 2021), *available at* https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/.

[54] ZD Net, *Ransomware is the biggest cyber threat to business. But most firms still aren't ready for it*, (October 11, 2021), *available at* https://www.zdnet.com/article/ransomware-is-now-the-most-urgent-cyber-threat-to-business-but-most-firms-arent-ready-for-it/.

Malware—NotPetya & Maersk Shipping

In 2017 Russian linked individuals reportedly unleashed a malware attack in Ukraine named NotPetya.[55] The malware affected virtually every federal agency in the country, crippling four hospitals in the capital, six power companies, two airports, more than 22 Ukrainian banks, as well as freezing ATMs and card payment systems in retail and transit sectors.[56] Ukraine later estimated that NotPetya wiped 10 percent of all computers in the country, and one government official said immediately after the attack, "the government was dead." [57]

Within hours, NotPetya had propagated far beyond Ukraine, affecting computer networks in companies in 65 countries around the world.[58] Among the companies affected were the multinational shipping company Maersk ($300 million in damage), the pharmaceutical giant Merck ($800 million), the French construction company Saint-Gobain ($384 million), FedEx's European subsidiary ($400 million), as well as smaller victims such as a hospital in Pennsylvania and a chocolate company in Australia.[59] The White House would later identify NotPetya as the most destructive and costly cyberattack in history, with overall damage above $10 billion.[60] The malware even infected the Russian state oil company, Rosneft, demonstrating the runaway nature of NotPetya's harms.[61] The U.S. issued sanctions against organizations involved in NotPetya's release and, in 2020, the Department of Justice indicted six Russian military officers for the cyberattack.[62]

Maersk is the world's largest container shipping company, responsible for shipping an estimated 25 percent of the world's food supply.[63] It is a $56 billion company present in 130 nations with over 700 ships and 17 percent of the world's cargo shipping container capacity.[64] The malware entered Maersk's IT network through a computer in the Ukrainian port of Odessa.[65] There, a finance executive had earlier asked IT administrators to upload the Ukrainian accounting program on a single computer.[66] From that computer, NotPetya propagated through the Maersk global IT system in seven minutes.[67] Within an hour, all Maersk's end-user devices, including 49,000 laptops and printers and 3,500 of 6,200 servers, were effectively destroyed.[68] Maersk's fixed phoneline ceased functioning and, due to system integration, all Outlook and cell phone contacts were wiped, crippling initial response efforts.[69] Though ships' computers were not affected, the software at Maersk termi-

[55] Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, (Aug 22, 2018), *available at* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[56] *Id.*

[57] *Id.*

[58] Jai Vijayan, *3 Years After NotPetya, Many Organizations Still in Danger of Similar Attacks*, Dark Reading, (June 30, 2020), *available at* https://www.darkreading.com/threat-intelligence/3-years-after-notpetya-many-organizations-still-in-danger-of-similar-attacks.

[59] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, (October 14, 2018), *available at* https://tech.industry-best-practice.com/2018/10/14/the-untold-story-of-notpetya-the-most-devastating-cyberattack-in-history/.

[60] *Id.*; The White House, *Statement from the Press Secretary*, (Feb 15, 2018), *available at* https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

[61] Wired, *Petya Ransomware Hides State-Sponsored Attacks, Say Ukrainian Analysts*, (June 28, 2017), *available at* https://www.wired.com/story/petya-ransomware-ukraine/.

[62] U.S. Dept of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, (Oct 19, 2020), *available at* https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[63] Statista, *The world's leading container ship operators as of September 30, 2021, based on number of owned and chartered ships*, (accessed on October 22, 2021), *available at* https://www.statista.com/statistics/197643/total-number-of-ships-of-worldwide-leading-container-ship-operators-in-2011/.

[64] Statista, *Number of APM-Maersk ships from February 2021 to September 2021*, (September 30, 2021), *available at* https://www.statista.com/statistics/199366/number-of-ships-of-apm-maersk-in-december-2011/; Statista, *Moeller-Maersk's assets from FY 2018 to FY 2020*, (February 24, 2021), *available at* https://www.statista.com/statistics/325993/total-assets-of-moeller-maersk/ ; Maersk, *A.P. Moller—Maersk enters strategic partnership with Danish Crown on global end-to-end logistics*, (October 15, 2021), *available at* https://www.maersk.com/news/articles/2021/10/15/maersk-enters-strategic-partnership-with-danish-crown.

[65] Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*.

[66] *Id.*

[67] Andy Powell, *Implementing the Lessons Learned from a Major Cyberattack*, (November 2019), *available at* https://www.youtube.com/watch?v=wQ8HIjkEe9o.

[68] Rae Richie, *Maersk: Springing back from a catastrophic cyberattack*, (Aug 2019), *available at* https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack.

[69] *Id.*

nals which received files from their ships, informing terminal operators of ships' content and how to direct cargo handling, had been wiped.[70] Paralysis resulted at seventeen Maersk terminals worldwide for days, with no one able to receive cargo for ground transport and perishable and time-sensitive materials stuck in place.[71]

Rebuilding Maersk's network began four days after the attack when the company recovered its domain controller, a detailed map of their network that controlled system users, from a Maersk office in Ghana where a coincidental power outage had protected the office's IT system.[72] A Maersk official flew with a copy of the critical software to England, where over five days, hundreds of IT workers used the recovered domain controller to reconstruct Maersk's active directory for worldwide operations, build out 2,000 new laptops, and reenable core business processes and systems.[73] It took several more days before Maersk could restart online shipment processes and more than a week before terminals around the world could function normally.[74] Over two months passed before Maersk IT personnel fully restored its software setup.[75]

Following the NotPetya attack, Maersk leadership shared their critical takeaways with the global community, which assisted many other NotPetya victims in recovery.[76] These included transparency, open communication, crisis recovery and business continuity plans, regular cyber incident response exercises, and a network of consultancies and government actors, among others.[77]

Intrusions—Oldsmar Wastewater Treatment Plant

On Friday, February 5, 2021, a hacker remotely accessed the computer system of the water treatment plant for the city of Oldsmar, Florida, which provides water to about 15,000 people.[78] The hacker changed chemical levels in the water, increasing the sodium hydroxide (otherwise known as lye) level from 100 parts per million to 11,100 parts per million.[79] In small quantities, sodium hydroxide is used to control acidity in water, but at higher levels, it is dangerous to humans. If the affected water had made it to the city's residents, they could have become seriously ill.[80] Ingesting as little as 10 grams of sodium hydroxide can be fatal.[81]

The hack at Oldsmar was discovered immediately when an employee noticed programs being opened on his computer and that the level of sodium hydroxide in the water had changed.[82] The employee first noticed his computer being accessed remotely earlier that day but had not reported it because it was common for supervisors or others to access the system to troubleshoot issues remotely.[83] Upon noticing later that the system was being remotely accessed again and that chemical levels were being changed to dangerous levels, the employee changed the chemical lev-

[70] Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*.

[76] Andy Powell, *Implementing the Lessons Learned from a Major Cyberattack; see also* Jim Snabe, *CyberSecurity Davos 2017—Maersk*, (June 2017), *available at* https://www.youtube.com/watch?v=VaqIYlYmDbA.

[77] *Id.*

[78] Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference*, (February 8, 2021), *available at* https://www.youtube.com/watch?v=MkXDSOgLQ6M&t=1s and Tampa Bay Times, *Someone tried to poison Oldsmar's water supply during hack, sheriff says*, (February 8, 2021), *available at* https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/.

[79] Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference*.

[80] The New York Times, *Dangerous Stuff: Hackers Tried to Poison Water Supply of Florida Town*, (February 8, 2021), *available at* https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html.

[81] Environmental Protection Agency (EPA), *Sodium Hydroxide*, (September 1992), *available at* https://www3.epa.gov/pesticides/chem__search/reg__actions/reregistration/fs__PC-075603__1-Sep-92.pdf.

[82] Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference*.

[83] Reuters, *Hackers try to contaminate Florida town's water supply through computer breach*, (February 8, 2021), *available at* https://www.reuters.com/article/us-usa-cyber-florida-idUSKBN2A82FV.

els back to a safe level and reported the intrusion.[84] The plant disabled remote access to their system after the hack and reported the hack to federal authorities.[85]

CISA and the FBI determined that the hackers gained access to the supervisory control and data acquisition (SCADA) system, likely exploiting cybersecurity weaknesses such as poor password security and an outdated operating system.[86] They also determined that hackers were likely able to access the SCADA system through the remote access TeamViewer software, which used the same password across all computers and lacked any firewall protection.[87] City officials have said that residents were never at risk because of the city's automated monitoring of the water's pH levels and its built-in alarms, which would have been triggered before the water made it to the public.[88]

The Oldsmar hack provides an example of the vulnerability of water systems to cybersecurity threats, especially smaller systems that lack the security controls, IT staff, and funding of larger organizations. It also shows how remote management applications, though efficient, create opportunities for attacks.[89] The water sector is well-protected from a large-scale attack on the entire system due to its decentralized nature, but the existence of thousands of small utilities across the country makes it challenging to ensure compliance with best practices throughout the entire sector.[90] The investigations from CISA, the FBI, and others, for example, show that the Oldsmar water treatment plant had poor password management, an outdated operating system, and an old remote access management system still on computers.[91] Further, an analysis done by Nozomi Networks' Labs determined that the Oldsmar hack was not very sophisticated and that it was likely perpetrated by someone without specific background knowledge of the water treatment process.[92]

Poor Cybersecurity Hygiene Creates Weak Links

As reliance on IT continues to dominate American lives and global competitiveness, the Colonial, Maersk, and Oldsmar attacks illustrate the cybersecurity vulnerabilities found in common items and the willingness of enemies, whether nation-state or not, to target these gaps. Cybersecurity in both the public and private sector can be significantly enhanced by making easy fixes, such as ensuring known software patches are implemented quickly, providing regular cybersecurity awareness training to staff, and using effective passwords and other authentication systems.[93] However, the federal government, organizations, and individuals often fail to take these "cyber hygiene" measures due to resource constraints or lack of awareness or will, creating easy targets for cybercriminals. These weak links may result in consequences that threaten the nation's transportation infrastructure and networks and potentially harm the public.

Recent surveys of the public transit and water and wastewater utilities sectors confirm that some U.S. transportation infrastructure assets are not making some

[84] Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference*.

[85] Vice, *Hacker Tried to Poison Florida City's Water Supply, Police Say*, (February 8, 2021), *available at* https://www.vice.com/en/article/88ab33/hacker-poison-florida-water-pinellas-county.

[86] CISA, *Alert (AA21–042A) Compromise of U.S. Water Treatment Facility*, (February 12, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa21-042a.

[87] ABC Action News WFTS Tampa Bay, *FBI: Water system hack likely caused by remote access program, old software and poor password security*, (February 10, 2021), *available at* https://www.abcactionnews.com/news/local-news/i-team-investigates/fbi-water-system-hack-likely-caused-by-remote-access-program-old-software-and-poor-password-security; Mass.gov, *Cybersecurity Advisory for Public Water Suppliers*, (accessed on October 4, 2021), *available at* https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers and FBI, CISA, EPA, MS–ISAC, *Joint Cybersecurity Advisory*, (February 11, 2021), *available at* https://www.mass.gov/doc/joint-fbi-cisa-cybersecurity-advisory-on-compromise-of-water-treatment-facility/download.

[88] Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference*.

[89] FBI, CISA, EPA, MS–ISAC, *Joint Cybersecurity Advisory*.

[90] CISA, *Water and Wastewater Systems Sector*, (accessed on October 27, 2021), *available at* https://www.cisa.gov/water-and-wastewater-systems-sector.

[91] FBI, CISA, EPA, MS–ISAC, *Joint Cybersecurity Advisory*.

[92] Nozomi Networks, *Hard Lessons From the Oldsmar Water Facility Cyberattack Hack*, (February 10. 2021), *available at* https://www.nozominetworks.com/blog/hard-lessons-from-the-oldsmar-water-facility-cyberattack-hack/.

[93] Cybersecurity & Infrastructure Security Agency (CISA), *Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness*, (Spring 2021), *available at* https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit__03.12.2021__508__0.pdf

of the recommended adjustments.[94] These surveys show gaps in the water and transit sectors' ability to detect, confront, and respond to cybersecurity incidents.[95] Research into other relevant T&I industries, such as aviation and maritime, indicates similar security vulnerabilities.[96]

- *Water Sector Survey*. In June 2021, water security stakeholders issued a report that included a survey of more than 600 water and wastewater utilities regarding cybersecurity gaps and needs.[97] More than 57 percent of water utilities that responded to the survey have a risk management plan that addresses cybersecurity threats, while 42 percent do not.[98] Further, 26 percent conduct cybersecurity risk assessments *less than* once per year.[99] More than 37 percent of small water utilities said they don't share cybersecurity data because they don't know who to share this information with or how to do so, while 22 percent feared the data would not be kept confidential.[100] While 75 percent of respondents have implemented or are in the process of implementing some "cyber protection efforts," more than 25 percent of water utilities have no plans to conduct these efforts. Nearly 64 percent do not employ a chief information security officer (CISO), and while over 50 percent of water utilities conduct some cybersecurity-related drill or exercises, 42 percent *do not*.[101] More than 68 percent do not participate in any cybersecurity-related drills or exercises, but 47 percent said they need cybersecurity technical assistance, advice, and other support, and 41 percent said they need federal grants or loans to improve cybersecurity.[102]
- *Transit Sector Survey*. The Mineta Transportation Institute and San Jose State University produced a recent report on transit-related cybersecurity issues that included a survey of 90 transit agencies serving more than 124 million people.[103] Among the results, over 50 percent of those surveyed had up to four staff dedicated to cybersecurity while nearly 39 percent had no dedicated staff, three of which are considered "extra-large" agencies with more than $100 million in operating expenses.[104] In addition, four of 20 agencies that reported having a cybersecurity incident still have no staff dedicated to cybersecurity.[105] Over 60 percent of transit agencies surveyed provide cybersecurity training to staff, while more than 24 percent provide no training, and more than 58 percent of those that don't provide training said it was due to a lack of resources.[106] In addition, 42 percent of the agencies don't have an incident response plan, and of those that had one, over half have not had an exercise in over a year.[107] Nearly 78 percent of the 90 agencies surveyed said they had not had a cybersecurity "incident."[108] The authors found this troubling since given the frequency of cyberattacks, it suggests that many of these transit agencies may simply not be detecting successful cybersecurity penetrations against their networks.[109] In

[94] Water Sector Coordinating Council, *Water and Wastewater Systems—Cybersecurity: 2021 State of the Sector*, (June 2021), *available at* https://www.waterisac.org/system/files/articles/FINAL__2021__WaterSectorCoordinatingCouncil__Cybersecurity__State__of__the__Industry-17-JUN-2021.pdf and Scott Belcher, et. al., *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, San Jose State University and Mineta Transportation Institute, (September 2020), *available at* https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf.

[95] *Id.*

[96] *See, e.g.*, For Aviation Cybersecurity, Airways Magazine, *The Current State of Cybersecurity in Civil Aviation* (June 5, 2021), *available at* https://airwaysmag.com/industry/the-current-state-of-cybersecurity-in-civil-aviation and for Maritime Cybersecurity, Atlantic Council, *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity* (Oct. 2021), pp 5–13, *available at* https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Cyber-Maritime-Final-Report.pdf.

[97] Water Sector Coordinating Council, *Water and Wastewater Systems—Cybersecurity: 2021 State of the Sector*.

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] Scott Belcher, et. al., *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, San Jose State University and Mineta Transportation Institute, (September 2020), *available at* https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf.

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.* at 36–37.

addition, more than 30 percent of those that said they had been the victim of a cybersecurity incident also said they never reported the incident to anyone.[110]

PRIVATE-PUBLIC COORDINATION

In the United States, it is generally cited that 85 percent of critical infrastructure is in private hands, and much of the transportation sector is subject to some government oversight.[111] As such, cooperation between the public and private sectors that fosters integrated, collaborative engagement and interaction is essential to maintaining transportation infrastructure cybersecurity, especially as technology makes transportation infrastructure increasingly vulnerable to cyberattacks.[112] The annual cost of malicious cyber activity to the U.S. economy, estimated recently at between $57 billion and $109 billion, demonstrates the pressing need for action in both the private and public sectors.[113]

As the federal government seeks to strengthen transportation infrastructure's cyber defenses, with an emphasis on cybersecurity preparedness, the perspective and experience of the private sector remains vital to create effective cyber resilience.[114] Addressing the biggest gaps, including those discussed below, will require collaboration between public and private stakeholders.

CYBERSECURITY WORKFORCE SHORTAGES

There is a dire shortage globally of workers with cybersecurity expertise. In the U.S., recent estimates show around 950,000 individuals currently employed in this field, with a need to fill an additional 464,000 cyber-related positions.[115] In the public sector alone, there are about 60,000 individuals employed in cyber jobs, with an additional 36,000 unfilled positions across all levels of government.[116]

In addition, a Center for Strategic and International Studies survey of public and private sector organizations in eight countries, including the United States, found that eighty-two percent of responding organizations have a shortage of employees with cybersecurity skills.[117] The survey results also show that the shortage of cybersecurity professionals can have real consequences. One-third of respondents said a shortage of skills makes their organizations more desirable hacking targets, and a quarter said insufficient cybersecurity staff strength has damaged their organization's reputation and led directly to the loss of proprietary data through a cyberattack.[118]

Although a shortage of federal cybersecurity workers remains, the federal government has taken several steps to address this shortage.[119]

- The Office of Management and Budget directed the Office of Personnel Management and other federal agencies to establish programs to assist federal agencies in using existing compensation flexibilities and explore opportunities for new or revised pay programs for cybersecurity positions to better enable them to compete with other employers.[120]
- CISA created the National Initiative for Cybersecurity Education framework for increasing the size and capability of the U.S. cyber workforce, and Girls Who

[110] *Id.*

[111] Lawfare, *Is It Really 85 Percent?* (May 11, 2021), *available at* https://www.lawfareblog.com/it-really-85-percent.

[112] CISA, *Critical Infrastructure Sector Partnerships*, (accessed on Oct 22, 2021) *available at* https://www.cisa.gov/critical-infrastructure-sector-partnerships.

[113] Council of Economic Advisors, *The Cost of Malicious Cyber Activity to the U.S. Economy* (2018), *available at* https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/

[114] Lawfare, *Is It Really 85 Percent?*

[115] CyberSeek, "Cybersecurity Supply/Demand Heat Map," *last accessed on October 22, 2021, at* https://www.cyberseek.org/heatmap.html; Washington Post, *The Cybersecurity 202: The government's facing a severe shortage of cyber workers when it needs them the most*, (August 2, 2021), *available at* https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/.

[116] *Id.*

[117] Center for Strategic and International Studies, *Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills*, (July 2016), *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf.

[118] *Id.*

[119] Washington Post, *The Cybersecurity 202*.

[120] Office of Management and Budget, "Memorandum for Heads of Executive Departments and Agencies: Federal Cybersecurity Workforce Strategy," (July 12, 2016), *available at* https://www.chcoc.gov/content/federal-cybersecurity-workforce-strategy.

Code, an effort to develop pathways for young women to pursue careers in cybersecurity and technology.[121]
- The United States Digital Service allows technology specialists to apply and essentially take a "tour of civic service" to bring real-world private sector knowledge into the federal government.[122]

VOLUNTARY STANDARDS AND NEW FEDERAL LEADERSHIP

In 2013, in response to an Executive Order, the National Institute of Standards and Technology (NIST) began developing the first national cybersecurity framework consistent with its mission to promote U.S. innovation and competitiveness.[123] In May 2017, applying the framework, widely touted by cybersecurity experts, became mandatory for federal agencies.[124] Compliance is still voluntary in the private sector, with NIST estimating a 50 percent adoption rate among private actors in 2020.[125]

In May 2021, President Biden issued Executive Order (EO) 14028 focused on improving the nation's cybersecurity and protecting federal government networks, building on past executive action, including executive orders issued in 2017 and 2013.[126] Although the primary aim of the EO is to strengthen federal systems, it also notes that much of the nation's infrastructure is owned and operated by the private sector and encourages these companies to "follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents."[127] The EO also establishes a Cybersecurity Review Board, modeled after the National Transportation Safety Board, composed of private sector entities and federal officials to review significant cyberattacks and share lessons learned.[128]

Following the EO, in June 2021, CISA issued guidance on Ransomware for Operators of Critical Infrastructure.[129] CISA's guidance addresses increasingly complex IT and OT systems that play a pivotal role in critical infrastructure, where the attack surfaces have expanded well beyond once-isolated systems.[130] The guidance will assist in establishing standards for preparing, mitigating, and responding to cyberattacks targeting critical infrastructure.[131]

In July 2021, the Biden administration also issued the National Security Memorandum on *Improving Cybersecurity for Critical Infrastructure Control Systems*.[132] The memorandum called for creating cyber-performance goals for critical infrastruc-

[121] CISA, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, (accessed on October 22, 2021), at https://www.cisa.gov/nice-cybersecurity-workforce-framework and CISA, *Girls Who Code Announce Partnership to Create Career Pathways for Young Women in Cybersecurity and Technology*, accessed on October 22, 2021, *available at* https://www.cisa.gov/news/2021/09/30/cisa-and-girls-who-code-announce-partnership-create-career-pathways-young-women.

[122] U.S. Digital Service, "Our Mission," *accessed on* https://www.usds.gov/mission.

[123] NIST, *History and Creation of the Framework*, (accessed on October 22, 2021), *available at* https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework.

[124] NIST, *Questions and Answers*, (accessed on October 22, 2021), *available at* https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics; Brandon Vigliarolo, *NIST Cyber Security Framework: A Cheat Sheet for Professionals* (March 5, 2021), *available at* https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/.

[125] NIST, *Cybersecurity Framework, available at* https://www.nist.gov/industry-impacts/cybersecurity-framework/ (*last visited October 22, 2021*).

[126] The White House, *Executive Order on Improving the Nation's Cybersecurity*, (May 12, 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; *see also* The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, (May 11, 2017), *available at* https://www.govinfo.gov/content/pkg/DCPD-201700327/pdf/DCPD-201700327.pdf; The White House, *Improving Critical Infrastructure Cybersecurity*, (Feb. 12, 2013), *available at* https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636.

[127] The White House, *FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cyber Security and Protect Federal Government Networks*, (May 12, 2021), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.

[128] *Id.*

[129] CISA, *Rising Ransomware Threat to Operational Technology Assets* (June 9, 2021).

[130] CISA, *FACT SHEET: Rising Operational Threat to Operating Technology Assets, available at* https://www.cisa.gov/sites/default/files/publications/CISA__Fact__Sheet-Rising__Ransomware__Threat__to__OT__Assets__508C.pdf (*last visited* October 22, 2021).

[131] *Id.*

[132] The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*, (July 28, 2021), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

ture companies, including the establishment of baseline cybersecurity performance standards across all infrastructure sectors.[133]

The Biden administration has supplemented voluntary cooperative efforts with new mandatory standards to protect critical infrastructure in some sectors.[134] At the end of July, TSA issued a security directive requiring owners and operators of TSA-designated critical pipelines to implement specific mitigation measures to protect against ransomware attacks and other known threats to IT and OT systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review to supplement mandatory cyber protocol requirements related to pipelines issued two months earlier.[135] TSA is reportedly preparing similar directives for the rail and aviation sectors. The DHS Secretary reports the administration continues "coordinating and consulting with industry as we develop all of these plans."[136] Given the Committee's role in the safety of transportation industries, as TSA issues directives, it will closely monitor these directives.

VOLUNTARY REPORTING AND LACK OF GOVERNMENT DATA SHARING

Reporting cybersecurity incidents—across the critical infrastructure spectrum—is also largely voluntary, a decades-old legacy of the days before large-scale cyberattacks and networked critical infrastructure.[137] Many actors responsible for critical infrastructure agree that what should be reported and to whom in the federal, state, and local governments regarding a cyber incident can be unclear.[138] Further, requiring private entities to report cybersecurity-related data to the government has long been subject to debate, and the complexity of some proposed reporting models has raised concerns about the disproportionate burdens placed on smaller private actors.[139] Therefore, a complete understanding of the cyber threats to the nation is likely underestimated in the face of these dynamics. In 2016, for example, the FBI estimated that only 15 percent of cybercrime victims reported the crime to law enforcement.[140]

Recent EO 14028 also encourages sharing cyber-related threat data between the private sector and the federal government and requires federal IT contractors to report cyber incidents to the government, although reporting cyber incidents from privately-owned infrastructure assets or transportation systems remains voluntary.[141] Obtaining a more holistic picture of the cyber threats our transportation systems and infrastructure assets face may help improve their own responses and the federal government's ability to identify these threats.[142]

While CISA leadership has recently expressed an interest in mandatory 24-hour reporting, potentially supported by fines for non-compliance, the private sector does not appear fully in favor of this approach.[143] Some private actors responsible for critical infrastructure have concerns with reporting cyber incidents to the federal

[133] *Id.*, Sec. 4.

[134] CRS, *Pipeline Cybersecurity: Federal Programs*, (September 9, 2021), pp 9–11, *available at* https://crsreports.congress.gov/product/pdf/R/R46903.

[135] *Id.*, p 10.

[136] DHS, *Secretary Mayorkas Delivers Remarks at the 12th Annual Billington CyberSecurity Summit*, (October 6, 2021), *available at* https://www.dhs.gov/news/2021/10/06/secretary-mayorkas-delivers-remarks-12th-annual-billington-cybersecurity-summit.

[137] Tatiana Tropina, *Public-Private Collaboration: Cybercrime, Cybersecurity and National Security*, (May 7, 2015); Alan Raul and Vivek Mohan, *The Privacy, Data Protection and Cybersecurity Law Review—United States* (Sept. 2018), 276–403, *available at* https://datamatters.sidley.com/wp-content/uploads/2018/11/United-States.pdf.

[138] Sujit Ramen, Bloomberg Law, *It's Time for National Cyber-Incident Reporting Legislation*, (July 12, 2021), *available at* https://news.bloomberglaw.com/us-law-week/its-time-for-national-cyber-incident-reporting-legislation.

[139] Coalfire, *Compliance in the Era of Digital Transformation* (May 24, 2021); Alan Raul and Vivek Mohan, *The Privacy, Data Protection and Cybersecurity Law Review—United States* (Sept. 2018), 276–403, *available at* https://datamatters.sidley.com/wp-content/uploads/2018/11/United-States.pdf.

[140] FBI, *2016 Internet Crime Report*, p. 4, (accessed on October 22, 2021), *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf.

[141] The White House, *Executive Order on Improving the Nation's Cybersecurity*, (May 12, 2021). Sec. 2, *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[142] CISA, *Information Sharing and Cyberawareness, available at* https://www.cisa.gov/information-sharing-and-awareness (*last visited* October 22, 2021).

[143] Adam Mazmanian, FCW, *CISA Seeks 24-Hour Timeline for Cyber Incident Reporting* (Oct 19, 2021), *available at* https://fcw.com/articles/2021/10/19/cisa-wales-reporting-timeline-cyber-incident.aspx.

government.[144] These concerns include bad press, regulatory reprisal, or minimal public consequences for cyber attackers.[145] Further, private actors who proactively seek out information from the federal government on current threats or reported vulnerabilities report being frustrated by the information sharing practices of the federal government.[146] Collaboration and coordination between the public and private sector in protecting the nation's critical infrastructure is critical, but still a work in progress.[147]

CONCLUSION

As America seeks to remain globally competitive and provide Americans with safe and secure infrastructure, cybersecurity will remain a top priority. During this hearing, the Committee will hear from private sector witnesses, but it intends to hold a second cybersecurity hearing on these issues in the future that will focus on federal agencies and their efforts to close the current cybersecurity gaps that put industry and government at greater risk of attacks, actions to assist the private sector, and what steps they are taking to implement recent federal cybersecurity directives.

WITNESS LIST

- Scott Belcher, President and Chief Executive Officer, SFB Consulting, LLC, *testifying on behalf of* Mineta Transportation Institute
- Megan Samford, Vice President and Chief Product Security Officer, Schneider Electric
- Thomas L. Farmer, Assistant Vice President, Security, Association of American Railroads
- Michael Stephens, General Counsel and Executive Vice President, Tampa International Airport
- John Sullivan, Chief Engineer, Boston Water and Sewer Commission, *testifying on behalf of* the Water Information Sharing and Analysis Center (WaterISAC)
- Gary Kessler, PhD, President, Gary Kessler Associates, *testifying on behalf of* The Atlantic Council

[144] Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cyber Security* (Dec 14, 2014), *available at* https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity.

[145] Dan Swinhoe, CSO, *Why businesses don't report cybercrimes to law enforcement* (May 30, 2019), *available at* https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html.

[146] Samantha Swartz, Cybersecurity Dive, *What Happens if Threat Data Isn't Shared?* (April 30, 2021), *available at* https://www.cybersecuritydive.com/news/information-sharing-threat-intelligence-analysis-cybersecurity/599319/; Jonathan Day and Michael Mahoney, *Private Sector Wants More—and Better—Cybersecurity Cooperation with Government* (Mar 9, 2020), *available at* https://morningconsult.com/opinions/private-sector-wants-more-and-better-cybersecurity-cooperation-with-government/.

[147] Jason Miller, Federal News Network, (*CISA's still overcoming challenges 5 years after Cybersecurity Information Sharing Act became law*, October 6, 2020), *available at* https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/10/cisas-still-overcoming-challenges-5-years-after-cybersecurity-information-sharing-act-became-law/.

Mr. DEFAZIO. The Committee on Transportation and Infrastructure will come to order.

I ask unanimous consent that the chair be authorized to declare a recess at any time during today's hearing.

Without objection, so ordered.

As a reminder, please keep your microphone muted, unless speaking. Should I hear any inadvertent background noise, I will request the Member please mute their microphone, or I will yell at you.

To insert a document into the record, please email it to DocumentsT&I@mail.house.gov.

With that, I will yield myself such time as I may consume.

Today, we are going to hear about the challenges and gaps in protecting our Nation's transportation systems and critical infrastructure from cyberattacks, and recommendations from private industry and cybersecurity experts on how to close those gaps.

Notably, this hearing is largely being conducted online, demonstrating how much we all rely on cyber systems to carry out our basic day-to-day tasks, particularly in the era of COVID.

And even with dedicated and superb IT support and lots of experience, getting everything right 100 percent of the time is tough. Well, with the House system it is not even close to that. But anyway, we won't go into that.

But when it comes to the Nation's critical infrastructure and transportation networks—pipelines that fuel our economy, water and wastewater treatment plants, shipping, aviation, railroads, and highways that play a critical role in bringing vital supplies to all Americans—getting everything right every time must be the goal. Lives are on the line. And each day, when you turn on a faucet, flush your toilet, or when you board a plane, fill up your car with gas, you trust that these systems will work.

But that trust has been shaken in recent years. We have seen headlines about blows to the Nation's economy from ransomware attacks by criminal networks on critical infrastructure, and close calls where individual hackers have tried to go after wastewater systems. By the way, they have, many of them, used massive amounts of chlorine. If they can valve that chlorine into the air, they are going to kill a lot of people. And otherwise infiltrate our drinking water systems.

The cyber threats and vulnerabilities are diverse, expanding, and constantly evolving, and have the potential to impact everyone. Yet, an estimated 85 percent—85 percent—of the Nation's critical infrastructure is in private hands, owned and operated by private entities.

Too often, leaders whose organizations are at risk from cyberattacks weigh the risks of an attack against the cost of increasing cybersecurity protections, and they decide to roll the dice. Hey, it might hurt the stock price if we actually spend a little money on an updated IT system, or better cybersecurity, and, hey, that will hurt my annual bonus. So, let's skate, and hope we get away with it. They are betting they won't get attacked.

The good news is, even basic steps, like mandating strong passwords—pathetic—and multifactor authentication, cybersecurity awareness training, and regularly practicing simple cybersecurity exercises, things that cost virtually nothing, and are common sense, can significantly harden cyber defenses and dramatically diminish a company, utility, or Federal agency's chances that they will fall victim to a successful attack.

Unfortunately, recent surveys have shown that too many public and private entities don't take these simple steps. In a recent survey of the transit sector, nearly 39 percent of those surveyed have no—none, zero—staff dedicated to cybersecurity, and more than 24 percent provide no cybersecurity training to their staff at all. Many of them are using the password on the device when they got it. They don't—you know, just crazy stuff. This doesn't cost anything.

The water sector is even worse. In a survey published in June of this year, 42 percent of water and wastewater utilities surveyed said they conduct no—no, zero—cybersecurity training for their staff, and more than 68 percent of them said they do not participate in any cybersecurity-related drills or exercises.

Many experts believe we don't have a full and transparent picture of the cybersecurity threats that confront us, impeding our ability to quantify the risks and to learn about lessons from past attacks. Reporting cyber breaches, yes, it can hurt your financial bottom line for a little bit, but overall, in the end, you are going to benefit, your stockholder is going to benefit, the American people are going to benefit if you put these protections in place.

The FBI has estimated only 15 percent of cyber crimes are actually reported—15 percent—to the Government. In a recent survey of the transit sector, more than 30 percent of those surveyed said they had been the victim of a cybersecurity incident, but they never reported the incident to anybody.

With the public's safety and national economic security of the United States at stake, it may be time for voluntary steps by the private sector to give way to mandatory Federal reporting requirements.

In 2013, NIST, the National Institute of Standards and Technology, in consultation with industry, academia, and Government, created a cybersecurity risk management framework. Since 2017, the framework has been mandatory for Federal agencies, but it hasn't eliminated all the problems, something that we will explore more at a future hearing.

In the private sector, however, use of the NIST framework remains voluntary and is used unevenly. NIST estimated that, in 2020, only 50 percent of private companies were even trying to reach NIST cybersecurity minimum standards.

The Biden administration has finally begun to change things. In May 2021, the President issued Executive Order 14028 to encourage critical infrastructure companies to, quote: "follow the Federal Government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents."

In June of this year, DHS's Cybersecurity and Infrastructure Security Agency issued guidance that addresses complex networked IT and operational technology, or OT systems, and helps to establish standards for preparing and responding to cyberattacks targeting critical infrastructure. The Biden administration also issued a National Security Memorandum that called for the creation of cyber performance goals, including establishing baseline cybersecurity performance standards consistent across all critical infrastructure sectors.

Just this summer, in the wake of the Colonial Pipeline cyberattack, the Transportation Security Administration abandoned voluntary compliance. They had already offered to do a full audit of cybersecurity for Colonial Pipeline. Colonial Pipeline—it wouldn't have cost them anything—they didn't want to do that, because they didn't want to know what their problems were. Well, it cost them a lot of money, and they could have had an evaluation, and perhaps closed the door before the ransomware attack.

So, the TSA has abandoned voluntary compliance for pipelines altogether, issuing a directive mandating specific protections to defend against ransomware, along with cybersecurity contingency and recovery plans. TSA is reportedly preparing similar directives for other critical infrastructure sectors, including rail and aviation.

So, we have an administration that is moving in the right direction. We need to do more.

No single technology, policy, or other action will completely eliminate all cyber threats. But every step can help close the gaps and make success for cyber criminals and cyber terrorists harder.

I look forward to hearing our witnesses' ideas about how we can do that. You have been in the trenches of the silent cyber conflict that goes on every day in our critical infrastructure sectors. You all have ideas on how Government, private industry, or both, working together, can increase our Nation's cyber resilience to protect our critical infrastructure and public, and to recover from cyberattacks when they do occur, despite our best efforts.

So, thanks to our witnesses for joining us, and I will turn now to the ranking member, Mr. Crawford, for his opening remarks.

[Mr. DeFazio's prepared statement follows:]

Prepared Statement of Hon. Peter A. DeFazio, a Representative in Congress from the State of Oregon, and Chair, Committee on Transportation and Infrastructure

Today we will hear about the challenges and gaps in protecting our nation's transportation systems and critical infrastructure from cyberattacks, and recommendations on how to close those gaps from private industry and cybersecurity experts. Notably, this hearing is largely being conducted online, demonstrating how much we all rely on cyber systems to carry out basic day-to-day tasks. Even with dedicated and superb IT support and lots of experience, getting everything right 100 percent of the time, is tough.

But when it comes to the nation's critical infrastructure and transportation networks—pipelines that fuel our economy, water and wastewater treatment plants, shipping, aviation, railroads, and highways that play critical roles in bringing vital supplies to all Americans—getting everything right, every time, must be the goal. Lives are on the line, and each day when you turn on a faucet or flush your toilet, when you board a plane, or fill up your car with gas, you trust that these systems will work.

But that trust has been shaken in recent years. We have seen headlines about blows to the nation's economy from ransomware attacks by criminal networks on critical infrastructure, and close calls where disgruntled individual hackers have tried to turn water from our faucets into poison that would do us harm.

These cyber threats and vulnerabilities are diverse, expanding, and constantly evolving, and have the potential to impact everyone. Yet, an estimated 85 percent of the nation's critical infrastructure is in private hands, owned and operated by private entities.

Too often leaders whose organizations are at risk from cyberattacks weigh the risks of an attack against the cost of increasing cybersecurity protections and they decide to roll the dice, betting they won't get attacked. The good news is, even basic steps like mandating strong passwords and multi-factor authentication, cybersecurity awareness training, and regularly practicing simple cybersecurity exercises can significantly harden cyber defenses and dramatically diminish a company, utility, or federal agency's chances that they will fall victim to a successful attack.

Unfortunately, recent surveys have shown that too many public and private entities don't take these simple steps. In a recent survey of the transit sector nearly 39 percent of those surveyed had no staff dedicated to cybersecurity and more than 24 percent provide no cybersecurity training to their staff at all. The water sector is even worse. In a survey published in June of this year, 42 percent of the water and wastewater utilities surveyed said they conduct no cybersecurity training for their staff and more than 68 percent of them said they do not participate in any cybersecurity-related drills or exercises.

Many experts believe we don't have a full and transparent picture of the cybersecurity threats that confront us, impeding our ability to quantify the risks and to learn the lessons from past attacks. Reporting cyber breaches can be harmful to a company's financial bottom line, endangering a company's reputation and their stock price, for instance. Overall, the FBI has estimated only 15 percent of cybercrimes are actually reported to the government at all. In a recent survey of the transit sector, more than 30 percent of those surveyed who said they had been the victim of a cybersecurity incident said they never reported the incident to anyone.

With the public's safety and the national and economic security of the United States at stake, it may be time for voluntary steps by the private sector to give way to mandatory federal reporting requirements.

In 2013, the National Institute of Standards and Technology, or NIST, in consultation with industry, academia, and government, created a cybersecurity risk management framework. Since 2017, that framework has been mandatory for federal agencies, but it has not eliminated all problems, something we will explore more at a future hearing. In the private sector, however, use of the NIST framework remains voluntary, and it is used unevenly. NIST estimated that in 2020 only 50 percent of private companies were even trying to reach NIST cybersecurity minimum standards.

The Biden administration has finally begun to change things. In May 2021, the president issued Executive Order 14028 to encourage critical infrastructure companies to quote, "follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents."

In June of this year, DHS's Cybersecurity and Infrastructure Security Agency issued guidance that addresses complex, networked IT and Operating Technology, or OT, systems and helps to establish standards for preparing and responding to cyberattacks targeting critical infrastructure.

The Biden administration also issued a national security memorandum that called for the creation of cyber-performance goals including establishing baseline cybersecurity performance standards consistent across all critical infrastructure sectors.

In late summer, in the wake of the Colonial Pipeline cyberattack, the Transportation Security Administration abandoned voluntary compliance for pipelines altogether, issuing a directive mandating specific protections to defend against ransomware attacks, along with cybersecurity contingency and recovery plans. The TSA is reportedly preparing similar directives for other critical infrastructure sectors, including rail and aviation.

So, we have an administration that is moving in the right direction. But we need to do more. No single technology, policy, or other action will completely eliminate all cyber threats. But each step can help close the gaps and make success for the cybercriminals and cyberterrorists harder.

I look forward to hearing our witnesses' ideas about how we can do that. You all have been in the trenches of the silent cyber conflict that goes on each day in our critical infrastructure sectors. And you all have ideas on how government, private industry, or both working together can increase our nation's cyber resilience to protect our critical infrastructure and the public, and to recover when cyberattacks do occur, despite our best efforts.

So, thank you to our witnesses for joining us. I look forward to your testimony. With that I recognize Ranking Member Graves for his opening statement.

Mr. CRAWFORD. Thank you, Mr. Chair. As we all know, the cyber threats facing our Nation's infrastructure have increased significantly as technology has become more essential and interwoven in our society, both in infrastructure and more broadly in our daily lives. While technology has allowed us to innovate and create efficiencies in infrastructure and transportation networks, it has also brought us new threats and vulnerabilities.

Unfortunately, with recent high-profile cyberattacks like those conducted on Colonial Pipeline or various wastewater treatment plants, we have seen a very clear need to better protect our Nation's infrastructure through strong cybersecurity defense measures.

Fortunately, many transportation and infrastructure operators are already taking action to protect their assets and the passengers and customers that rely on them.

While the Federal Government is working to help the private sector prevent, mitigate, and respond to cyber threats, our cyber adversaries' technology is advancing more quickly than anything the Federal Government can mandate. In light of this reality, I look forward to hearing from our witnesses today about their best practices for cyber defense across varying transportation modes.

I would also like to highlight a specific concern regarding the TSA's recent mandatory security directives on cybersecurity for pipelines, and forthcoming directives for rail, transit, and aviation. I am concerned that the TSA's recent security directives are overly prescriptive, rushed, and fail to take into account holistic feedback from diverse stakeholders. I would like to hear stakeholders' input on this issue today, but we must also hear from Government witnesses to get the full picture. So, I look forward to following up on this topic to ensure that we get every perspective, as well.

We need to hear how the various agencies are working with the operators of our Nation's infrastructure as true partners in improving the standards and practices we are using to protect America's infrastructure and transportation networks from growing cyber threats.

Thank you, and I yield back the balance of my time.

[Mr. Crawford's prepared statement follows:]

Prepared Statement of Hon. Eric A. "Rick" Crawford, a Representative in Congress from the State of Arkansas

Thank you, Chair DeFazio.

As we all know, the cyber threats facing our Nation's infrastructure have increased significantly as technology has become more essential and interwoven in our society—both in infrastructure, and more broadly in our daily lives. While technology has allowed us to innovate and create efficiencies in infrastructure and transportation networks, it has also brought us new threats and vulnerabilities.

Unfortunately, with recent high-profile cyberattacks, like those conducted on the Colonial Pipeline, or various wastewater treatment plants, we have seen a very clear need to better protect our Nation's infrastructure through strong cybersecurity defense measures.

Fortunately, many transportation and infrastructure operators are already taking action to protect their assets, and the passengers and customers that rely on them.

While the federal government is working to help the private sector prevent, mitigate, and respond to cyber threats, our cyber adversaries' technology is advancing more quickly than anything the federal government can mandate. In light of this reality, I look forward to hearing from our witnesses today about their best practices for cyber defense across varying transportation modes.

I also want to highlight a specific concern regarding the Transportation Security Agency's (TSA) recent mandatory security directives on cybersecurity for pipelines and forthcoming directives for rail, transit, and aviation.

I am concerned that TSA's recent security directives are overly prescriptive, rushed, and fail to take into account wholistic feedback from diverse stakeholders. I want to hear stakeholders' input on this issue today, but we must also hear from government witnesses to get the full picture. So, I look forward to following up on this topic to ensure we get that perspective as well.

We need to hear how the various agencies are working with the operators of our Nation's infrastructure as true partners in improving the standards and practices we're using to protect America's infrastructure and transportation networks from growing cyber threats.

Thank you and I yield back the balance of my time.

Mr. DEFAZIO. I thank the gentleman. I will now like to welcome the witnesses on our panel: Scott Belcher, president and chief executive officer, SFB Consulting, LLC, testifying on behalf of the Mineta Transportation Institute; Megan Samford, vice president, chief product security officer–energy management, Schneider Electric, on behalf of the International Society of Automation Global Cybersecurity Alliance; Thomas L. Farmer, assistant vice president–security, Association of American Railroads; Michael Stephens, general counsel and executive vice president for information technology, Tampa International Airport; John Sullivan, chief engineer, Boston Water and Sewer Commission, testifying on behalf of the Water Information Sharing and Analysis Center; and Gary Kessler, nonresident senior fellow, Atlantic Council.

Thanks for joining to us today and giving us some of your time. We look forward to your testimony.

Without objection, all of your full statements will be included in the record, and I would ask you to summarize in 5 minutes your most succinct and telling points.

With that, I would now recognize Mr. Belcher for 5 minutes.

[Pause.]

Mr. BELCHER. There we go.

Mr. DEFAZIO. Mr. Belcher? Oh, there we go.

Mr. BELCHER. Chairman DeFazio, there we go.

TESTIMONY OF SCOTT BELCHER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, SFB CONSULTING, LLC, ON BEHALF OF MINETA TRANSPORTATION INSTITUTE; MEGAN SAMFORD, VICE PRESIDENT, CHIEF PRODUCT SECURITY OFFICER–ENERGY MANAGEMENT, SCHNEIDER ELECTRIC, ON BEHALF OF THE INTERNATIONAL SOCIETY OF AUTOMATION GLOBAL CYBERSECURITY ALLIANCE; THOMAS L. FARMER, ASSISTANT VICE PRESIDENT–SECURITY, ASSOCIATION OF AMERICAN RAILROADS; MICHAEL A. STEPHENS, GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT FOR INFORMATION TECHNOLOGY, HILLSBOROUGH COUNTY AVIATION AUTHORITY, TAMPA INTERNATIONAL AIRPORT; JOHN P. SULLIVAN, P.E., CHIEF ENGINEER, BOSTON WATER AND SEWER COMMISSION, ON BEHALF OF THE WATER INFORMATION SHARING AND ANALYSIS CENTER; AND GARY C. KESSLER, PH.D., NONRESIDENT SENIOR FELLOW, ATLANTIC COUNCIL

Mr. BELCHER. Chairman DeFazio, Ranking Member Crawford, and members of the committee, thank you for the opportunity to appear for you today and discuss the pressing need to strengthen cybersecurity capabilities of the U.S. public transit.

Enterprise risk management in the U.S. public transit industry needs a 21st-century upgrade.

Mr. DEFAZIO. Mr. Belcher, could you either perhaps speak up a little, turn up your volume, or maybe we can do it on our end? Just a little bit would be great.

Mr. BELCHER. OK, let me—enterprise risk management in the U.S. public transit industry needs a 21st-century upgrade, whereby specific attention is paid to strengthening cyber protection and preparedness across the industry.

Is that better? Can you hear me better now?

Mr. DEFAZIO. Yes, thank you.

Mr. BELCHER. OK. It is critical that transit agencies better understand how their risk profile is changing, and the threat landscape is evolving. Even the smallest and most conventional public transit agencies today rely on multiple digital technologies that expose them to cyber threats, whether it is through digital enabled hardware or systems that are managed in their yards.

Last year, my colleagues and I released a report from the Mineta Transportation Institute entitled, “Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness.” Our bottom line takeaway was that most transit operators have a lot of work to do to elevate their understanding of and preparedness for cyber-related risks to their operations, their data, and their business infrastructure. Our report concludes that, for many transit agencies, internal resources for cybersecurity are scarce, and even among those agencies that have resources, and that are aware, acquiring these resources are a long and laborious activity.

In our view, there needs to be a collaborative effort between the Federal Government, the industry, and agency leadership to establish, maintain, refine, and support cybersecurity programs.

Most transit agencies are unprepared to prevent or respond to the broad array of threat vectors, ranging from phishing and business email compromise to data breaches and ransomware attacks.

In fact, a key finding from our report is that many agencies do not have an accurate sense of their cybersecurity preparedness.

On the one hand, 81 percent of the responding agencies believe that they are prepared to manage and defend against cybersecurity threats. In fact, 73 percent of those respondents felt that they had adequate information to help implement their cybersecurity preparedness programs. Even so, only 60 percent of the respondents have a cybersecurity program in place; 43 percent of the respondents do not believe they have the resources necessary for cybersecurity preparedness; and only 47 percent of the respondents audit their cybersecurity programs on an annual basis. That is simply unacceptable.

Despite the industry differences, cybersecurity maturity models exist, and assessment practices that are used across other industries are transferable, and can be transferred and utilized in the transit industry.

The transit industry is experiencing an increasing number of high-profile attacks. We have seen the Metropolitan Transportation Authority in New York City, we have seen Martha's Vineyard Ferry in Massachusetts, we have seen the Southeastern Pennsylvania Transportation Authority, or SEPTA, in Philadelphia be hacked in the last year. And in fact, just last week we saw the Toronto Transit Commission be attacked by a malware attack, and that had a significant impact. And in fact, between June of 2020 and June of 2021, there has been a 186-percent increase in weekly ransomware attacks in the transportation industry.

Risk management priorities identified by transit executives identified that business continuity and data protection are the two areas most immediately at risk to cyber threats.

So, with that, thank you for the opportunity, and for your continued leadership in this space. My written testimony has been submitted for the record, and I look forward to responding to your questions.

[Mr. Belcher's prepared statement follows:]

Scott Belcher, President and Chief Executive Officer, SFB Consulting, LLC, on behalf of Mineta Transportation Institute

Enterprise risk management in the U.S. public transit industry needs a twenty-first century upgrade, whereby specific attention is paid to strengthening cyber protections and preparedness across the industry. Risk as defined by most industry providers focuses primarily on the physical risks posed to the organization and its service delivery. Investments have been made for decades to reduce this risk, as it is understood that most threats that are likely to impair transit operations with regularity are physical (*e.g.*, threats against operators and passengers, damage to vehicles, and theft). However, as digital technologies continue to be woven into the operations of even the most conventional public transit agency, any system, process, or function dedicated to reducing physical risk likely includes an array of digital vulnerabilities that need to be managed in concert with current security operations. The increasing frequency and magnitude of cyber threats also increases their potential to negatively impact existing systems designed to reduce physical risk. Risk governance decisions should prioritize potential physical threats, but the design and management of any comprehensive enterprise risk infrastructure in today's world must improve and integrate cybersecurity best practices alongside the physical security priorities.

Based on the findings of the 2020 Mineta Transportation Institute (MTI) Report, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations* *to Enhance Surface Transit Cyber Preparedness*[1] (hereinafter, the 2020 MTI Report) and research to date, the authors believe transit operators need to elevate their understanding of and preparedness for cyber-related risks to their operations, data, and business infrastructure. Further, given the dependence transit agencies have on vendors, opportunities exist for the industry to enlist the help of the vendor community to support and in some cases lead the improvement of cyber risk management across the supply chain.

> *Enterprise Risk Management*: The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.[2]

The 2020 MTI Report highlights that some agencies have taken action to protect themselves by seeking technical leadership from outside the transit industry, contracting out the management of personally identifiable information (PII), and seeking support from their supply chain partners. Some include cybersecurity requirements in their contracts with suppliers, one of the more basic and least expensive means to begin maturing an organization's cyber risk posture. And still others have operationalized cybersecurity requirements through actions in partnership with their supply chain, such as annual audits and ongoing monitoring and alerting that is closely coordinated between agency and vendor. Many agencies, however, have not yet embarked on such efforts.

The 2020 MTI Report concludes that for many transit agencies, internal resources for cybersecurity are scarce, as even among those agencies and individuals that recognize the growing threat, acquisition of necessary resources is a long, laborious activity. In the view of the authors, there needs to be a collaborative effort between the federal government, the industry, and transit agency leadership to establish, maintain, refine, and support cybersecurity programs. Both carrots and sticks are required to ensure the necessary resources are made available and utilized. The authors emphasize that the Federal Transit Administration (FTA) should require transit organizations to adopt and implement minimum cybersecurity standards prior to receiving federal funding. To date, the U.S. Department of Transportation, and the FTA has largely deferred to the Transportation Security Administration (TSA) in this space. This is about to change.

Transportation infrastructure is a target for nefarious actors seeking to disrupt, be it for personal or political gain. The avenues to exploit this vital infrastructure will continue to evolve along with the technology that enables the industry's core operations and goals. As these technologies are further embedded in operations, new vulnerabilities will arise. Accounting for the risk today will foster greater resiliency and preparedness in the years to come.

The mission of public transit is to move people as safely and efficiently as possible. Public transportation is a multi-faceted, complex, and expansive ecosystem that relies on people, processes, and associated technologies to ensure that it achieves its mission as seamlessly as possible. Security has always been a foundational aspect of public transit operations. Moving people at scale has inherent risk, and every transit agency takes deliberate steps to reduce physical risk wherever possible. An unsafe public transit system impairs the agency in executing its mission, as the public's sense of safety has a direct correlation to their willingness

[1] https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness

[2] https://csrc.nist.gov/glossary/term/enterprise_risk_management

to use the public transit system to move about the community. Digital technologies are playing an increasingly important role in operations security. It is critical that transit agencies understand how their risk profile is changing, and ensure their systems, processes, and procedures engaged to address such risk are effectively resourced and adequately managed.

The transit industry depends on a myriad of technologies, from the physical systems that manage access to the garage to the databases that house operational data or employee information. Technological advancements in general and their expanded application to the transit industry more specifically offer significant advantages for both providers and customers—improved service quality, operational efficiencies, and reduced costs. With each of these advancements, however, comes an additional level of risk that must be weighed and managed by transit providers and their suppliers. Cyber vulnerabilities attributable to the expanding digital ecosystem are prime among these growing risks.

In the 2020 MTI Report, the authors described the unprecedented increase in the volume of data collected and maintained by modern transit operators, the addition of numerous vendors to help manage these growing technology demands on the industry, and the resulting need to spend more time and money securing newly exposed cybersecurity threats. Many transit agencies, the report found, were unprepared to prevent or respond to the broad array of identified threat vectors—ranging from phishing and business email compromise to data breaches to ransomware attacks.

A key finding from the 2020 MTI Report is that many agencies do not have an accurate sense of their cybersecurity preparedness.

- 81% of responding agencies believe they are prepared to manage and defend against cybersecurity threats, and;
- 73% feel they have access to information that helps them implement their cybersecurity preparedness program

Yet . . .

- Only 60% actually have a cybersecurity preparedness program;
- 43% do not believe they have the resources necessary for cybersecurity preparedness; and
- Only 47% audit their cybersecurity program at least once per year.[3]

It is essential for transit agencies to develop and maintain mature enterprise risk management systems to mitigate threats to people, operations, and data. This need is neither new nor unique to the transit industry. Part of running any business is taking the necessary steps to protect critical assets. The added challenge organizations face today, however, is the increasing role of digital technologies in all areas of business operations. The resulting need is to have robust cyber risk management practices that span the organization to ensure the continued protection of critical assets.

Moreover, greater cybersecurity oversight is on its way. The Biden Administration has been vocal about the need for greater engagement in cybersecurity oversight by the federal government. The President on May 12, 2021, issued an Executive Order stating:

> It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.[4]

[3] https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness p. 32.

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

The Executive Order applies specifically to Federal agencies and their suppliers, but it is only a matter of time before the extensive set of requirements included in this Executive Order flow down to recipients of Federal funds.

In a similar vein, the Department of Defense on November 20, 2020, began implementation of the Cybersecurity Maturity Model Certification (CMMC), which is a unifying standard for vendors to ensure they are implementing cybersecurity across the Defense Industrial Base (DIB).

> The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.[5]

Again, while the CMMC currently only applies to contractors in the DIB, procurement practices that start in the defense arena regularly move into the non-defense arena and procurement and cybersecurity professionals both anticipate this transition.

Finally, Congress has introduced several bills to address cyberattacks against private-sector targets and critical infrastructure, which includes the U.S. transportation sector. The U.S. House Energy and Commerce Committee on July 20, 2021, passed eight cybersecurity bills. The eight-bill package will increase requirements for private companies to report on cybersecurity incidents and provide funding for state and local governments to increase cybersecurity measures.[6] Subsequently, Senator Mark Warner (D–VA) on July 22, 2021, introduced a bipartisan bill that would require the Cybersecurity and Infrastructure Security Agency (CISA) to identify and mitigate threats to the operational technology systems of pieces of critical infrastructure.[7]

Both the public and private sector have developed a great deal of cybersecurity guidance over the past two decades. Cybersecurity experts will tell you that the tools used to manage cybersecurity and associated threats do not vary greatly across industries but that some industries are more mature in their understanding when it comes to managing cyber risks. Industries such as the financial management industry where billions of dollars are moved digitally every minute have been forced to invest heavily in cybersecurity protection. Other industries such as the transit industry, which has traditionally been a hardware-based industry that relied largely on firmware and closed networks, have not faced the same urgency until recently.

The 2020 MTI Report observes that "[t]he existing cybersecurity guidance for public transit is spread across numerous government and industry entities . . . [and that] federal resources exist for agencies to improve their cybersecurity readiness."[8] The same baseline documents are at the core of every industry cybersecurity program. Despite industry differences, cybersecurity maturity models and the assessment practices used to strengthen policies, procedures, and practices are transferable.

One of the key foundations for cybersecurity programs across any industry comes from the National Institute of Standards and Technology (NIST). NIST is a non-regulatory agency that has no authority to dictate the use of any standard, but its standards carry significant weight. The work of NIST is defined by federal statutes, executive orders, and policies—including developing cybersecurity standards and guidelines for federal agencies. NIST's cybersecurity program supports its overall mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and related technology through research and development.[9]

In 2014, NIST released the "Framework for Improving Critical Infrastructure Security" in response to Presidential Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[10] which called for a standardized security framework for

[5] https://www.acq.osd.mil/cmmc/faq.html

[6] https://energycommerce.house.gov/newsroom/press-releases/pallone-praises-committee-passage-of-eight-bipartisan-cybersecurity-bills

[7] https://www.warner.senate.gov/public/__cache/files/4/2/422a0de2-3c56-4e56-a4be-0e83af5b0065/F90B3C493BA4FAB09E546FAF40E4B116.alb21b95.pdf

[8] https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness MTI Report p. 35.

[9] https://www.nist.gov/cybersecurity

[10] Barack Obama. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11737, February 19, 2013, https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

critical infrastructure in the United States. This guidance is not intended to be a how-to guide for cybersecurity; rather, it is a framework designed to help a wide range of organizations assess risk and make sound decisions about prioritizing and allocating resources to reduce the risk of compromise or failure in their computer networks. For any organization to leverage the NIST Framework, customized implementation is required in ways that are not necessarily obvious from the document. The guidance is equally applicable to public and private industry.

To further support organizations in the face of a growing cyber threat, Congress established the CISA at the U.S. Department of Homeland Security (DHS) through the Cybersecurity and Infrastructure Security Agency Act of 2018.[11] According to DHS, "CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future."[12] CISA coordinates a collective defense to identify and vet procedures to manage and reduce the impact from disruption to critical infrastructure. In this role, the organization builds and coordinates relationships across industries working with sector specific agencies, such as the U.S. DOT, the FTA, the TSA, among others.

CISA's role is to unite government and private sector partners, with a particular focus on 16 Critical Infrastructure Sectors:

> There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[13]

The public transit industry is part of the Transportation Security Sector (TSS), which is one of the 16 critical sectors. As such, the industry has direct access to CISA's capabilities and resources, such as intelligence analysis, data assessment, response methods development, and assistance to manage risks to critical infrastructure that often spike from emerging threats. CISA leads a systematic approach to manage and reduce cyber risk that includes providing services, cyber training, support to critical infrastructure operators, and risk analysis.

The TSA is another critical cybersecurity player. TSA's origins date back to the days after September 11, 2001, when it was formed as part of the Aviation and Transportation Security Act. Its "mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce."[14] Given its provenance, TSA's original orientation centered on physical security, but the agency "is responsible for securing the nation's transportation systems from all threats, including both physical and cyber."[15] In this latter role, TSA overlaps with CISA. TSA explains the division of labor as follows:

> Although TSA has responsibility for oversight of both the physical security and cybersecurity of the [TSS], TSA is not directly responsible for the defense of the private sector portion of TSS information technology infrastructure. Rather, TSA serves a vital role in ensuring the cybersecurity resilience of the TSS infrastructure and will work with the Cybersecurity and Infrastructure Security Agency (CISA), with its mission to protect the critical infrastructure of the United States.[16]

DHS in 2015 built upon the NIST Framework and issued a document "to provide the TSS guidance, resource direction, and a directory of options to assist a TSS organization, [including public transit agencies], in adopting an industry-compatible version of the NIST Framework."[17] This guidance was designed both for transit agencies that have an existing risk-management program and for agencies that do

[11] https://www.congress.gov/bill/115th-congress/house-bill/3359

[12] https://www.cisa.gov/about-cisa

[13] https://www.cisa.gov/critical-infrastructure-sectors

[14] Transportation Security Administration (TSA), "Mission," https://www.tsa.gov/about/tsa-mission (accessed March 13, 2020).

[15] TSA, "TSA Releases Cybersecurity Roadmap," December 4, 2018, https://www.tsa.gov/news/releases/2018/12/04/tsa-releases-cybersecurity-roadmap (accessed March 13, 2020).

[16] TSA, "Cybersecurity Roadmap 2018," 4 November 2018, https://www.tsa.gov/sites/default/files/documents/tsa__cybersecurity__roadmap.pdf (accessed March 13, 2020).

[17] Department of Homeland Security (DHS), Transportation Systems Sector Cybersecurity Framework Implementation Guidance, 2 June 26, 2015, https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2__0.pdf (accessed February 24, 2020).

not yet have a formal cybersecurity program.[18] The TSS Cybersecurity Framework Implementation Guidance and its companion workbook provide an approach for Transportation Systems Sector[19] owners and operators to apply the tenets of the NIST Cybersecurity Framework to help reduce cyber risks.

Recent events have demonstrated the need to be proactive when it comes to cybersecurity. Major attacks such as SolarWinds, Colonial Pipeline, JBS Foods, and Acer have caused significant interruption and cost to the global economy. The transit industry has experienced a number of high-profile attacks as well. Cyber-attacks have involved the Metropolitan Transportation Authority (MTA) in New York City, the Martha's Vineyard Ferry in Massachusetts, and the Southeastern Pennsylvania Transportation Authority (SEPTA) in Philadelphia. Between June of 2020 and June of 2021, the global transportation industry witnessed a 186% increase in weekly ransomware attacks.[20]

This flood of activity and associated attention has raised a level of alarm throughout the government and the transit industry. Working with industry experts from other more mature fields such as financial management and defense, the researchers learned that the executives of these industries have come to treat cybersecurity threats as they treat the many other high-profile threats that the organizations' executive teams must evaluate, prioritize, and manage on an on-going basis.

Of the risk management priorities identified by transit executives, business continuity and data protection are the two areas most immediately at risk to cyber threats. The good news is that there are steps that transit providers can take—with the participation and support of vendors—to mature existing risk management practices and implement industry-specific cyber defenses.

People Safety

Creating and maintaining a safe environment for customers, employees, and the communities in which transit agencies provide services is essential for general risk mitigation and continuity of operations. Whether the safety incident involves a bus or train encountering another vehicle or an obstruction, or it involves a physical threat posed to a passenger, the transit operating system and its digital assets have rarely been directly involved. The increasing connectivity of vehicles both to other networked systems and to the internet is changing this dynamic.

Until recently, the potential for digital tools to access physical operating systems among most public transit agencies was not feasible, as most systems were safely segregated from the internet. The advent and exponential growth of internet-enabled devices has stripped most systems of this protection. Applications enabling automatic vehicle locator (AVL) or global positioning systems (GPS) technologies to track vehicles in real time, for example, are also generally reliant on connected and networked operating systems. Even the transition to electric buses brings with it a whole new level of cyber exposure and other security risks not previously anticipated.

Connected vehicle technologies that enable communication among vehicles on the road, infrastructure, and personal devices, can connect to the internet and vital operating systems—creating new access points for disruption. Transit operators have been piloting and, in some cases, deploying this new safety technology, which brings with it a new cybersecurity threat vulnerability that must be managed. Similarly, as transit operators test and deploy new levels of autonomy, whether it is for bus rapid transit or for first and last mile shuttles, they are exposing their operating systems and their passengers to new cyber risks. Fortunately, to date, there are no known recorded instances of malicious actors exploiting these vulnerabilities to remotely hijack or otherwise disrupt public transit vehicles. The access points to do so, however, are there and have been breached by researchers.

Business Continuity

Interruptions to day-to-day business operations face the most pronounced cyber risk because an increasing amount of transit operations relies on digitally connected systems. Everything from when a bus is scheduled to depart a yard to which operator should be driving it are managed by internet-enabled devices and systems.

[18] DHS, Transportation Systems Sector Cybersecurity Framework Implementation Guidance, June 26, 2015, 3, https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2__0.pdf (accessed February 24, 2020).

[19] CISA, "Transportation Systems Sector," https://www.cisa.gov/transportation-systemssector (accessed March 13, 2020).

[20] https://www.cybertalk.org/2021/07/28/ransomware-attacks-on-the-transportation-industry-2021/

Yard management and operator scheduling software are increasingly commonplace in public transit agencies. These systems, in turn, feed into public-facing route-planning services on which customers rely to complete their journeys. The public schedules also live on an increasing array of digital systems and services, from the agency's website and mobile applications to third-party services like Google Maps and Uber. A disruption to any one of these systems and the transmission of the data they produce can impair or halt service delivery. For example, SEPTA, suffered a ransomware attack resulting in severe network disruption in August 2020. Vancouver, Canada's TransLink transportation suffered a similar attack in December 2020. Like SEPTA, the services and systems on which TransLink relied to conduct day-to-day business operations were disrupted or sidelined. TransLink suffered from deactivated ticket kiosks and metro card readers, phone and internet outages, and offline GPS, tracking, and reporting services.

> *Operational Technology (OT)* is the hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events.
>
> *Information Technology (IT)* is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.[21]

Personal and Financial Data

The acquisition and exploitation of personal and financial data is a common goal of cyber criminals because it can be easily monetized in forums where individuals and organizations are willing to trade or pay for the information. Transit agencies are in possession of employee and customer data, specifically personal and financial information, which can hold appeal to nefarious actors. The previously cited Vancouver TransLink ransomware attack resulted in a lawsuit against TransLink by employees who accused the company of not doing enough to protect their personal and banking information—much of which was compromised during the attack.

As transit providers adopt new systems to augment and improve service—mobile pay, advanced trip planning, on-board Wi-Fi, etc.—they are increasingly likely to be in possession of more high-value customer data. Special services for older adults and paratransit services for individuals unable to use fixed route services may also require communication or documentation about sensitive health information—none of which the transit agency nor the customer wishes to have in the hands of a nefarious actor. Without implementing robust protection systems, the transit provider is likely to be risking the security of their passengers' data and may not even be in the position to know if or when a system is breached.

Most transit operators outsource fare management and the associated passenger data to PCI compliant vendors, which helps them to manage one of their biggest cybersecurity risks. Operators are now becoming more sophisticated in the contractual requirements that they impose upon their fare management partners to ensure that these vendors have a mature and comprehensive cyber protection system in place.

Transit operators are entering into a challenging new world where digital technology increases their cyber threat risks exponentially. Simultaneously, the Federal Government is increasing its focus on cybersecurity. As such, the transit industry will need to sharpen its focus, take advantage of available resources, and rely increasingly on its partners for support as it elevates its response to these dual pressures. It will have to address these challenges while it is also called upon to respond

[21] https://www.gartner.com/en/information-technology/glossary

to growing pressure to address congestion, emissions, and social equity. No easy task.

Mr. DEFAZIO. Thank you, Mr. Belcher.

Ms. Samford?

Ms. SAMFORD. Chairman DeFazio, Ranking Member Crawford, and members of the Committee on Transportation and Infrastructure, on behalf of the International Society of Automation Global Cybersecurity Alliance, the ISAGCA, and its over 50 public- and private-sector automation and cybersecurity member organizations that cross all 16 critical infrastructure sectors and comprise over $1.5 trillion in aggregate revenue, thank you for the opportunity to testify on Incident Command System for Industrial Control Systems, ICS4ICS.

My name is Megan Samford. As the Advisory Board chair of the ISAGCA, I am representing the member organizations that are all aligned around the ISA/IEC 62443 standard for cybersecurity, and that are strongly committed to securing the industrial control systems that are at the heart and lungs of American critical infrastructures.

I am also the vice president of product cybersecurity and chief product security officer for Schneider Electric's energy management business. Schneider Electric was a founding member of the ISAGCA, and is committed to ensuring the efficiency, resiliency, sustainability, and cybersecurity of electric grids, globally.

Lastly, I am cochair of the U.S. Department of Homeland Security's Control Systems Working Group.

My background in emergency management dates back to 2007, when I graduated from Virginia Commonwealth University as one of the first 50 individuals in the United States with a bachelor of arts degree in homeland security and emergency preparedness. From there, I worked under Governors Tim Kaine and Bob McDonnell, lastly serving as Virginia's critical infrastructure protection coordinator. Most recently, and what I am happy to testify on today, I became one of four cybersecurity first responders to be formally credentialed as a type 1 cyber incident commander under the FEMA National Incident Management System Incident Command System.

The private sector lacks a consistent, repeatable, and scalable framework to respond to day-to-day cyber incidents, as well as cyber incidents where the impact spans suppliers, customers, and coordination with local, State, and Federal Government. This is due to a lack of interoperability of individual company response plans. In the event of a large-scale cyber incident, this deficiency can lead to poorly executed responses that have impacts on lives and property.

The goal of ICS4ICS is to identify how the private sector can adopt portions of the FEMA Incident Command System to ensure coordinated, uniform, and more effective cyber incident response. Implementing ICS4ICS at scale will help the United States more effectively coordinate response and recovery efforts, especially for critical infrastructures.

Together with members from DHS and the National Labs, the ISAGCA and its member organizations such as Schneider Electric, Honeywell, Johnson Controls, and Mandiant have established a fully volunteer public-private partnership to deliver the ICS4ICS framework. The success of the program thus far indicates that it provides value for both the private sector, as well as Government.

In a little over a year from its standup, the program has proven that it is possible to apply the NIMS Incident Command System framework to cyber incident responses in the private sector, credential and type cyber incident response roles into a common response structure, similar to fire and emergency services, as well as create draft common response templates to speed up responses and reduce error. This is especially critical when responding to events like ransomware attacks, as was the case with Colonial Pipeline.

Poorly managed cyber incident responses can be devastating to our national security, safety, and economy. Even after 20 years, many of the same response challenges that faced emergency responders on 9/11 continue to be challenges for us now, except in cyber incident response—lack of common response frameworks and interoperability.

With so much at stake, we must effectively manage cyber incidents together, with both the private sector and Government. The Incident Command System allows us to do so. The effort is ramping up quickly and deserves a home in the United States Government. On behalf of the ICS4ICS effort, I respectfully request your bipartisan support for this important program, in requesting that the Government investigate ways to expand the spirit of language captured in Homeland Security Presidential Directive 5, which directed public-sector adoption of Incident Command System, to now encourage adoption within the private sector.

Additionally, we respectfully request that Congress make the necessary plans and investments for the private sector to become trained and credentialed in Incident Command System and, lastly, that ICS4ICS be operationalized as an official Government program residing in the U.S. Department of Homeland Security or another entity, if appropriate.

Thank you so much for your time today and your consideration. I look forward to answering any questions you all may have.

[Ms. Samford's prepared statement follows:]

Megan Samford, Vice President, Chief Product Security Officer–Energy Management, Schneider Electric, on behalf of the International Society of Automation Global Cybersecurity Alliance

Introduction

Chairman DeFazio, Ranking Member Graves, and Members of the Committee on Transportation and Infrastructure, on behalf of the International Society of Automation Global Cybersecurity Alliance—the ISAGCA—and its over 50 public- and private-sector automation and cybersecurity member organizations that cross all 16 critical infrastructure sectors and comprise over $1.5 trillion in aggregate revenue, thank you for the opportunity to testify on "Incident Command System for Industrial Control Systems" (ICS4ICS).

Abstract

The private sector lacks a consistent, repeatable, and scalable framework to respond to day to day cyber incidents as well as cyber incidents where the impact spans partners, suppliers, customers, and coordination with local, state, and federal government. In the event of a large-scale cyber incident, this deficiency can lead to poorly executed responses that have impacts on lives and property.

The goal of "Incident Command System for Industrial Control Systems," which we refer to as ICS4ICS, is to identify how the private sector can adopt portions of the National Incident Management System (NIMS) Incident Command System (ICS) to ensure coordinated, uniform and more effective cyber-incident response.[1] Implementing ICS4ICS at scale will help the United States more effectively coordinate cyber incident response and recovery efforts within the private sector, especially for critical infrastructures.

Together with the United States Department of Homeland Security Cyber and Infrastructure Security Agency (CISA), the ISAGCA and its member organizations such as Schneider Electric, Rockwell Automation, Johnson Controls International, Honeywell, Ford Motor Company, Pfizer, Exelon, Mandiant, Dragos, ClarOTy, Nozomi, and Idaho National Labs, have established a public-private partnership to deliver the ICS4ICS cyber-incident response framework.[2]

The success of the program thus far indicates that it provides value for both the private sector as well as government. This is evidenced by the number of daily, active volunteers, contributed by both the private sector and government. In a little over a year from its creation, the program has proven that it is possible to apply the NIMS Incident Command System framework to cyber-incident responses in the private sector, credential and type cyber-incident response roles into a common response structure (similar to fire and emergency services), as well as create draft common response templates to speed up responses and reduce error. This is all being done on volunteer time because the membership of this understands how badly the lack of scalability in cyber-incident response is hurting industries both in the United States, as well as globally.

While we are pleased with the rate at which the program is growing through the ISAGCA, we recognize that to make it adoptable at scale, we need the bi-partisan support of this Congress in developing a path for the program to be transitioned to operations within the United States government.

My name is Megan Samford.

As the Advisory Board Chair of the ISA Global Cybersecurity Alliance, I am representing the member organizations that are strongly committed to securing the industrial control systems that are the heart and lungs of not only American but global critical infrastructures. As a global organization, members of the ISAGCA are all aligned around the ISA/IEC 62443 standard for cybersecurity for industrial automation. I am also the Vice President of Product Cybersecurity and Chief Product Security Officer for Schneider Electric's Energy Management business. Schneider Electric was a founding member of the ISAGCA and is committed to ensuring the efficiency, resiliency, sustainability, and cybersecurity of electric grids globally. Lastly, I am Co-Chair of the US Department of Homeland Security's Control Systems Working Group within the Cybersecurity and Infrastructure Security Agency (CISA).

My background in emergency and incident management dates back to 2007, when I graduated from Virginia Commonwealth University as one of the first 50 individuals in the United States with a Bachelor of Art's degree in Homeland Security and Emergency Preparedness. From there, I worked under Governors Tim Kaine and Bob McDonnell, lastly serving as Virginia's Critical Infrastructure Protection (CIP) Coordinator. During this time, I had great exposure to traditional physical security and emergency management principles, to include the NIMS Incident Command System, which I will refer to as "ICS" moving forward. I saw firsthand by working in the Virginia Emergency Operations Center (VEOC) that ICS was a great way to efficiently coordinate responses and I began to adapt much of the work I was doing in Critical Infrastructure Protection planning to model ICS principles. My first attempt at more closely integrating private sector response capabilities was in an article I published in 2014 titled, "Framework for the Integration of Emergency Support Function, Infrastructure Protection and Supply Chain Management Efforts" which aimed to describe how the private sector could "hook into" local, state, and federal disaster response efforts through integration with state level Emergency Operation

[1] *IS–100.C: Introduction to the incident command system, ICS 100*. Federal Emergency Management Agency / Emergency Management Institute. (n.d.). Retrieved October 28, 2021, from https://training.fema.gov/is/courseoverview.aspx?code=is-100.c.

[2] Greig, J. (2021, July 13). *Cybersecurity organizations announce New First Responder Credentialing program*. ZDNet. Retrieved November 1, 2021, from https://www.zdnet.com/article/cybersecurity-organizations-announce-new-first-responder-credentialing-program/.

Center Emergency Support Functions (ESFs).[3] As such, the effectiveness and efficiency of coordinated responses between the private and public sectors has been a focus area of my work for nearly the past decade.

Because of my background in critical infrastructure protection and focus on government and private sector collaboration, I was recruited into the private sector to help companies build and implement product cybersecurity programs, of which response has always been a strong element. I've had roles at both the tactical and strategic levels of program design and implementation, I've worked for the top manufacturers of Industrial Control Systems products and systems, and now I'm working on my third product security program, at Schneider Electric's Energy Management Business.

Most recently, and what I am happy to testify on today, I became one of four cybersecurity first responders to be formally credentialed under the United States National Incident Management System Incident Command System as a Type I Cyber Incident Commander. This role plays a critical function in leading and directing cyber-incident responses as well as ensuring proper span and control, and resourcing. I am one of only four the United States has, and one of only two within the private sector: The other two are within the United States Army Reserves Innovation Command the United States Department of Homeland Security, respectively.

- *Mark Bristow*, Branch Chief, United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)
- *Colonel Brian Wisniewski*, US Army Reserves Innovation Command G2/G6
- *Neal Gay*, Senior Manager, Managed Defense, Mandiant
- *Megan Samford*, Vice President, Product Cybersecurity, Schneider Electric

Today, I hope to tell you what the ICS4ICS program is, why the United States government and private sector needs it, and why this effort needs a home in the United States government to scale.

WHAT IS ICS4ICS?

ICS is a standardized, repeatable, and scalable approach to managing both day-to-day and complex incidents. It was created here in the United States during the 1970s as a result of the California Wildfire responses, where multiple fire departments and state and federal agencies had come together to respond in a unified and coordinated way.[4] ICS has been tested in more than 40 years of emergency and non-emergency applications by all levels of government and in the private sector. At its foundation, ICS recognizes a need for different organizations to work together toward common goals.

ICS addresses:

- Nonstandard terminology among responding entities
- Lack of capability to expand and contract as required
- Lack of an orderly, systemic planning processes
- Nonstandard & nonintegrated communications
- Lack of personnel accountability, including unclear chains of command and supervision
- No common, flexible, predesigned management structure that enables commanders to delegate responsibilities and manage workloads efficiently

In preparing for this testimony, I found the below expert from the United States Department of Agriculture Incident Command System 101 Course material to be very helpful in plainly explaining what Incident Command System is.

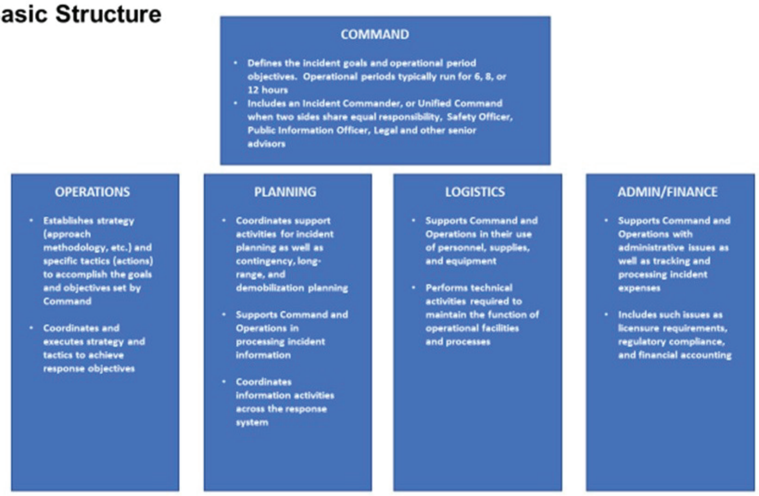
> "The Incident Command System or ICS is a standardized, on-scene, all-risk incident management concept. ICS allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents without being hindered by jurisdictional boundaries. ICS has considerable internal flexibility. It can grow or shrink to meet different needs. This flexibility makes it a very cost effective and efficient management approach for both large and small incidents. Designers of the system recognized early that ICS must be interdisciplinary and organizationally flexible to meet the following management challenges:
>
> - Meet the needs of incidents of any kind or size
> - Be useable or repeatable for routine or planned events such as conferences, as well as large and complex emergency incidents

[3] Samford, M. (2014). Framework for the Integration of Emergency Support Function, Infrastructure Protection and Supply Chain Management Efforts. Homeland Security Today.

[4] *ICS 100—Incident Command System—USDA*. (n.d.). Retrieved October 28, 2021, from https://www.usda.gov/sites/default/files/documents/ICS100.pdf.

- Allow personnel from a variety of agencies to meld rapidly into a common management structure
- Provide logistical and administrative support to ensure that operational staff, such as Forensic investigators and malware reverse engineers, can meet tactical objectives
- Be cost effective by avoiding duplication of efforts”[4]

ICS Basic Structure



COMMAND

- Defines the incident goals and operational period objectives. Operational periods typically run for 6, 8, or 12 hours
- Includes an Incident Commander, or Unified Command when two sides share equal responsibility, Safety Officer, Public Information Officer, Legal and other senior advisors

OPERATIONS

- Establishes strategy (approach methodology, etc.) and specific tactics (actions) to accomplish the goals and objectives set by Command
- Coordinates and executes strategy and tactics to achieve response objectives

PLANNING

- Coordinates support activities for incident planning as well as contingency, long-range, and demobilization planning
- Supports Command and Operations in processing incident information
- Coordinates information activities across the response system

LOGISTICS

- Supports Command and Operations in their use of personnel, supplies, and equipment
- Performs technical activities required to maintain the function of operational facilities and processes

ADMIN/FINANCE

- Supports Command and Operations with administrative issues as well as tracking and processing incident expenses
- Includes such issues as licensure requirements, regulatory compliance, and financial accounting

The above chart explains the five basic management functions within ICS: Command, Operations, Planning, Logistics, and Admin/Finance. As incidents expand, additional sub structures can be broken out to support scaling incidents. The functions apply in both small- and large-scale incidents.

A key principle within the application of the management functions is span of control. No one leader can have more than seven people directly reporting to them to ensure span of control. This helps to ensure accountability and reduce confusion during responses.[4] Of note, is that as incidents contract, the organization can scale down accordingly, until only a few responders remain to support the incident.[4]

Since its early adoption in the 1970s, to its full adoption across the public sector today through the Federal Emergency Management Agency (FEMA), the Incident Command System has saved thousands of lives, businesses, and property; has been endorsed by the United Nations; and now, the most developed countries in the world follow this system for emergency management.[5] Every local fire, EMS, state agency, and federal response entities in the US follow and know ICS by heart—it’s simply how we respond.

Additionally, many private sector organizations now use ICS to run day-to-day operations, planned events, as well as responses because of its proven effectiveness in safety critical environments. This is particularly common within electric utility companies. ICS has been a gift to the world and the United States should be proud of this proven response framework.

The Private Sector Cyber-Incident Response Problem—Scaling & Interoperability

Having worked in product security programs for nearly a decade, I speak from experience when I say that while individual companies may have a cyber response plan, or “playbook” as they are commonly referred, that is robust and effective, these plans often suffer during larger crisis because of a lack of coordination capac-

[5] Millner, G. C., & Murta, T. L. (n.d.). *Incident management*. Incident Management—an overview / ScienceDirect Topics. Retrieved October 28, 2021, from https://www.sciencedirect.com/topics/nursing-and-health-professions/incident-management.

ity that can scale outside of their organization, and their control.[6] Each plan is unique to the organization and defines who does what within the organization, notification procedures, technical team capabilities, interaction with legal and communications, and regulatory requirements—the playbooks are comprehensive, but written on a company-by-company basis and lack interoperability. Existing cybersecurity standards do not specifically address a larger response framework concept like ICS.

The breakdown with this planning approach occurs when the response is larger than one organization. The individual plans cannot scale effectively into a collaborative response when multiple companies, jurisdictions, and government entities need to be brought to bear for a large-scale attack scenario. The Solar Winds supply chain attack highlights the trend that cross-company, cross-sector, multiple party responses are on the rise. Currently, there is no repeatable and consistent framework to support cyber-incident response interoperability among the stakeholders.

What Are the Larger Impacts of not Having a Common Framework?

The larger impacts for both the private sector and the government of not having a common framework are that disasters can become catastrophes when the responses cannot be contained. The consequences of not having a structure like ICS4ICS can lead to inefficient and costly responses, both for life and property due to a lack of a common response framework.

From my observations, for the private sector:

- There lies an inability for responses to scale outside of one or two organizations. No larger structure exists for the private sector to share resources through mutual aid agreements.
- There is no standard terminology, "common language", or common response templates. Common language and templates help to speed up responses and lessen confusion. Lack of communications interoperability was cited in the Implementing Recommendations of the 9/11 Commission Act of 2007.[7]
- There are no "typed" cyber-incident responder roles. Typing is a way of characterizing roles so that they are shared across a function. Example: A Type 1 Incident Management Team in Virginia has essentially the same training and experience as a Type 1 Incident Management Team in California. This creates baseline capability and understanding and is a foundational premise of Incident Command System.
- The private sector playbooks are based on traditional enterprise information technology and are focused on tactical actions needed to mitigate harm to the organization, gather evidence, and determine what internal and external escalations/notifications are needed.
- Time and resources are not well tracked or managed resulting in response fatigue, and hindered decision making over extended operational periods. Surge capacity is rarely available to provide relief, which also compounds response fatigue.

From my observations, what this in turn means for the government is:

- Out of the many defined natural and man-made disaster types, cyber is the only disaster type that currently does not follow Incident Command System.
- If 85% of critical infrastructures are owned and operated within the private sector, the US government lacks a way to effectively coordinate under a common structure with a large percentage of its cyber response resources.
- There is a lack of understanding of the degree of cyber expertise and capability the private sector could bring to bear.

If you take the example of the Colonial Pipeline ransomware attack, the asset owner and operator had detected ransomware on the enterprise network and made the decision to safely shut down pipeline operations to prevent the potential spread of the ransomware into that safety critical environment. For all intents and purposes, this was a responsible decision given the information available to decision makers at that time. What we see in this scenario is that the major impacts of the attack occurred not from the inherent ransomware attack, but from the cascading impacts of proactively shutting down the pipeline. Again, "disasters become catastrophes when responses cannot be contained".

While shutting down pipeline operations was the appropriate and safe decision, the cascading impacts of that decision meant the response became less centralized

[6] Singh, A. *What are cyber incident response playbooks & why do you need them?* APMG International. Retrieved October 28, 2021, from https://apmg-international.com/article/what-are-cyber-incident-response-playbooks-why-do-you-need-them.

[7] *Implementing recommendations of the 9/11 ...-congress.gov*. (n.d.). Retrieved October 28, 2021, from https://www.congress.gov/110/plaws/publ53/PLAW-110publ53.pdf.

because other impacted organizations, such as the United States Department of Homeland Security, were brought in to support the response. While I was not personally involved in the response and remediation efforts, it can be inferred from the aftermath that a unified public and private coordination structure could have resulted in increased public confidence over the response. The lack of public confidence and trust contributed to reactionary demand for gas, resulting in shortages.

While the Colonial Pipeline example demonstrates how large responses can scale, even for mature and well-resourced organizations, in many cases, smaller organizations face even larger resource constraints. A system like ICS4ICS can help companies provide mutual aid to one another. This is not unlike how electric utility companies share lineman during power restoration efforts following hurricanes. You frequently see lineman from Dominion Energy based in Virginia support hurricane recovery efforts in Florida. As such, the electric utilities are also investigating the use of ICS4ICS: Sharing resources is a well understood concept for that industry.

THE IDEA OF ICS4ICS

Given these critical gaps and my past experience as an emergency manager, I had the idea to apply the NIMS Incident Command System framework and train cyber-incident responders in the same way we train every other first responder in the United States. I put pen to paper and drafted a cyber-incident coordination framework that could be applied to cyber-incident responses based on Incident Command System.

After I introduced the ICS4ICS idea at one of the largest Industrial Control Systems Cybersecurity conference in the world, the ISAGCA agreed to pick up the effort and it has grown: We now have training programs on ICS4ICS, have updated response templates, and we are educating cybersecurity experts on the framework.

APPROACH OF ICS4ICS IN DELIVERING CYBER RESPONSE CAPABILITY TO THE PRIVATE SECTOR

Through ICS4ICS we are encouraging member organizations to start adoption by overlaying this organizational structure over their current response playbooks. We are not suggesting that ICS4ICS become a replacement for existing response playbooks; instead, the Incident Command System should be applied as a higher-level way of structuring command and control as well as management of resources. The typing of resources is also significant as it enforces common terminology and expectations for each typed role.

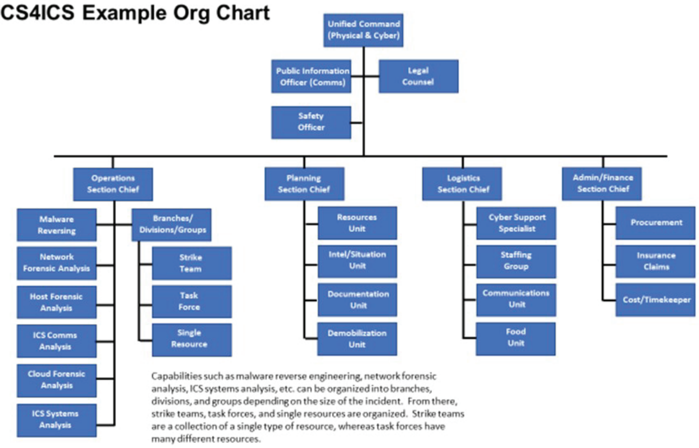
Currently ICS4ICS has over 350 cyber volunteers registered to become credentialed—most within the United States but there has been increasing interest from cyber security experts in Europe, Canada, Latin America, Asia, Australia, and New Zealand. These international groups will likely stand up their own local implementation and credentialing processes. To become credentialed, a cyber-incident responder must:

- Submit an application to ICS4ICS
- Create an account through FEMA's One Responder system
- Complete 18 hours of online FEMA ICS training (the courses may be able to be shortened at a later date)
- Complete the Position Task Book application clearly demonstrating where the applicant has obtained experience working cyber-incidents (a third-party verification is required to be filled out by a former supervisor or person in an authority role for the described cyber-incident)

Once the application is completed, the applicant will receive notice of the opportunity to appear before the ICS4ICS adjudication committee (includes a representative from DHS CISA) to discuss their application and answer any questions the adjudication committee may have. Once approved, the credential is assigned and documented within the FEMA One Responder portal.

Below is an example template that can be used by the private sector when organizing a response in an Operational Technology (OT) environment:

ICS4ICS Example Org Chart



Capabilities such as malware reverse engineering, network forensic analysis, ICS systems analysis, etc. can be organized into branches, divisions, and groups depending on the size of the incident. From there, strike teams, task forces, and single resources are organized. Strike teams are a collection of a single type of resource, whereas task forces have many different resources.

The next phase of the program will include continued creation of response plan templates, hazard specific annexes to support events like ransomware, Incident Action Plan templates, and needed credentialing. DHS will also need to decide if private sector companies with trained cyber-incident responders should integrate into the current NIMS, state multi-agency coordination center (MACC) model, or if a centralized office should be created within DHS.

Closing

Poorly managed cyber-incident responses can be devastating to our national security, health and safety, and economy. Even after twenty years, many of the same response challenges that faced emergency responders on 9/11 continue to be challenges for us now, except in cyber-incident response—lack of common response frameworks and interoperability. With so much at stake, we must effectively manage cyber-incidents, together, with both the private sector and government. The Incident Command System allows us to do so.[4]

This effort is ramping up quickly and deserves a home in the United States government. On behalf of the ICS4ICS effort, I respectfully request your bi-partisan support for this important program in requesting the government investigate ways to expand and enhance the spirit of language captured in Homeland Security Presidential Directive-5 to encourage adoption of Incident Command System within the private sector for cyber-incident response:

> “The Federal Government recognizes the role that the private and nongovernmental sectors play in preventing, preparing for, responding to, and recovering from terrorist attacks, major disasters, and other emergencies. The Secretary will coordinate with the private and nongovernmental sectors to ensure adequate planning, equipment, training, and exercise activities and to promote partnerships to address incident management capabilities.”[8]

Additionally, we respectfully request that Congress make the necessary plans and investments for the private sector to become trained and credentialed in Incident Command System in the same way that fire and emergency services are trained today, and lastly, ICS4ICS be operationalized as an official government program, residing in the United States Department of Homeland Security, or another entity, if appropriate.

Mr. DeFazio. Thank you, Ms. Samford.

Mr. Farmer?

Mr. Farmer. Thank you, sir.

[8] *Homeland Security Presidential Directive 5*. (n.d.). Retrieved October 28, 2021, from https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf.

Mr. DEFAZIO. You are recognized for 5 minutes.

Mr. FARMER. Thank you, sir. Chairman DeFazio, Ranking Member Crawford, members of the committee, thank you all for the opportunity to address such an important subject on behalf of America's railroads.

Across the industry, railroads and the organizations that support them take their role as critical infrastructure underpinning the U.S. economy very seriously. In all efforts, the commitment to safety is paramount. This commitment applies with equal strength to our comprehensive and collaborative effort in cybersecurity.

The key point we hope you take away today is this: railroads have a proven and longstanding commitment to collaboration within our industry, across sectors, and with Government to protect against cyberattacks. The underlying premise is that prevention is attainable with the right structures supporting the right people armed with timely and actionable cyber threat intelligence and security information. We can prevent attacks and mitigate their effects, should they occur.

The right people with the experience—cybersecurity professionals and railroads, deeply familiar with their networks and operations, who bring expertise and judgment to bear in planning, protective measures, and collaborative efforts. They ensure those fundamental measures outlined by the chairman earlier are taken consistently and effectively.

Serving as a focal point for the industry's unified effort is the Rail Information Security Committee, the right structure formed by major freight, railroads, and Amtrak more than two decades ago. Comprised of chief information security officers and cybersecurity leads for railroads and industry organizations, the committee focuses continuously on addressing cyber threats, incidents, and significant security concerns.

What are we seeing?

Sharing effective practices and protective measures, what we are doing about it.

Coordinated cyber incident response planning, how we work together, effectively.

Benchmarking cybersecurity posture against the NIST cybersecurity framework, continuous attention to how we can get better.

Working with key industry suppliers in a dedicated joint coordination and information-sharing group, how we strive to detect and act upon vulnerabilities and concerns before they can be exploited.

And engaging proactively with Government departments and agencies of the United States and Canada, how we support informed vigilance and effective action across sectors.

The industry, as a whole, benefits from the expertise and shared experience, accomplishments, and priorities of network protection for safety and operational resilience.

In support of this vital work, a top priority for our industry is maximizing effectiveness through information sharing. Reports by railroads and industry organizations is a linchpin for this effort. These reports are made to the Railway Alert Network, which works with the reporting railroad to produce a cybersecurity advisory on the activity of concern, describing how it manifested, what the indicators are, and what measures should be taken to narrow risk profile. Through this network we disseminate these advisories widely, among freight and passenger railroads in the United States and Canada, and to hundreds of recipients and fellow Government organizations, including CISA, TSA, the FBI, DOT, the Department of Defense commands, and Transport Canada.

Further, meeting a commitment we made at the inaugural Transportation Sector Cybersecurity Tabletop Exercise held by TSA in August 2015, we shared with the advisors and representatives of each of the transportation modes and other critical infrastructure sectors, and we have done so consistently for more than 6 years now.

Unfortunately, what we have not seen is consistency in analyses of the reports we have submitted to Government organizations. And we believe these efforts can and should be enhanced, and are committed to working with Government for this purpose.

The overall aim remains consistent: get the right information through the right structures to the right people to make a difference. Government action should foster these proven collaborative efforts in order to expand them and enhance them, not override or disrupt them.

The President specifically urged this caliber of collaborative effort in his National Security Memorandum on Improving Cybersecurity, issued in late July of this year. The railroad industry supports the President's approach and desired outcomes. We sought to attain them in a third proposal submitted to TSA in mid-August on enhancing cybersecurity posture across the transportation sector.

However, in early October, the Secretary of Homeland Security announced that TSA will issue security directives to mandate cybersecurity actions by railroads and rail transit agencies. These mandates are not only unnecessary, but also could prove counterproductive, disrupting well-established and proven practices. Railroads are meeting the main mandates the planned directives will impose, but the prescriptive elements for each raise serious concerns that what we have done so well and for so long, in partnership with Government, will be undermined. We must avoid a command-and-control approach, and instead build upon an impressive track record of collaboration.

My written statement to the committee outlines considerations for legislative action on cybersecurity, on which I am happy to address questions this morning. But two points merit emphasis here.

First, Congress has already acted effectively through the Cybersecurity Information Sharing Act of 2015. This statute is vastly underutilized by security agencies and Government. It should not be, for it expressly authorizes sharing of cyber threat intelligence and related security information within industries, across sectors, and between industry and Government. It also provides essential protections that build and alleviate impediments to the flow of timely and actionable information. Had this statute been effectively implemented, it would not be even a perceived need for new legislation or security directives on cyber incident reporting.

And second, the gap in analysis of reporting of significant cybersecurity concerns should be resolved, closed, by expanding the analytical capabilities of systems workforce before any more mandates requiring more reporting are made. CISA Director Jen Easterly testified earlier this week, emphasizing her view that her agency's most effective role is in support and collaboration for sustained enhancements across sectors of cybersecurity posture. Legislation should enable accomplishment of this admirable purpose.

In closing, we are proud that we have been proactive, effective, and collaborative for so long in this challenging arena. Policymakers here and executive agencies play an important role alongside private enterprise. Creating nimble and effective—without concerns for liability or enforcement action and financial penalties for business is vital.

As Congress considers new measures, please look to build upon the collaborative approach that has largely succeeded to date. Thank you, and I am very happy to address any questions you may have this morning.

[Mr. Farmer's prepared statement follows:]

Thomas L. Farmer, Assistant Vice President–Security, Association of American Railroads

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to offer this testimony. AAR's freight railroad members account for the vast majority of North American freight railroad mileage, employees, and traffic. Passenger railroad members include Amtrak and several major commuter carriers as well.

Railroads are indispensable to our nation. They connect producers and consumers of goods across the country and the world, expanding existing markets and opening new ones. Whenever Americans grow something, mine something, or make something; when they send goods overseas or import them from abroad; when they eat their meals or take a drive in the country, there's an excellent chance freight railroads helped make it possible. Passenger railroads enhance mobility and connectivity, alleviate highway and airport congestion, reduce pollution, promote local and regional economic development, and improve transportation safety.

Unified Commitment to Security Preparedness, and Continuous Improvement

Railroads and rail industry organizations address both cyber and physical security through unified efforts under a longstanding comprehensive security plan. Applying a risk-based and intelligence-driven approach to rail security, this plan has four alert levels that call for increasingly stringent security measures.

Responsibility for managing the security plan and assuring its sustained effectiveness to meet evolving threats is vested in two dedicated industry coordinating committees: the Rail Security Working Committee, which is comprised of senior law enforcement and security officials focused on domestic and international terrorism; and the Rail Information Security Committee (RISC), which consists of the chief information security officers and information assurance officials of major North American railroads, with support from security experts at AAR and the American Short Line and Regional Railroad Association (ASLRRA). The rail industry, through RISC, has maintained a dedicated and effective coordinating forum for cybersecurity protection and risk mitigation for more than two decades. Together, the two committees constitute the Rail Sector Coordinating Council (RSCC), which serves as the rail industry's main channel of communication and coordination with government agencies on cyber and physical security and preparedness.

Because of the devoted work of these committees, the rail industry's security plan does not just sit on a shelf, occasionally taken down and dusted off. Rather, it is a living document, evaluated and enhanced continuously through recurring exercises, integration of effective practices, and frequent consultations with government and private-sector security experts to ensure maximum sustained effectiveness in the face of evolving security threats. Early in 2020, the two industry committees completed the most substantial review and update of the plan since its inception some 20 years ago. This update highlighted the substantial progress the industry has made in terms of capabilities, monitoring and analysis of threats, coordination with government agencies, electronic reporting, and joint decision-making on alert levels, measures, and actions.

RAILROADS ADDRESS CYBERSECURITY HEAD ON

Railroads of all kinds rely on advanced software and information technology in every aspect of their operations. These technologies run the gamut from advanced train dispatching software to smart sensors along tracks that identify equipment in need of repairs, and from real-time shipment tracking tools to sophisticated train control technology.

Railroads recognize their critical importance to our nation, as well as the risks associated with their extensive reliance on information technology, which is why they are continuously on guard against cyberattacks and working diligently to enhance their capabilities to guard against them. Railroads' cybersecurity efforts are comprehensive, multi-faceted, and supported by specialized, highly skilled cybersecurity staff.

A recent report by the Congressional Research Service rightly concludes, "Cybersecurity is a risk management process rather than an end-state. It involves continuous work to (1) identify and (2) protect against potential cybersecurity incidents; and to (3) detect; (4) respond to; and (5) recover from actual cybersecurity incidents." Entities "may choose to evaluate their information technology (IT) risks by understanding the threats they are susceptible to, the vulnerabilities they have, and the consequences a successful attack might have for their mission and their customers."[1] The rail industry consistently focuses on these priorities through unified, multifaceted, and proactive cybersecurity efforts.

RAIL INDUSTRY CYBERSECURITY EFFORTS SPAN TWO DECADES

For railroads, cyber awareness is a fundamental component of their day-to-day operations, but even the best cybersecurity plans and practices will falter if useful information on cyber threats is not shared. Information sharing allows organizations to learn from one another, reduce their vulnerabilities, and quickly adapt to changing conditions. For this reason, railroads and industry organizations prioritize proactive engagement with government partners to share information on cyber threats and effective countermeasures. Insights gained from risk assessments and threat advisories, along with experience gained in drills, enable railroads and industry organizations to incorporate effective safeguards and protective measures into their own systems.

The rail industry focuses on analyzing four categories of protective measures: the tactics most commonly employed to gain illicit access to computer systems; vulnerabilities most commonly exploited; indicators of illicit activities most often noted in post-incident analyses that were missed or disregarded; and protective measures that could have made a difference if they had been implemented. We use these four categories based on experience best demonstrated by the Australian Cyber Emergency Response Team (CERT), which found that the vast majority of the cyberattacks against private entities in which CERT provided aid would not have been successful if the targeted entity had paid sufficient attention to these four protective measures.

Further steps that the rail industry has taken to enhance timely information sharing, in coordination with partners at DHS, FBI, TSA, and DOT, include:

- Deploying secure telephone equipment to connect major railroads, the AAR, and government officials.
- Sharing classified information with authorized Canadian railroad officials who hold security clearances issued by the government of Canada.
- Establishing a classified information sharing network with TSA, which enables authorized rail industry personnel to review relevant materials in dozens of metropolitan areas nationwide.
- Participating in a multi-industry initiative with DHS to establish a secure video teleconference network that simultaneously links more than 40 U.S. metropolitan areas.

As a result of these cooperative efforts between industry and government, what had often required weeks, or even months, of effort can often now be accomplished in hours. This progress greatly enhances the ability of those in the private and public sector to identify and effectively respond to cyberthreats in a collaborative manner.

[1] Congressional Research Service, "Federal Cybersecurity: Background and Issues for Congress," September 29, 2021. Available at https://crsreports.congress.gov/product/pdf/R/R46926.

The President Urges Government-Industry Collaboration on Cybersecurity

The rail industry supports the President's emphasis on government-industry collaboration to enhance cybersecurity as laid out in the National Security Memorandum on *Improving Cybersecurity for Critical Infrastructure Control Systems*, issued on July 28, 2021.

In response to the memorandum, the rail industry developed a detailed proposal on how government and industry can work collaboratively to elevate cybersecurity posture in all transportation modes. We submitted this to TSA just three weeks after the memorandum was issued and more than a month before TSA's initial outreach to stakeholders regarding Security Directives to mandate cybersecurity measures by railroads and rail transit agencies.

Work on this initiative began over two months earlier in the wake of the Colonial Pipeline cyberattack. In early June 2021, AAR's security lead joined his colleague at the American Public Transportation Association (APTA) to propose a "strategic concept" for enhancing cybersecurity in the transportation sector. Over the next couple of months, the rail industry took the lead in drafting this strategic concept.

Submitted in mid-August, the industry proposal delineates 13 areas of emphasis that outline actions for transportation organizations and federal government organizations to take to implement TSA's Cybersecurity Roadmap. TSA Administrator David Pekoske has frequently cited the Roadmap as defining "clear pathways" for enhancing cybersecurity posture and mitigating cyber risk in the transportation sector. Additionally, the rail industry's August proposal covers recommend conduct of cybersecurity self-assessments, something on which TSA plans to issue a non-compulsory information circular.

Unfortunately, although the rail industry's strategic concept proposal was submitted in August and meets the President's repeated emphasis on collaboration to enhance critical infrastructure cybersecurity, we have received no official response.

TSA Security Directives Are Unnecessary

As members of this committee know, in public remarks about a month ago, Secretary of Homeland Security Alejandro Mayorkas announced that TSA will issue Security Directives laying out cybersecurity actions and measures that must be implemented by "higher-risk railroad and rail transit entities." In making this announcement, Secretary Mayorkas said, "There is no better example of how the cybersecurity threat can impact our lives than in the transportation sector and how people commute, see one another, engage with one another."

Railroads and industry organizations certainly agree that the cybersecurity threat merits priority attention—as demonstrated by the rail industry's rigorous attention to this issue for more than 20 years. Significantly, each of the actions the Secretary said will be covered by TSA security directives for railroads and rail transit agencies is already covered by the rail industry's August 2021 proposal noted above. Put another way, railroads are already doing what they should be doing in terms of cybersecurity.

Moreover, issuing a Security Directive is an exercise of emergency authority by the TSA Administrator that allows imposition of requirements "immediately in order to protect transportation security."[2] Railroads and rail industry organizations have not been advised by federal officials of any prevailing emergency conditions that justify use of this authority, despite the many opportunities available. TSA officials have indicated that work to produce and provide a current cyber threat briefing is ongoing, but to our knowledge no briefing has been proposed or scheduled for this purpose.

In addition, the Security Directives could undermine the 20-year effort of the industry to develop and share cybersecurity information among railroads and government agencies, as explained above. If reports are required to be made to government and are deemed security-sensitive information, then private industry stakeholders may be reluctant to share the information through our established network. This outcome will ultimately have a deleterious effect on the security of the industry and the purported goal of these proposed Security Directives.

Lastly, the announcement of the Security Directives has produced erroneous perceptions that railroads, and rail transit agencies, have not been rigorously and effectively engaged for many years in defending against cyber threats. This false impression could have negative ripple effects if rail customers and the communities in which railroads operate lose confidence in railroads' ability to operate safely and securely.

[2] 49 U.S.C. § 114(l).

Railroads' cybersecurity efforts are far more likely to be effective if they involve continued collaborative efforts with government than if they are mandated through top-down security directives or rulemakings. To that end, our concerns are as follows:

- The requirement that the appointed primary and alternate cybersecurity coordinators be U.S. citizens will make compliance by two major Canadian railroads (CN and Canadian Pacific) that also have substantial U.S. operations extremely difficult. Given that TSA and the rail industry have long successfully shared classified information with Canadian nationals who hold security clearances issued by the government of Canada, this prescriptive measure is unwarranted.
- The mandate to report a "cybersecurity incident" is overly broad and, if left unchanged, will result in high volumes of reports on matters that are not significant from a cybersecurity perspective. The directive should focus instead on "significant" cybersecurity incidents so that developing threats and effective preventive measures can be more readily identified.
- The inflexibility of an overriding government mandate of risk-based determinations on preparedness and response planning, protective measures, and implementing capabilities.

WHAT FUTURE CYBERSECURITY LEGISLATION SHOULD INCLUDE

As noted above, information sharing is crucial to the success of all cybersecurity plans. The Cybersecurity Information Sharing Act of 2015 (CISA 2015) expressly authorized sharing of cyber threat intelligence and related security information and created a framework of protection to facilitate and encourage such exchanges within industries, across critical infrastructure sectors, and with federal government entities. Unfortunately, many of the authorizations and protections Congress established in CISA 2015 have either been inconsistently utilized or left unimplemented.

Policymakers should build upon the collaborative approach described in this testimony and that has worked effectively for years, rather than implementing mandates that would needlessly disrupt existing organizational structures and practices that prove their value daily. In this regard, freight railroads respectfully suggest that the following elements should be included in future cybersecurity legislation:

1. *Include the reasonable protections provided in CISA 2015.*

- Antitrust exemptions, civil liability protections, and other protections (Division N–CISA 2015; Secs. 104(e), 105(d));
- Disclosure law exemptions, such as freedom of information statutes, open meetings laws, or similar enactments requiring the disclosure of information or records at the state, federal, and tribal or territorial levels (Division N–CISA 2015; Sec. 104(d)(4)(B)(ii)); and
- Certain regulatory use exemptions, which prevent any federal, state, tribal, or territorial government from bringing an enforcement action based on the sharing, but not the development or implementation, of a regulation (Division N–CISA 2015; Sec. 104(d)(4)(C)(ii)).

Together, these provisions provide reporting entities with the protections and confidence needed to sustain the unencumbered flow of cybersecurity information with government authorities. Including these protections in all future cybersecurity legislation will build upon the successful partnerships CISA 2015 has formed.

2. *Expand the analytical capabilities of the Cybersecurity and Infrastructure Security Agency's (CISA) workforce.*

Private sector entities, including railroads, already report significant cybersecurity incidents and security concerns to CISA and other federal government agencies. A persistent challenge, raised often by private sector entities with federal partners, is the lack of analysis of the reports by the government. Given the breadth of the reporting mandate in the planned Security Directives for railroads and rail transit agencies, the volume of reporting to CISA will increase substantially. CISA must have the capacity to review, evaluate, and analyze reports received from railroads and rail transit agencies. Feedback should focus on why the reported activity matters to those transportation organizations and what can be pragmatically done in order to narrow future susceptibility. The lack of this focused analysis and feedback to transportation sector entities indicates that CISA may lack staffing and resources to meet this need.

3. *Direct CISA to regularly update a cyber threat profile based on analyses of attacks, failed attempts, and successful disruptions.*

This profile should focus on the following parameters:

- Tactics most commonly used to perpetrate breaches;

- Vulnerabilities most frequently targeted and exploited;
- Protective measures most often found lacking or inadequately implemented that could have prevented incidents; and
- Indicators of developing threats that are often missed or misunderstood.

The aim is to build understanding of how prevailing cyber threats materialize and the measures most effective to prevent them or seriously mitigate their adverse effects. The profile should undergo constant review to enable updates on a quarterly basis. Organizations across sectors and industries would contribute to the development of this profile through reporting on significant cyber threats, incidents, and indicators of concern and on measures or actions taken for risk mitigation.

4. Direct CISA and Sector Risk Management Agencies (SRMAs) to work with private entities to establish early notification networks.

The importance of cyber-attack analyses rests in what they yield, which are discernible indicators that assist in identifying the illicit activity that took place. Consistency in identifying and sharing these indicators in a timely and efficient manner is crucial to prevent and mitigate future attacks. Early notification networks provide an effective means for proactive, streamlined, and continuous sharing by governmental and private entities of these types of indicators based on trust and shared interests.

5. Define and publicize procedures for stakeholders to submit requests for information (RFIs) and requests for assistance (RFAs) to enhance cooperative cybersecurity efforts.

As part of cyber preparedness plans, as well as in the wake of a cyber-attack that affects a particular entity or industries, organizations across sectors use RFIs and RFAs to gain insights based on federal analyses of cyber threats and risk mitigation measures. Timely responses can make prevention attainable. Unfortunately, CISA, Sector Risk Management Agencies (SRMAs), and other federal components lack consistency regarding submission, review and consideration, and responses to RFIs, RFAs, and proposals for action to enhance cybersecurity. Ad hoc processes are applied. These can vary substantially with the type of incident, the information or action sought, and the federal government organization that takes responsibility for acting on the request or proposal. The result is a lack of response or an action that fails to meet the stated needs or reasonable expectations.

6. Direct CISA to establish consistent standards for software bills of materials (SBOM) from vendors and suppliers

A recurring theme in the evaluation by CISA of cyber-attack campaigns over the past year is the exploitation of vulnerabilities in software that end users could not detect. To redress this gap in cybersecurity awareness, CISA has repeatedly urged end users to ask their suppliers to provide a software bill of materials that provides an inventory list of all open source/third-party components present in the source code used to build a particular software system, application, or software or component. Legislation should transition CISA's recommended measure and define consistent and effective practices for vendors and suppliers of information technology. Proven supported equipment, devices, and components need to produce sturdy software bills of materials and make them available or accessible to their buyers and end users.

The railroad industry, TSA, and CISA share a common purpose: ensuring that effective and sustainable measures are in place, and regularly reviewed for continuous improvement, to mitigate risk in the face of evolving cyber threats. Railroads have a proven track record of cooperative engagement with federal agencies, and we firmly believe that collaborative effort is the best way to achieve this aim. We should be afforded the opportunity to do what the President so rightly urges in his National Security Memorandum.

Thank you again for the opportunity to present this testimony. When it comes to cybersecurity, railroads have been proactive, effective, and collaborative for many years. They will continue to work cooperatively with private and public entities to ensure that our nation's rail network and the people, firms, and communities it serves, remain protected.

Mr. DeFazio. OK, thank you, Mr. Farmer.

Mr. Stephens?

Mr. STEPHENS. Chairman DeFazio, Ranking Member Crawford, and distinguished members of the committee, good morning. My name is Michael Stephens. I am the general counsel and executive vice president for information technology at Tampa International Airport. We thank you for the opportunity to participate in today's hearing, and to offer the aviation perspective.

More than 2.9 million passengers travel through America's airports each and every day. The five largest U.S. airports alone have more passengers flowing through them than the entire population of the United States.

U.S. commercial airports are connected, critical infrastructure ecosystems that are essential not only to our Nation's economic prosperity, but to our national security.

The aviation industry accounts for more than 5.2 percent of our national GDP and supports nearly 11 million jobs.

The aviation sector, like other sectors represented here today, faces significant challenges from persistent and increasingly pernicious cyber threats. In short, digital code, computers, and keyboards have become the newest tools of criminals, and the preferred weapons of war for nation states and other U.S. adversaries.

It is my opinion that cybersecurity threats, without question, represent the most persistent danger to the safe, secure, and efficient operations of U.S. airports in the global aviation system. And while there is no silver bullet or perfect defense against cybersecurity threats, there are numerous critical activities that can be undertaken by key stakeholders to increase our overall cybersecurity preparedness and resilience.

For the purpose of this hearing, I have distilled my remarks down to four key areas.

First, the mandatory adoption of minimum cyber standards. Although aviation and airports and other sector stakeholders have engaged in building and achieving various levels of cyber maturity, there are currently no significant requirements for adherence to minimum baseline standards or preparedness frameworks. Given the growing threat environment, the aviation sector has approached an inflection point, where voluntary cyber compliance is simply no longer adequate. I believe significant consideration should be given by aviation sector regulatory agencies to mandating the adoption and periodic testing of established cybersecurity standards and resiliency frameworks.

Second, the timely and effective sharing of information and threat intelligence is essential to assessing and mitigating cyber vulnerabilities. Consideration should be given to mandatory disclosure of critical and actionable cyber incidents that meet an agreed-upon threat threshold, irrespective of whether or not the incident resulted in an actual data breach or system compromise.

Third, we must close the human factors gap. Notwithstanding the most effective standards, technological defenses, and threat sharing efforts, the human factor remains the most highly exploited vector for penetrating cyber defenses.

The aviation sector has taken cybersecurity seriously and continues to implement processes to enhance cyber awareness and security. However, the depth and the quality of training can vary significantly, depending upon the entity. Requiring the adoption of baseline standards, which establish minimum training requirements for critical aviation sector employees should be given significant consideration.

And finally, we must dramatically increase our national focus on workforce development in order to build our cyber defense capacity. In short, we are losing the race for talent. In the U.S., we have a critical shortage of cybersecurity talent with essential skills, such as security and network engineers and software developers. These types of skills are absolutely necessary in order to increase our cyber resilience capabilities. The scarcity of these types of skills represents a significant risk to U.S. competitiveness and security.

As the use of current and future technologies increases to support airports, airlines, and other critical aviation systems, the threat of disruptive cyberattacks will undoubtedly increase, as well. The need for additional Federal assistance, information sharing, workforce training, and the adoption of baseline standards are all essential to our national security and long-term economic prosperity.

Again, we thank you for the opportunity to testify before you today, and I look forward to answering any questions that you may have.

[Mr. Stephens's prepared statement follows:]

Michael A. Stephens, General Counsel and Executive Vice President for Information Technology, Hillsborough County Aviation Authority, Tampa International Airport

Chairman DeFazio, Ranking Member Graves, and distinguished members of the Committee thank you for the opportunity to participate in today's hearing on the critically important topic of understanding and mitigating cybersecurity threats to our nation's critical infrastructure.

According to the Federal Aviation Administration (FAA), more than 2.9 million passengers travel through America's airports each and every day. Based on some of the most recent available data, US airports facilitated the shipment of more than 44 billion pounds of cargo. In total, our nation's airports, along with our airline partners and all other aspects of the US aviation industry, account for more than 5.2% of our national GDP, contribute $1.6 trillion in total economic activity and support nearly 11 million jobs. By any standard, airports, particularly our commercial airports, are incredibly complex, connected critical infrastructure ecosystems that are essential not only to our nation's economic prosperity but to our national security as well.

The size and scope of operations, as well as the passenger volume activity in our nation's airports, are vast. The FAA classifies the nation's 30 largest airports by passenger volume as large hub airports, of which Tampa International is in that category. Out of those 30 airports designated as large hubs, the largest five have more passengers flowing through them on an annual basis than the entire population of the United States.

As with most industries in order to meet the increasing demand and needs of global commerce and the traveling public, airports, along with our airline partners, have increasingly relied on technology both out of operational necessity and to enhance passenger safety, security and convenience. The ubiquitous use of technology has made airports, airlines, and aviation more efficient and has undergirded and facilitated the tremendous growth of global mobility, commerce, and connectivity.

In today's modern and technologically advanced airports, there are virtually no areas or functions that do not interface with or rely on some level on a digital network, data transfer, computer application, or internet interface. Virtually all functions essential to airport operations and aviation safety and security, such as access controls, navigation, airfield lighting, communications, industrial system controls, and emergency response systems, rely heavily on a multitude of technology applications and platforms. Moreover, airport information systems contain or process tremendous amounts of sensitive data such as passenger manifests, security plans, and data containing financial and personally identifiable information (PII).

The operational importance of these systems, coupled with the fact that they are increasingly supported and connected through networks that rely on global technology supply chains, makes airports immensely appealing targets and increasingly vulnerable to criminal organizations and state-sponsored bad actors.

Airports, airlines, and the aviation sector, like other industries, face significant challenges from a persistent and increasingly pernicious cyber threat environment. Imagine, if you will, the potentially dire consequences of a successfully coordinated major cyber-attack on any one or more of our large hub airports, airlines, or the Air Traffic Management System. The potential resulting national and international disruption, economic harm, erosion of safety, and degradation of vital aspects of our national defense capability would be enormous.

In short, computers, keyboards, and digital code have become the newest tools of criminals and some of the preferred weapons of war for nation-states and other US adversaries. That is why it is of paramount importance that we exercise increased urgency and vigilance to anticipate, identify and mitigate cyber threats to our nation's airports, airlines, and other critical aviation infrastructure. Given the nature of these existing and growing threats, proactively implementing standards, protocols, and countermeasures to protect ourselves against potential catastrophic system disruption must become one of our highest priorities.

While there is no silver bullet or perfect defense against cybersecurity threats within the aviation industry or any industry for that matter, there are critical activities that we must undertake to increase our cyber resilience and mitigate as much risk as possible. For the purposes of this hearing, I have distilled my remarks down to a few critical areas that I believe present the best opportunity for airports along with our airline partners and aviation sector stakeholders to achieve greater preparedness, responsiveness, and resilience.

Mandatory Minimum Standards

Under the Federal Information Security Management Act (FISMA), which defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats, Federal agencies are required to adopt and implement a national baseline standard for cybersecurity preparedness. In 2013, President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which called for the development of a voluntary risk-based cybersecurity framework that is "prioritized, flexible, repeatable, performance-based, and cost-effective." Subsequent executive orders and recent Presidential Directives have also been issued to address and respond to the ever-changing cybersecurity threat landscape and strengthen the requirements by Federal agencies for ensuring and maintaining a baseline level of preparedness.

Although airports, airlines, and other aviation stakeholders have engaged in building and achieving various levels of cybersecurity capability, maturity and resilience, there are currently no significant requirements for adherence to a minimum baseline set of standards for preparedness. According to a 2015 survey of airports in the United States by the Airport Cooperative Research Program (ACRP) in its *Guidebook on Best Practices for Airport Cybersecurity*, only nine out of twenty-four (34%) airport respondents indicated that they had implemented a cybersecurity standard or framework. Even assuming that the percentage has increased, given the voluntary nature of implementing a standard within the industry, there is no meaningful way to assess adoption, adequacy, or consistency.

Moreover, according to a 2018 SITA Air Transport Cybersecurity Insights report of aviation industry participants, only 41% of respondents identified cybersecurity as part of their top organizational risks. Only 42% of respondents planned to include cyber risk in their organizational critical risk assessments in 2021. Fewer than 35% of the responding organizations had a dedicated Chief Information Security Officer (CISO), which is essential to raising cybersecurity resilience as a priority to most executive and governance levels.

Given these numbers, I believe that the aviation sector is at an inflection point in the growing threat environment where voluntary compliance is no longer adequate. This position is clearly evidenced by the increasing sophistication and adverse impact on our economic and national security from attacks such as SolarWinds and Colonial Pipeline. It is my opinion that strong consideration should be given by Congress and regulatory agencies such as the FAA and TSA to mandate the adoption and implementation of minimum baseline cyber security standards and frameworks throughout the aviation sector. The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure for Cybersecurity, for example, provides substantial guidance for establishing a minimum cyber resilience framework for the aviation sector and other critical infrastructure sectors.

Such a baseline cybersecurity framework would not replace an existing cybersecurity program that an organization already has in place. The framework would be used to augment, enhance and strengthen any existing program and align it with best practices for greater coordination and effectiveness throughout the aviation industry. For airports, airlines, and key stakeholders that do not have a baseline cybersecurity program, such a requirement would ensure a minimum level of readiness and facilitate the development of more effective sector cyber preparedness and maturity.

Cyber Security Information Sharing & Communication

While one of the stated objectives of EO 13636 focused on increasing information sharing between the government and the private sector, it has not been as effective as it could be due to the program's voluntary nature. The sharing of information and threat intelligence is a critical component to assessing airport and aviation sector vulnerabilities, enhancing our preparedness posture, as well as giving airports and our airline partners the ability to respond more effectively and recover in the event of a cybersecurity incident.

Often information sharing practices within the aviation sector have been reactive versus proactive. Voluntary information-sharing programs have demonstrated utility when reacting to and recovering from a cyber-incident when shared in a timely manner. However, the exponentially growing threat landscape will require significantly more investment by the public and private sectors both nationally and internationally.

In order to strengthen information sharing, consideration should be given to requiring mandatory disclosure of cyber incidents that meet an agreed-upon threat threshold irrespective of whether or not the incident resulted in an actual data breach or system compromise. The information reporting and sharing requirement should focus on actionable threats and risks in order to minimize the data and information overload, or the creation of information "white noise".

Laws such as the Cybersecurity Information Sharing Act (CISA) and related programs such as the DHS Cyber Information Sharing and Collaboration Program (CISCP), if coupled with the implementation of mandatory minimum standards within the aviation sector, may help to accelerate the progress of information sharing and collaboration. However, mandating a minimum baseline common standard and enhancing opportunities to share critical cybersecurity threat intelligence in a timely manner within the aviation and across other critical infrastructure sectors will ultimately result in the greater national capability to combat cyber security risks.

Information Security Awareness Training and Workforce Development

Closing the human factors gap is a critical and integral part of a successful and effective cyber resilience strategy within all critical infrastructure sectors. Notwithstanding the most effective program standards, technological cybersecurity defenses, and threat intelligence information-sharing efforts, the human factor remains the most highly exploited vector for penetrating cybersecurity defenses within the aviation sector. In a recent study by Airports Council International (ACI) of key aviation leaders and stakeholders, 87% of the respondents reported that social engineering attacks were the leading vector of cyberattacks.

Cybersecurity threat awareness and information security training programs for all airport, airlines, and aviation industry employees is perhaps one of the most efficient and cost-effective ways of increasing cybersecurity preparedness in the aviation sector. The NIST "Framework for Improving Critical Infrastructure Cybersecurity" (NIST 2014) specifically indicates that cybersecurity awareness and training is a critical and indispensable component to an entity's overall cybersecurity program.

Airports, airlines, and the aviation sector take cybersecurity seriously and have implemented creative processes to educate staff and tenants to further enhance cyber awareness, hygiene and security. Numerous resources are increasingly being made available for cybersecurity training at the federal, department, and state level. According to the survey of airports in the United States by the Airport Cooperative Research Program (ACRP), 20 of 27 (74%) of the responding airports indicated that they engage in some form of employee information security training.

However, due to the multitude of differences within airport governance and organizational structures, the scope, depth, and quality of training may vary significantly from airport to airport. Numerous additional factors may also adversely impact the quality and breadth of training, such as availability of budgets particularly in a post COVID environment, lack of available subject matter expertise and adequate buy-in from senior management in prioritizing spending on resiliency efforts.

To combat the exponential growth of cyberattacks, we must make significant investments to develop cyber literacy and equip people with the necessary tools to detect and defend against bad actors. This will require efforts beyond typical awareness training and would ideally build on aviation's physical safety-and-security culture to develop a cybersecurity culture across all industry stakeholders.

Adopting and requiring a uniform standard which establishes a minimum baseline training requirement for airport, airlines and other aviation sector employees on a defined and reoccurring basis should be given significant consideration by the appropriate aviation sector regulatory agencies such as the FAA and TSA.

Workforce Development

We are losing the race for talent. Professionals, specifically within the aviation industry, with critical cybersecurity skills and competencies are in scarce supply. In the US, we have a critical shortage of cybersecurity lent such as software engineers, software developers and network engineers. By some industry estimates, the US currently has a shortage of more than one million security experts, and that number is expected to grow significantly over the next decade. These essential skills are necessary to increase our cyber resilience and response capabilities d represent a significant risk to US national security and competitiveness.

We must invest in building future cyber capacity by identifying and recruiting highly sought-after talent and developing and retaining our current cyber workforce. In order to close the cybersecurity skills gap, substantial national public and private efforts should be undertaken to develop and expand the capabilities of current and future workforces. Particular focus should be placed on developing cyber competencies through high school and university education programs promoting science, technology, engineering, mathematics, and foreign language (STEM–L).

Conclusion

Our nation's airports, airlines, and other critical aviation infrastructure rely heavily on information technology and complex data networks to support the growing demands of our economic, strategic, and national security interests. As the adoption of current and future technologies increases to support the aviation sector both here and abroad, the threat of disruptive cyber-attacks on airports, airlines, and critical aviation information systems and data will undoubtedly increase as well. Evolution towards a more effective, non-voluntary cyber risk mitigation strategy against this pernicious and imminent threat must be undertaken proactively and with a renewed sense of urgency. The need for increased assistance, improved regulatory oversight, and the urgent adoption and implementation of a baseline cybersecurity protection framework and standard for information sharing and workforce training are essential to the nation's security and long-term economic prosperity.

Mr. DeFazio. Thank you for your testimony, Mr. Stephens, and now we would move to John Sullivan.

Mr. Sullivan, you are recognized for 5 minutes.

Mr. Sullivan. Chairman DeFazio, Ranking Member Crawford, and members of the committee, thank you for the opportunity to testify on cybersecurity challenges facing the Nation's water and wastewater infrastructure. I am John Sullivan, chief engineer of the Boston Water and Sewer Commission. I am also chair of the Water Information Sharing and Analysis Center, or WaterISAC, and deliver my testimony today in that capacity.

WaterISAC is a nonprofit organization established in 2002 by the national water and wastewater associations at the urging of EPA and the FBI to provide utilities with critical information on physical and cybersecurity threats, and best practices for prevention and response. WaterISAC member utilities currently serve 206 million people across the United States, about 60 percent of the U.S. population. While EPA and Congress provided some funding to get the service up and running in the early 2000s, today member dues payments support 100 percent of the WaterISAC's budget.

We know that water and wastewater utilities pose attractive targets for cyberattackers. My written testimony references several recent cyber intrusions against water and wastewater systems that occurred last year, targeting utilities across the country. Perhaps best known is the attack early this year against the water utility serving Oldsmar, Florida. While utility staff immediately observed the breach and took corrective action that prevented any impacts to water quality or public health, it is easy to imagine how the outcome could have been much worse.

For example, consider an attack that infiltrates the industrial control systems of a wastewater system, and disables the treatment train or the pumps that move sewage from one part to another. This could result in the release of large amounts of sewage into rivers and streams, harming the natural ecology of the receiving waters, creating a public health nuisance, and potentially contaminating sources of drinking water.

The Boston Water and Sewer Commission had its own experience with a cybersecurity incident last year in the form of a ransomware attack. While it complicated the day-to-day business and was costly to recover from, there was never any threat to public or environmental health, due to precautions such as our business network being segregated from our control systems. This is a best practice in any sector that uses industrial control systems, but this approach is not consistent across the Nation's 16,000 wastewater systems and 50,000 drinking water systems.

With such a large universe of water systems across the country, many are bound to have a lack of understanding of these cyber best practices, or a lack of expertise and equipment to implement them. This is where the WaterISAC can help. In Boston's case, the center was instrumental in our recovery from our incident, as it referred us to a firm specializing in ransomware incident response, which helped us navigate our way through the events.

More broadly, WaterISAC offers resources such as 15 security fundamentals for water and wastewater utilities, a set of best practices for the protection of information technology and industrial control systems. The 15 fundamentals provide straightforward, but sometimes overlooked, tasks like enforcing user access controls, performing asset inventories, addressing vulnerability management, and creating a cybersecurity culture.

As the committee conducts oversight of cybersecurity at wastewater utilities and other critical infrastructure entities, we recommend an approach that provides more resources to both wastewater systems themselves and to the EPA in its capacity as the sector risk management agency for the water and wastewater sector. These resources could come in the form of technical assistance programs to help medium and small wastewater systems implement technology upgrades and secure external services; initiatives to expand the reach of the Water Rights Act to all wastewater systems nationwide; and assessment assistance and training to help wastewater systems comply with best practices.

One promising approach can be found in the Infrastructure Investment and Jobs Act. One provision in this bill would encourage electric utilities to bolster their cyber preparations and would seek to increase participation in the electricity information sharing and analysis setup, WaterISAC's counterpart from the electric sector.

A similar direction for EPA to take steps to bolster water sector participation in the Water Rights Act, especially among the wastewater systems serving fewer than 100,000 people, would help get threat information and best practices into more hands across the country.

We would be happy to work with you on this effort. Thank you for the chance to testify today, and I am happy to answer any questions.

[Mr. Sullivan's prepared statement follows:]

John P. Sullivan, P.E., Chief Engineer, Boston Water and Sewer Commission, on behalf of the Water Information Sharing and Analysis Center

Chairman DeFazio, Ranking Member Graves, and members of the committee: I appreciate the opportunity to appear at today's hearing on "The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure."

I am John P. Sullivan, and for many years I have served as the Chief Engineer of the Boston Water and Sewer Commission. The Commission is the largest and oldest water system of its kind in New England and provides drinking water and sewer services to more than one million people daily. In addition, I currently chair the Water Information Sharing and Analysis Center, better known as WaterISAC, and serve on the Water Sector Coordinating Council, comprising the national water and wastewater associations,[1] which advises the U.S. Environmental Protection Agency and the Cybersecurity and Infrastructure Security Agency (CISA) on their security programs. I am also a member of the board of directors of the Association of Metropolitan Water Agencies and the National Association of Clean Water Agencies, and serve on the Water Utility Council of the American Water Works Association.

I testify today on behalf of WaterISAC, a non-profit organization established in 2002 by the national water and wastewater associations, at the urging of EPA and the FBI, to provide utilities with critical information on physical and cybersecurity threats and best practices for prevention and response. The designated information-sharing arm of the Water Sector Coordinating Council, WaterISAC is the most comprehensive and targeted single point source for data, facts, case studies, and analysis on water security and threats from intentional contamination, terrorism, and malicious cyber actors. WaterISAC member utilities currently serve 206 million people across the United States—about 60% of the U.S. population.

We commend the committee for holding today's hearing because protecting the nation's critical infrastructure against a growing range of cyber threats is an issue of increasing urgency. My testimony will provide an overview of the cyber risks faced by water and wastewater systems, the sector's response thus far, and what we can do looking forward.

Water and Wastewater Systems' Cyber Risks

Water and wastewater systems are an attractive target for cyber attackers, and the implications of an attack could be significant. This is why water, along with transportation, energy, and communications, are the four "lifeline functions" designated by the Department of Homeland Security. This means that the operations of these sectors are so critical that any disruption or loss will directly affect the security of other critical infrastructure sectors as well.

However, it is important to distinguish between different types of cyber-attacks that could target water and wastewater systems. The first are attacks against utilities' information technology systems, also known as business or enterprise systems. These include email systems, websites, and billing databases. In recent years water and wastewater systems have reported a variety of such attacks, which include ransomware incidents, email compromise scams, and social engineering and

[1] The Water Sector Coordinating Council consists of the American Water Works Association, the Association of Metropolitan Water Agencies, the National Association of Clean Water Agencies, the National Association of Water Companies, the National Rural Water Association, WaterISAC, the Water Environment Federation, and the Water Research Foundation.

phishing attempts. And while these attacks, if successful, can disrupt day-to-day business and compromise sensitive data, they, alone, would not have any impact on the treatment or management of drinking water or wastewater.

A more concerning type of cyber-attack would target a utility's industrial control system. Industrial control systems operate treatment processes, valves, pumps, and other utility infrastructure.

Last month EPA published a joint cyber advisory along with the FBI, Cybersecurity and Infrastructure Security Agency, and NSA outlining "Ongoing Cyber Threats to U.S. Water and Wastewater Systems."[2] The advisory featured input from WaterISAC and summarized some common cyber threats to water and wastewater systems, recommended mitigation actions, and resources for systems to access. It also cited several cyber intrusions against U.S. water and wastewater systems since last year, including incidents affecting utilities in California, Maine, Nevada, New Jersey, and Kansas. While none ultimately affected public health or environmental quality, the growing number of incidents makes clear that utilities must be prepared to defend against and respond to these attacks.

One of the most-publicized recent cyber intrusions against a U.S. water utility played out this past February at the drinking water system serving the city of Oldsmar, Florida. In this case, an unknown malicious actor infiltrated the city's water treatment plant and made changes to chemical levels in the treatment process. According to the Pinellas County sheriff, the attacker accessed a computer in the treatment plant's control system using an application called TeamViewer. A plant operator observed two intrusions that were hours apart. In the second intrusion, which lasted about five minutes, the operator saw the mouse moving around as the malicious actor accessed various functions. One of these functions controls the amount of sodium hydroxide in the water, which the actor changed from about 100 parts per million to 11,100 parts per million. The operator in Oldsmar observed this change and immediately reversed it.

If the intrusion had not been detected in real time, reports say that it would have taken between 24 and 36 hours for the affected water to reach the distribution system, and prior to that point it most likely would have been detected by redundancies that are in place to check water quality before release. But this incident is emblematic of how bad actors can take advantage of cyber vulnerabilities that may be present in many of the nation's roughly 50,000 drinking water systems and 16,000 wastewater systems, and it is easy to imagine how the outcome might have been far worse. What if, for example, the intruder was not immediately detected, and was able to manipulate pumps to drain a water tower or restrict distribution to certain areas? Such an outcome not only would have undermined the public's confidence in their water service but would have carried severe impacts on the community's environmental, fire protection, and public health.

With wastewater systems, one danger is that an attack can disable the treatment train or the pumps that move treated and untreated sewerage from one point in the process to another. A successful attack could release large amounts of sewerage into rivers and streams, harming the natural ecology of the receiving waters, creating a direct public health risk and also contaminating sources of drinking water.

It is important to recognize that organizations—from federal agencies to large and small businesses—can implement every best practice in the book and still suffer a cybersecurity attack. Notwithstanding that nation states have sophisticated methods of gaining unauthorized access to even the most secure systems, compromises can also be caused simply by one employee clicking on a malicious link in an email. So not only is it critical to implement the best technologies, but it is also critical to educate employees and to have incident response plans in place should attacks occur.

The Boston Water and Sewer Commission had its own experience with a cybersecurity incident in the form of an Egregor ransomware attack last year. While it complicated day-to-day business for many weeks and was costly to recover from, there was never any threat to public or environmental health, due to our business network being segregated from our control system, among other precautions. This saved the utility from suffering much greater impacts and is a best practice in any sector that uses industrial control systems, but this approach is not consistent across water and wastewater systems. This is likely due to a lack of understanding, among many utilities, of its importance and a lack of expertise and budget to implement it.

WaterISAC was instrumental in helping Boston Water and Sewer recover from this incident. The center referred the utility to a firm specializing in ransomware

[2] https://us-cert.cisa.gov/sites/default/files/publications/AA21-287A-Ongoing__Cyber__Threats__to__U.S.__Water__and__Wastewater__Systems.pdf

incident response, which helped us navigate our way through the event. In situations such as these, WaterISAC has access to a field of subject matter experts at other utilities and at private firms that it can tap in support of its members.

Water and Wastewater Systems Cybersecurity: State of the Sector

We know there is more the water and wastewater sector could be doing to prepare for cyber-attacks. According to a cybersecurity survey on water and wastewater systems—*2021 State of the Sector* [3]—released in June by the Water Sector Coordinating Council, adoption of cyber best practices varies across the sector. For instance, the Council found that while cybersecurity is an element of most utility risk management plans, that is not the case for nearly 40% of respondents, which included many systems serving less than 500 people, but in some cases those serving hundreds of thousands. On the whole we found that larger utilities—with more resources—have fewer challenges to implementing cybersecurity practices, while many smaller utilities lack funding and expertise.

Sector Efforts to Improve Cybersecurity

One resource available to the sector is WaterISAC, established in 2002 with seed money from EPA and subsequent congressional appropriations. A critical component of cybersecurity preparedness is having access to the latest cyber threat and vulnerability information and to best practices from subject matter experts. One of two dozen other ISACs across critical infrastructure sectors, WaterISAC annually issues hundreds of advisories, maintains a portal for members and hosts webinars and threat briefings. The center also receives incident reports and conducts threat analyses to help water and wastewater utilities stay ahead of the threat curve.

In more recent years, in collaboration with EPA, through the Government Coordinating Council, the water sector as a whole has recommended that utilities implement best practices and has offered resources to that end.

Among these is WaterISAC's free *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*, a set of best practices for the protection of information technology and industrial control systems. First published in 2012 and most recently updated in 2019, the *15 Fundamentals* provide straightforward but sometimes overlooked tasks like enforcing user access controls and performing asset inventories. Other recommendations in the guide address vulnerability management and creating a cybersecurity culture.[4]

Another key sector resource is the American Water Works Association's *Cybersecurity Guidance & Tool*, which is based on the NIST Cyber Security Framework. The AWWA guidance offers a sector-specific approach for implementing applicable cybersecurity controls and recommendations and is widely used.

WaterISAC and the sector associations also promote EPA tools and those offered by CISA, as well as small-system resources through AWWA and the Department of Agriculture.

In terms of federal oversight of the sector's cybersecurity drinking water and wastewater systems are not subject to the same requirements. On the drinking water side, America's Water Infrastructure Act of 2018 (P.L. 115–270) requires drinking water utilities, under the oversight of EPA, to periodically take an "all-hazards" look at potential threats, including risks to "electronic, computer, or other automated systems." This provides an opportunity to evaluate potential threats and

[3] waterisac.org/2021survey

[4] The complete list of 15 water sector cybersecurity fundamentals, available at waterisac.org/fundamentals, consists of:

1. Performing Asset Inventories
2. Assessing Risks
3. Minimizing Control System Exposure
4. Enforcing User Access Controls
5. Safeguarding from Unauthorized Physical Access
6. Installing Independent Cyber-Physical Safety Systems
7. Embracing Vulnerability Management
8. Creating a Cybersecurity Culture
9. Developing and Enforce Cybersecurity Policies and Procedures
10. Implementing Threat Detection and Monitoring
11. Planning for Incidents, Emergencies, and Disasters
12. Tackling Insider Threats
13. Securing the Supply Chain
14. Addressing All Smart Devices
15. Participating in Information Sharing and Collaboration Communities

develop response measures. However, there is no statutory requirement for wastewater systems to take similar actions.

A New Approach to Water Sector Cybersecurity

Despite these differences, both water and wastewater systems are implementing best practices to safeguard their information systems and industrial control systems from attacks and fulfilling their missions to protect public health and the environment. However, the water and wastewater sector is large and diverse, and we see room for improvement, as demonstrated by the *State of the Sector* report noted above. The current approach could leave utilities vulnerable to cybersecurity attacks that could endanger health and the environment.

One of the most effective ways for Congress to help the nation's wastewater systems withstand cyber threats is to provide more resources to both the systems themselves and to EPA in its capacity as the Sector Risk Management Agency (Sector-Specific Agency) for the water and wastewater sector. These resources could come in the form of technical assistance programs to help medium and small wastewater systems, additional grant funding to help individual wastewater systems implement technology upgrades and secure external services, initiatives to expand the reach of WaterISAC to all wastewater systems nationwide, assessment assistance, and training to help wastewater systems comply with best practices. Indeed, the *State of the Sector* survey cited resources such as these among utilities' top needs.

One promising model could be based on provisions included in Section 40125(c) of the Infrastructure Investment and Jobs Act. This proposal aims to improve the cybersecurity of bulk power systems and would authorize $250 million over five years to support a new Energy Sector Operational Support for Cyberresilience Program at the Department of Energy. Among the objectives of this program would be supporting efforts "to expand industry participation in [Electricity]-ISAC," the Electricity Information Sharing and Analysis Center, WaterISAC's counterpart for the electricity sector. Should the Transportation and Infrastructure Committee develop legislation related to cybersecurity in the wastewater sector, a similar EPA program aimed at increasing participation in WaterISAC should be considered.

As previously mentioned, WaterISAC currently counts among its members water and wastewater utilities that serve about 60% of the U.S. population. Some members serve as few as 2,000 people, but most members serve larger populations. However, only about 400 of the nation's nearly 50,000 community water systems and 16,000 wastewater systems are paying WaterISAC members that enjoy full access to all of the nonprofit's threat and vulnerability alerts, subject matter expertise, and other information.

Congress provided funding to get the center up and running in the first decade of the 2000s, but since that time the center has been funded exclusively through member dues. These dues are structured on a sliding scale—beginning at $100 per year—so as to be affordable for smaller utilities, but nevertheless many utilities are not able to take advantage of the resources available. At the same time, many thousands of utilities are simply unaware of WaterISAC. Unless more utilities are part of WaterISAC, then lack of awareness of threats will prevail.

WaterISAC member utilities have more and better information with which to build a security and resilience program than those that don't belong to the center.

Therefore, federal assistance to underwrite membership fees for small and medium-sized water and wastewater systems and a federal program to increase awareness of the center would help get threat information and best practices into more hands across the country. As noted in the *State of the Sector* report, the greatest challenge for smaller systems is awareness of threats and best practices.

We estimate that federal assistance at a level of just $6 million over three years would enable WaterISAC to provide a broader array of services to water and wastewater systems nationwide. Specifically, this level of funding would be used to cover the cost of membership for thousands of small and medium systems, expand our threat analysis capabilities, conduct exercises and training, and offer technical support to utilities.

Conclusion

WaterISAC appreciates the opportunity to share our views on the cyber threat landscape facing the nation's water and wastewater systems, and effective strategies to help utilities respond to these challenges. I am proud of the work the water and wastewater sector has done on its own to spread awareness of sound cyber practices, but additional resources and assistance from the federal government would go a long way toward ensuring the greatest number of water and wastewater utilities are as prepared as they can be. We stand ready to work with you to make this a reality.

Mr. DeFazio. Thank you, Mr. Sullivan. And our last witness will be Gary Kessler.

Mr. Kessler, 5 minutes.

Mr. Kessler. Thank you. Chairman DeFazio, Ranking Member Crawford, and members and staff of the committee, thank you for the invitation and opportunity to speak today. I am Gary Kessler, a nonresident senior fellow at the Atlantic Council, and one of the coauthors of the Council's report, "Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity."

I have spent my professional career since the 1970s in the information technology and information security field. I am a retired professor of cybersecurity, coauthor of a book on maritime cybersecurity, and a principal consultant at Fathom5 working on cyber issues related to maritime operational technology testbeds. I also hold a national office in the U.S. Coast Guard Auxiliary Cybersecurity Division, and I am a visiting faculty member at the U.S. Coast Guard Academy.

Most people in the United States do not think of our country as a maritime nation. They don't understand and appreciate our Nation's reliance upon the maritime transportation system, or MTS, for our very way of life. Our report addresses that dependence in some very tangible ways, from the $5.4 trillion contribution to the U.S. economy, representing about 25 percent of our country's gross domestic product, to the 30 million jobs.

Roughly 80 percent of global trade and nearly two-thirds of the world's total petroleum and other liquid energy supply is carried by ship. In the United States, approximately 90 percent of our imports/exports move by sea, emphasizing the fact that most global supply chains are existentially dependent upon maritime.

Consider the disruption to the global supply chain caused earlier this year, when *Ever Given* became stuck in the Suez Canal, costing the global trading community nearly $9 billion each day. Much closer to home, note the current disruption to U.S. supply chains because of the backlog of the Ports of Long Beach and Los Angeles, the entry for nearly 40 percent of U.S. imports.

The ability to move military personnel and materiel by sea, combined with the global presence of U.S. Navy warships and the U.S. Coast Guard, are fundamental to U.S. military power projection around the world.

The maritime transportation system is critical and poses significant challenges to policymakers. The MTS is composed of many independent, yet co-dependent and inextricably intertwined systems representing ships, ports, shipping lines, inland waterways, and intermodal transfers.

The system of systems metaphor speaks to the fact that the maritime sector is not monolithic, where a single set of rules or regulations can manage the industry. This provides a particular challenge to legislators, regulators, and those with administrative responsibility alike. Like the rest of the industrial world, MTS stakeholders take advantage of new technology, and this goes to the very heart of why we are here today.

The modern computer age dates back only about 75 years. Commercialization of the internet began a mere 30 years ago. The acceleration of change in computing and communication technologies is now almost beyond comprehension, and includes advances in processors, sensors, embedded computers, operational technology, cyber physical systems, navigation, big data, machine learning, and artificial intelligence. These advances have led to the Internet of Things, smart ships and ports, the Ocean of Things, automation and maritime systems, and fully autonomous vessels.

Computer attacks that were almost unheard of 30 years ago are commonplace today. Ships that barely had a computer on board 25 years ago are now susceptible to cyberattack, even in the middle of the ocean. Multiple sources report a sharp uptick in the number of cyberattacks directed toward the MTS since 2019, including more than a dozen ransomware events in the last 18 months.

Cybersecurity has risen to become a significant threat to the maritime sector, no less than the food security, energy security, economic security, homeland security, and national security of the United States are dependent upon the seas. The maritime transportation sector is broad, diverse, and global, so that, while international cooperation is essential, central management is impossible. Cyber vulnerabilities are as plentiful in the maritime sector as in the nonmaritime world and provide unique threats to the industry.

The National Maritime Cybersecurity Plan was a clarion call about a significant threat facing this country. Our report, "Raising the Colors," was a first step at trying to provide a tactical approach to addressing that threat. We have to continue pushing forward to address this critical issue.

Thank you, and I look forward to your questions and further discussion.

[Mr. Kessler's prepared statement follows:]

Gary C. Kessler, Ph.D., Nonresident Senior Fellow, Atlantic Council

Chairman DeFazio, Ranking Member Graves, and members and staff of the committee—thank you for the invitation to provide testimony to the committee. I am a Non-Resident Senior Fellow at the Atlantic Council and one of the authors of the Council's report, *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity*.[1] I have spent my professional career since the 1970s in the information technology and information security fields, am a retired professor of cybersecurity, and the co-author of a book on maritime cybersecurity.[2] I am also a Principal Consultant at Fathom5 working on cyber issues related to maritime operational technology (OT) testbeds, am a visiting faculty member at the U.S. Coast Guard Academy, and hold a national office in the U.S. Coast Guard Auxiliary's Cybersecurity Division.

United States Dependence Upon Maritime Transportation

Most people in the United States do not think of our country as a maritime nation. They view our nation's waterways as a venue for recreation or a vacation getaway, a source of food, or the home of 12 million recreational boats and pleasure craft. Our citizens, in large part, neither know about nor appreciate our reliance upon the maritime transportation system for our very way of life.

Our report addresses that dependence in some very tangible ways—the maritime transportation system (MTS) contributes $5.4 trillion to the U.S. economy, rep-

[1] Loomis, W., Singh, V.V., Kessler, G.C., & Bellekens, X. (2021, October). *RAISING THE COLORS: Signaling for Cooperation on Maritime Cybersecurity*. Cyber Statecraft Initiative, Scowcroft Center for Strategy and Security, Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Raising-the-colors-Signaling-for-cooperation-on-maritime-cybersecurity.pdf

[2] Kessler, G.C. and Shepard, S.D. (2020, September). *Maritime Cybersecurity: A Guide for Leaders and Managers*. Amazon Kindle Direct Publishing, http://www.maritimecybersecuritybook.com

resenting about 25% of our country's gross domestic product, as well as 30 million jobs.[3] Roughly 80% of global trade and nearly two-thirds of the world's total petroleum and other liquid energy supply is carried by ship. In the U.S., approximately 90% of our imports/exports are by ship, emphasizing the point that no global supply chain is independent of maritime transport, and most, in fact, are existentially dependent upon it.

Consider the disruption to the global supply chain caused when the cargo ship EVER GIVEN was stuck in the Suez Canal in March of this year, costing the global trading community nearly $9 billion each day. Although the blockage only lasted for six days, the 20,000-container vessel did not leave the Canal area for nearly four months pending a dispute with the Suez Canal Authority.[4] Much closer to home, consider the current disruption to the U.S. supply chain due to the backlog at the Ports of Long Beach and Los Angeles, the entry way for nearly 40% of U.S. imports. There are myriad causes for the backlog but the bottom-line impact is higher costs, delays in getting goods to market, and global disruption of many product supply chains.[5]

In addition, the ability to move military personnel and matériel—a capability known as *sealift*—combined with the global presence of U.S. Navy warships and U.S. Coast Guard cutters are the basis of U.S. military power projection around the world. These latter capabilities have served the nation in time of war, provided a capability to protect shipping routes, and acted as a deterrence to ensure peace.[6]

THE MTS IS NOT MONOLITHIC

While we often talk about the MTS as if it was a single, monolithic entity, it is actually a system of systems, representing ships, ports, shipping lines, inland waterways, and intermodal transfers.[7] All of these systems operate independently, yet are co-dependent and inextricably intertwined. The life cycle of a ship, for example, intersects with the lifecycle of a port and is only a part of the life cycle of a shipping line. The life cycle of people and cargo within the MTS intersect with a ship's voyage and transit through ports, intermodal transfers, and inland waterways. The cybersecurity threats to the MTS are similar to threats everywhere else in information space, but are unique to our industry and way of life.

Ports are one of the primary focus points of our report. Intellectual property (IP) theft related to port operations and construction can yield very valuable information to competitors and adversaries, alike. The deliberate installation of a Stuxnet-type of vulnerability[8]—i.e., software that can attack and destroy hardware—into a vessel or vessel component during construction could provide the basis for a ransomware or other cyber attack years later.

The adage, "If you've seen one port, you've seen one port"[9] is well-known in the maritime industry. All ports are unique in terms of their ownership and management, the mix of civilian and military vessels and operations, the interconnection of information and communication technology (ICT) systems by port operators and

[3] United States Coast Guard (USCG). (2021, August). *Cyber Strategic Outlook: The United States Coast Guard's Vision To Protect and Operate in Cyberspace*. https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf

[4] Chellel, K., Campbell, M., & Ha, K.O. (2021, June 24). Six Days in Suez: The Inside Story of the Ship That Broke Global Trade. *Bloomberg Businessweek*. https://www.bloomberg.com/news/features/2021-06-24/how-the-billion-dollar-ever-given-cargo-ship-got-stuck-in-the-suez-canal

[5] Caplan, J. (2021, October 14). Port of Long Beach Director Warns Cargo Backlog is 'National Crisis.' *Breitbart*. https://www.breitbart.com/politics/2021/10/14/port-of-long-beach-director-warns-cargo-backlog-is-national-crisis/; Meeks, A., Isidore, C., & Yurkevich, V. (2021, October 19). North America's Biggest Container Port Faces Record Backlog. *CNN Business*. https://www.cnn.com/2021/10/18/business/container-port-record-backlog/

[6] Harris, S., & Fasching, Sr., J. (2020, May 21). Sealift: The Foundation of U.S. Military Power Projection. *LMI blog*. https://www.lmi.org/blog/sealift-foundation-us-military-power-projection; Masters, J. (2019, August 19). Sea Power: The U.S. Navy and Foreign Policy. *Council on Foreign Relations*. https://www.cfr.org/backgrounder/sea-power-us-navy-and-foreign-policy; Schuler, M. (2021, October 21). New USTRANSCOM Commander is 'Laser-Focused' on Buying Secondhand Ships to Boost Military's Surge Sealift. *gCaptain*. https://gcaptain.com/new-ustranscom-commander-is-laser-focused-on-buying-secondhand-ships-to-boost-militarys-surge-sealift/

[7] Kessler & Shepard, 2020; Mansouri, M., Gorod, A., Wakeman, T.H., & Sauser, B. (2009). A Systems Approach to Governance in Maritime Transportation System of Systems. *Proceedings of the IEEE International Conference on System of Systems Engineering (SoSE)*. Albuquerque, NM.

[8] Kushner, D. (2013, February 26). The Real Story of Stuxnet. *IEEE Spectrum*. https://spectrum.ieee.org/the-real-story-of-stuxnet

[9] Keefe, J. (2019, March 6). Port Security: If You've Seen One Port, You've Seen One Port. *Maritime Logistics Professional*. https://www.maritimeprofessional.com/news/port-security-seen-port-seen-343481

tenants, personnel management, intermodal connections, volume of traffic, cargo, passengers, etc. While all ports have the same general functions, each is unique.[10]

Ships, another focus point of the report, are floating networks. There are multiple operational networks onboard a vessel, including passenger/entertainment networks, navigation systems, satellite communications, ballast control, engineering control, propulsion and steering, cargo management, and more. Global Positioning System (GPS) and Automatic Identification System (AIS) communications are essential to positioning, navigation, timing, and situational awareness, and are both susceptible to jamming and spoofing.

Shipping lines are a business like any other business; they just happen to own and operate ships. Thus, they have the same potential information security vulnerabilities that any business does, from finance and logistics to communications and cargo/passenger management. There is a significant amount of third-party software and systems employed by shipping lines, so the business is not even in charge of all of their own computers and networks. Remember the havoc in companies and governmental agencies around the world with the attack on SolarWinds less than a year ago.[11]

Intermodal transfers are where the MTS touch every other form of transportation, including trucking, rail, and aviation. Even if the port, ship, and shipping line have outstanding security, a cyberfraud or cyberattack might still be perpetuated via a compromised trading partner.

People are often the largest security attack vector, both in physical space and cyberspace. People are our passengers, our workers, our adversaries, our clients, and our colleagues. We need to vet the people that are engaged in any way with the MTS, obviously at different levels of access to information and systems. Cyberattacks on the personnel or passport control systems, for example, can render the ordinary security checks worthless, not to mention the enormous amount of personally identifiable information (PII) and financial information in the personnel and passenger databases.

Cyber security in the maritime sector is a very broad endeavor. Regulation and administrative controls apply very differently to each of the sector's sub-systems.

TECHNOLOGY ADVANCES IN THE MTS

Technology in the MTS and cyber attacks go to the heart of why we at the Atlantic Council issued our report. The beginning of the modern computer age dates back only about 75 years. Modern digital communications technologies date back to the 1960s. The beginning of the global Internet started slowly just more than 50 years ago but, once commercialized a mere 30 years ago, was adopted more rapidly than any other technology in human history—at least up until that time.[12]

The acceleration of change affecting information and computing technologies is now almost beyond comprehension and includes advances in processors, sensors, embedded computers, OT, cyber-physical systems. *Digitization*—the conversion of all forms of information into a binary format—has provided the ability to store, process, analyze, and integrate all sorts of information. This has led to the huge data sets commonly known as *big data*, providing significant advances in machine learning and artificial intelligence (AI).

Indeed, digitization of information and full integration of many data streams has led to *digitalization*, the transformation that offers an incredibly broad understanding of systems that heretofore was impossible.[13] As an example, the concept of a *smart ship* allows the master of a vessel to be aware of almost every aspect about the state of the vessel, from the speed, course, bearing, water temperature, and salinity level to the stress on the hull, instantaneous fuel consumption, cargo container status, and power generation levels. Smart ports, the Internet of Things,

[10] Polemi, N. (2018). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*. Amsterdam: Elsevier.

[11] Herr, T., Loomis, W., Schroeder, E., Scott, S., Handler, S., & Zuo, T. (2021, March). *Broken Trust: Lessons from Sunburst*. Cyber Statecraft Initiative, Scowcroft Center for Strategy and Security, Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf

[12] Kleinrock, L. (2010, August). An Early History of the Internet. *IEEE Communications Magazine, 48*(8), 26–36. https://www.lk.cs.ucla.edu/data/files/Kleinrock/An%20Early%20History%20Of%20The%20Internet.pdf

[13] Sanchez-Gonzalez, P.-L., Díaz-Gutiérrez, D., Leo, T.J., & Núñez-Rivas, L.R. (2019, February 22). Toward Digitalization of Maritime Transport? *Sensors, 19*(4), 926. https://doi.org/10.3390/s19040926; United Nations Conference on Trade and Development (UNCTAD). (2019, June). Digitalization in Maritime Transport: Ensuring Opportunities for Development. *Policy Brief No. 75*. https://unctad.org/system/files/official-document/presspb2019d4__en.pdf

the Ocean of Things,[14] increased automation in maritime systems, and fully autonomous vessels are a direct result of this transformation within our knowledge base and AI software. Taken all together, the combination of advanced ICT and smart systems is driving Industry 4.0, or what is recognized as the fourth industrial revolution.[15]

The drivers for this rapidly increasing level of intelligence include safety and efficiency in operation. The majority of maritime accidents are caused by human error, often due to fatigue; automated systems can respond more quickly to unexpected events and a smart ship is better able to anticipate events. In addition, more complete knowledge of the state of the vessel can allow the officers to provide more efficient operation and routing, which can lead to a lowering of operation and fuel costs.[16]

These data-driven systems, however, offer a larger cyberattack surface than ever before. Computer attacks that were almost unheard of 30 years ago are commonplace today; ships that barely had a computer onboard 25 years ago are now susceptible to cyberattack even in the middle of the ocean. There has been a significant uptick in cyberattacks targeting the MTS since 2019,[17] including more than a dozen ransomware attacks since early 2020. Cybersecurity has risen to become a significant threat to the smooth operation within the maritime sector.

Additional Thoughts and Considerations

The cyberthreat landscape to the MTS raises the question about the role of government in helping improve the state of maritime cybersecurity. The government's response to a physical attack is very different than that of a cyber attack. If a foreign country were to fire a missile at a private company within the U.S., for example, the government would take the lead to track down the source and, undoubtedly, respond militarily. Conversely, when foreign entities launch cyberattacks against American companies, the government response is essentially that the target is on their own.[18]

The MTS represents a concentration of cyber risk. In this context, risk is a function of system vulnerabilities, exploits that can take advantage of these vulnerabilities, and threat actors willing to use these exploits to cause harm. The *Vulnerabilities Trump Threats* maxim says that a cyberdefender needs to concentrate on vulnerabilities in their systems because these are internal and manageable, rather than focusing on threats because those are external and largely unknown.[19]

One example of a significant vulnerability to the MTS are the systems used for positioning, navigation, and timing (PNT), and situational awareness at sea. The primary source for PNT in maritime—in fact, the primary timing source for all U.S. critical infrastructures—is the Global Positioning System (GPS). GPS has been a victim of jamming (i.e., blocking of the signal) and spoofing (i.e., sending false timing and location information) for some years.[20] The Automatic Identification System (AIS) is used for maritime situational awareness. AIS information will be incorrect

[14] See the Defense Advanced Research Projects Agency OoT Web page at https://oceanofthings.darpa.mil/

[15] Marr, B. (2018, September 2). What is Industry 4.0? Here's a Super Easy Explanation for Anyone. *Forbes*. https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/; Reni, A., Hidayat, S., Bhawika, G.W., Ratnawati, E, & Nguyen, P.T. (2020, February 20). Maritime Technology and the Industrial Revolution. *Journal of Environmental Treatment Techniques, 8*(1), 210–213.

[16] Kosowatz, J. (2019, September 2). Sailing Towards Autonomy: Future of Self-Driving Cargo Ships. *The American Society of Mechanical Engineers*. https://www.asme.org/topics-resources/content/sailing-toward-autonomy-future-of-self-driving-cargo-ships

[17] Maritime Cyber Attacks Increase by 900% in Three Years. (2020, July 29). *Vanguard*. https://www.vanguardngr.com/2020/07/maritime-cyber-attacks-increase-by-900-in-three-years/; Report: Maritime Cyberattacks Up by 400 Percent. (2020, June 4). *The Maritime Executive*. https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent

[18] Why Do We Call it Cyber CRIME? Gary Warner at TEDxBirmingham 2014. (2014, March 1). https://www.youtube.com/watch?v=MPMr5jPwA7I

[19] Johnston, R.G. (2020, July). Security Maxims. *Right Brain Sekurity*. http://rbsekurity.com/Papers/Johnston__Security__Maxims.pdf

[20] Balduzzi, M., Wilhoit, K., & Pasta, A. (2014, December). A Security Evaluation of AIS. Trend Micro Research Paper. https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf; Center for Advanced Defense Studies (C4ADS). (2019). *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria*. https://www.c4reports.org/aboveusonlystars; U.S. Coast Guard (USCG). (2021, April 22). Worldwide Navigational Warnings Service. Marine Safety Information Bulletin (MSIB 05–21). https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2021/MSIB__21-05__Worldwide NavigationalWarningsService.pdf

when bogus GPS information has been received by a ship or an attacker can insert false information into the system. Although it is of some value to know the Threat Actors that might employ GPS or AIS spoofing, it is more important to fix or augment the systems to be more resistant to the attacks in the first place. This is an important role for government to play.

Unfortunately, regulators, administrators, and managers usually respond to threats rather than vulnerabilities. New laws and funding sources do not appear merely because a new vulnerability is discovered but rather once a new threat is identified. This is a mindset that needs to be re-examined.

We need the federal government to take a more active role in the cyberdefense not only of the MTS, but of transportation as a whole. Industry self-inspection has been cited as partial causes for the Boeing 737 Max[21] and EL FARO[22] disasters. While neither of those were cybersecurity incidents, both speak to the reduced involvement in the inspection and compliance process by responsible government agencies. This is not a question of big government versus small government, but a close examination of the issues in order to determine the appropriate level of government. In general, the level of an agency's authority should match the level of its responsibility. The USCG has the regulatory responsibility to protect the MTS from all forms of threat, in both real space and cyberspace. They must be provided with the necessary resources to carry out this vital mission.

Another critical defensive tactic is related to intelligence sharing. Cyber-related incidents, reports, and analysis must not only be freely shared amongst all of the government regulatory agencies, but between all MTS stakeholders that wish to participate. The maritime entities most at risk are the small shipping lines, ports, cargo handlers, and manufacturers that do not have the financial assets to have a large information security team or join one of the industry information sharing organizations. A central maritime security information sharing center—such as Singapore's Information Fusion Centre[23]—would go a long way to assisting the MTS in protecting itself against new and emerging threats in both real space and cyberspace.[24]

Maritime regulators also need to prepare better reporting requirements about cyber-related events for information flow to the Department of Homeland Security (DHS), the Cyber and Infrastructure Security Agency (CISA), and/or USCG, as well as a central location for such reporting, and clearinghouse and reporting distribution center for the industry.

Additionally, we have to recognize cybersecurity as a safety issue in the maritime environment. The maritime industry prides itself on it focus—and relatively strong record—on safety. But cyber safe environments require excellent cybersecurity hygiene on the part of the users and that requires regular training for all members of the MTS.[25]

[21] Schwellenbach, N. & Stodder, E. (2019, March 28). How the FAA Ceded Aviation Safety Oversight to Boeing. *Project on Government Oversight (POGO)*. https://www.pogo.org/analysis/2019/03/how-the-faa-ceded-aviation-safety-oversight-to-boeing/; U.S. Department of Transportation. (2015, October 15). *FAA Lacks an Effective Staffing Model and Risk-Based Oversight Process for Organization Designation Authorization*. Office of the Inspector General, Audit Report No. AV–2016–001. https://www.oig.dot.gov/sites/default/files/FAA%20Oversight%20of%20ODA%20Final%20Report%5E10-15-15.pdf

[22] National Transportation Safety Board. (2017,December 12). Sinking of US Cargo Vessel SS *El Faro*—Atlantic Ocean, Northeast of Acklins and Crooked Island, Bahamas, October 1, 2015. NTSB Marine Accident Report (MAR)–17/01, PB2018–100342, Notation 57238. https://www.nhc.noaa.gov/pdf/ElFaro-NTSB-full.pdf; United States Government Accountability Office (GAO). (2020, April). *VESSEL SAFETY: The Coast Guard Conducts Recurrent Inspections and Has Issued Guidance to Address Emergency Preparedness*. Report to Congressional Committees, GAO–20–459. https://www.gao.gov/assets/710/705785.pdf

[23] https://www.ifc.org.sg

[24] U.S. Coast Guard. (2021, August). *CYBER STRATEGIC OUTLOOK: The United States Coast Guard's Vision To Protect and Operate in Cyberspace*. https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf; U.S. Department of Homeland Security (DHS). (2016, October). *Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community*. https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

[25] Canepa, M., Ballini, FD. Dalaklis, D., & Vakili, S. (2021, March). Assessing the Effectiveness of Cybersecurity Training and Raising Awareness Within the Maritime Domain. In *Proceedings of the 15th International Technology, Education and Development (INTED) Conference*. http://dx.doi.org/10.21125/inted.2021.0726; Tam, K., & Jones, K. (2019). Factors Affecting Cyber Risk in Maritime. In *Proceedings of 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Oxford, UK, 2019, 1–8. https://www.researchgate.net/profile/Kimberly-Tam/publication/334051022__Factors__Affecting__

Continued

Finally, the designers and builders of maritime systems that depend upon any ICT or OT equipment need to have a mindset of *security by design*. All too often, systems are protected by layering security on during implementation rather than designing security into every device. Indeed, a vessel network composed of a collection of secure devices might itself not be secure; the network must be designed with security in mind.

CONCLUSION

The United States is very much a maritime nation where our food security, energy security, economic security, homeland security, and national security are dependent upon the seas. The maritime transportation sector is broad, diverse, and global so that, while international cooperation is essential, central management is impossible. Cyber vulnerabilities are as plentiful in the maritime sector as in the non-maritime world and provide unique threats to the industry. Both the commercial maritime industry and our military maritime interests demand our proactive response to this ongoing threat.[26]

The *National Maritime Cybersecurity Plan* was a clarion call about a significant threat facing this country. Our report, *Raising the Colors*, was a first step at trying to provide a tactical approach to addressing that threat. We have to continue pushing forward to address this critical issue.

Thank you again for the opportunity to provide testimony and information for the committee. I look forward to your questions and further discussion.

Mr. DEFAZIO. Thank you. With that, I will begin with questions to the panel.

A major point of contention is—I guess there are two, it is two issues.

One is reporting. And, for instance, Mr. Belcher, you talked about 30 percent of transit systems you surveyed had been the victim of cybersecurity, but they never reported the incident. So, that is one issue, is reporting, whether or not reporting should be mandatory. And what is the value of people reporting? I would assume that there are many things to be learned when someone reports, and we properly analyze, and they report what the attack was. It may well benefit others in their same sector of industry, whichever one of these sectors we are talking about.

And secondly is the idea of whether or not there should be a mandate. Now, I understand concerns about a very prescriptive mandate. But a mandate that all critical sector organizations have some sort of cybersecurity officer, or at least designee, if they have very few employees among their staff, and that they are sort of bird-dogging the people within their organization.

So, I guess I would like briefly, if we could, each member of the panel to just quickly opine on the value of mandatory reporting, and a requirement that doesn't have to be totally prescriptive, but you have to have someone designated for cybersecurity within your organization if you are involved in critical infrastructure.

So, any member of the panel who wishes to respond briefly would be appreciated.

Mr. BELCHER. I am happy to start. I am very comfortable with mandatory reporting, and very comfortable with a designated cy-

Cyber__Risk__in__Maritime/links/5e60e9cb299bf182deea63a6/Factors-Affecting-Cyber-Risk-in-Maritime.pdf

[26] Demchak, C.C., and Thomas, M.L. (2021, October 15). Can't Sail Away from Cyber Attacks: 'Sea-Hacking' from Land. *War on the Rocks*. https://warontherocks.com/2021/10/cant-sail-away-from-cyber-attacks-sea-hacking-from-land/; Zorri, D.M., & Kessler, G.C. (2021, September 8). Cyber Threats and Choke Points: How Adversaries are Leveraging Maritime Cyber Vulnerabilities for Advantage in Irregular Warfare. *Modern War Institute at West Point*. https://mwi.usma.edu/cyber-threats-and-choke-points-how-adversaries-are-leveraging-maritime-cyber-vulnerabilities-for-advantage-in-irregular-warfare/

bersecurity official. I recognize that—I mean, I work with a large number of very small and mid-sized transit organizations that do not have cybersecurity professionals. In fact, they are lucky to have IT professionals.

Nevertheless, this is an important issue that is part of something that they have to do. It is part of an enterprise management issue. And I think one of the things that we have to do, as we look at managing organizations, is to make cybersecurity just part of the enterprise management, the management of risk, and the management of security of the organization.

And so, identifying somebody, whether it is an employee or a consultant that is there and that can engage with TSA on a 24-hour basis, I think, is absolutely essential.

Mr. DEFAZIO. OK, thank you. Thank you, Mr. Belcher.

Anyone from any of the other sectors who wish to respond?

Mr. STEPHENS. Chairman, this is Michael Stephens from Tampa International. I would echo that sentiment.

While I don't think that there is a problem with mandates, we are not unfamiliar with mandates for reporting in the aviation sector. For example, if you have an airfield incursion that is not authorized, we have to report that. If you have an [inaudible] airside incursion, we have to report that. So, there is not a problem with reporting and mandates for reporting.

The problem becomes, though, what are we reporting? Part of the TSA proposed guidance that we have been providing comments to is very, very broad-based, in terms of what is being required to be reported. And information just for the sake of information is not necessarily a good thing, because it leads to information overload, and white noise, and a lot of times gets ignored. So, I think, while reporting mandates are appropriate, we have to tailor those to make sure that they are actionable, as I said in my opening comment.

And then, secondly, I do believe that, if we have mandatory minimum standards, baseline standards for cyber resilience, a lot of those types of things that are falling through the cracks—reporting, identification, mitigation strategies—will start to be resolved.

So, I think that both of those things are things that we need to do, but we need to do them in the right way.

Mr. DEFAZIO. Thank you, that was very valuable comment on too much reporting of things that would not be of value.

And just——

Mr. FARMER. And Mr. Chairman, may I add to that, please?

Mr. DEFAZIO. Sure, quickly, yes.

Mr. FARMER. Thank you, sir. The key challenge here with the reporting mandate that has been presented to us by TSA is just what Mr. Stephens highlighted.

And CISA Director Jen Easterly, she has made a point to emphasize that her agency is interested in signals, not noise. And that is what we have been providing in the rail sector for several years, dating back at least to the 2014–2015 timeframe. We are providing them with information products that delineate what happened, what a railroad observed, what the indicators were, and what they did about it, in terms of a security response, with recommendations that we share widely on measures that other railroads can take.

And additionally, as I indicated in the opening statement, we provide thoroughly to our partners, and other transportation modes and sectors, and to Government.

And on the appointment of the coordinator, again, we don't object to that. We have had [inaudible] coordinators for an extended period of time. But the draft TSA directive has a significant limitation. It requires U.S. citizenship. And the challenge there is we have two major operations, railroads that operate from Canada into the United States, CN and Canadian Pacific. And they are going to have an extremely difficult time meeting that standard, because their network operations, their expertise, is in Canada.

What is really disconcerting here is we have put a lot of effort in with TSA in working collaboratively to overcome objections to a sharing of classified information with those cleared staff in Canada, with clearances from Canadian Government. And so, we just don't understand the basis for that restriction, because it is really setting up two major freight railroads for failure in meeting the future directive. Thank you.

Mr. DEFAZIO. OK, thank you. That was very helpful. My time is expired, and now I recognize Mr. Crawford.

Mr. CRAWFORD. Thank you, Mr. Chairman. This month it was reported that TSA will soon issue mandatory security directives for rail transit and, potentially, aviation.

Mr. Farmer, how much stakeholder engagement has TSA conducted in advance of their release?

Mr. FARMER. So, there have been two outreaches from TSA, where we have been provided drafts of the directives to provide comments. In each case, they were done on a 72-hour response timeline.

Mr. CRAWFORD. Is that typical for TSA?

Mr. FARMER. When the decision is taken to issue a security directive, the timelines are narrow.

We believe that there is a clear opportunity here, consistent with the President's National Security Memorandum, to collaborate on the content of the directives, so that the disruptive effects that we see can be alleviated and avoided.

Mr. CRAWFORD. The previous mandatory directives for pipelines followed the Colonial Pipeline ransomware attack, if you recall. What incident or security threats are necessitating a mandatory security directive for freight, rail, or transit?

Mr. FARMER. Sir, we have not been apprised of any imminent or elevated threat to railroads or rail transit agencies as a justification for this emergency action. Nor are railroads seeing the sort of activity that would be indicative of an elevated, specific, persistent threat to rail.

Mr. CRAWFORD. If you were apprised of such a threat, how would that be communicated to you?

Mr. FARMER. We have well-established procedures with TSA for sharing information. We have quarterly teleconferences with their surface division. There is a group called the Surface Transportation Security Advisory Committee that meets quarterly. We have our Industry Cybersecurity Committee. The Rail Information Security Committee convenes twice a month. So, there are ample opportunities to communicate with us on an unclassified level.

But we have taken it a step further. We have worked with the agency to establish a secure video teleconference network, so that they can deliver classified presentations up to the secret level nationally, so that railroad cyber leads can participate from locations in their headquarters' areas, and——

Mr. CRAWFORD. So, there is a robust exchange protocol already in place?

Mr. FARMER. Yes, sir, we have devoted extensive efforts to creating a range of options to communicate information, both unclassified and classified, up to the secret level.

Mr. CRAWFORD. So, you are confident that, if there were some threats to rail, you would be warned in a timely manner, you would be aware of it, and that those communications channels are open and available?

Mr. FARMER. Yes, sir.

Mr. CRAWFORD. And you don't see any threat, or have not been apprised of any threat that, to your mind, would warrant the mandatory security directive that is being proposed by TSA right now?

Mr. FARMER. Yes, sir. We have not been apprised of the threat that is the justification for this emergency action through any of those communications channels I have referenced. I am based in Washington, DC. My colleague at the American Public Transportation Association, as well. We can be read in at the top-secret level. That initiative has not been taken.

In fairness to TSA, they have referenced that there is a briefing being developed, and that it will be given. It has not yet been scheduled.

But our concern is we have cybersecurity leads who, as part of our industry protocol, our emphasis on cybersecurity, every quarter, at board of directors meetings, cybersecurity is a recurring subject, and they are being asked questions about these directives, what the driving impetus is, and they can't answer them because we have not been provided that detail.

Mr. CRAWFORD. Let me ask you how you think the security directive might interact with what you already have in place, your current rail cybersecurity measures or reporting systems.

Mr. FARMER. On the reporting systems, sir, the key challenge is the breadth of the definition of "cybersecurity incident" is such that it is going to overwhelm what Director Easterly at CISA wants to accomplish, and that is to get signals that are indications of potential cybersecurity concerns, significant cybersecurity concerns, as opposed to a lot of noise.

Mr. CRAWFORD. And you are afraid that this might just, basically, create more noise, and it might be more difficult to catch those signals.

Mr. FARMER. Yes, sir. And I think the challenge is—and it is twofold—it is the breadth of the reporting protocol; "cybersecurity incident" is widely defined.

Secondly, the timeline. Initially, it was 12 hours, based on input we provided. It has been extended to 24, and I think many cybersecurity experts would tell you that it is very difficult in that first 24-hour period to have insight into whether what is taking place is actually significant, from a cybersecurity perspective.

We have got the right experts in place, and they can provide the right information.

Mr. CRAWFORD. Yes, just real quick in the time I have remaining, can you give us some ideas of some of the cybersecurity practices that you have already adopted and implemented in rail recently?

Mr. FARMER. Yes, sir. And the efforts in this area go back more than two decades. That is how long we have had a cybersecurity focus committee. And it is a continuous analysis process of what the prevailing threats are, and what we can be doing effectively to address them.

The committee provides a collaborative approach. We share information on cybersecurity concerns. We share information on effective practices. The chairman, in his opening remarks, outlined a series of actions: multifactor authentication, the conduct of assessments, action on those assessments, strong passwords. Those fundamental measures are being taken.

I think, most importantly, no one is resting on laurels. We take the NIST cybersecurity framework, and we assess our cybersecurity posture against that framework at least every 2 years. And, based on the lessons learned, we focus on enhancing our practices. And all the effort we are devoting to information sharing is designed to make sure the right people have what they need and can take the right measures to narrow their risk profile and prevent harm from happening.

Mr. CRAWFORD. Thank you, Mr. Farmer. My time has expired.

Ms. NORTON [presiding]. Thank you very much. I now recognize myself for 5 minutes.

Cybersecurity presents a fairly unique challenge to Members of Congress: we're supposed to do something about problems, recognizing, however, that there is no cure-all for cybersecurity.

But Mr. Belcher, you discussed the need for carrots and sticks to ensure the necessary resources are utilized by transit and their agencies. You also mentioned the need for the Federal Transit Administration to require organizations to adopt and implement minimum cybersecurity standards prior to receiving Federal funding.

I would like you to briefly explain the specific carrots and sticks you would recommend the Federal Government use to get transit organizations to the minimum cybersecurity standards you see as urgently needed, Mr. Belcher.

Mr. BELCHER. Sure. I would be happy to. So, Mr. Farmer described a situation in the rail industry that is a little bit different from the situation in the transit industry.

The transit industry has over 3,000 transit operators, public transit operators, that range in size and sophistication. And my experience with them is that they are desperate for regulation, and they are desperate to be told what to do. This is really an area where they don't know what to do. And in fact, just yesterday I was speaking, and I had a transit CEO ask me what they needed to do to secure their Zoom calls. So that was the level of sophistication that they have when it comes to cybersecurity. And this was a CEO. So, they get the same briefings that Mr. Farmer talked about, but they don't have the resources to do it.

So, you have a couple of things. You have a series of agencies that are underresourced, and that have to manage, and then, through the pandemic, have found their resources have been stretched further. And so, they have a whole new series of challenges facing them.

So, the carrots are to provide funds to support them, and to provide them with tools to support them. And those tools are contractual language, the tools are to provide them with cybersecurity assessments. The large transit operators do get resources, do get Federal funding, do get support from TSA to do assessments, to do audits, to do cybersecurity plans, but the vast unwashed do not. The small to midsized transit agencies do not get funds for that, do not get that level of support. So, those are the ones who really need it desperately. They need that help.

And as it relates to what you can do with respect to the agencies, I think you need to have the—before a transit agency receives Federal money from the FTA, they need to certify that they have a cybersecurity plan in place, because we found that almost 50 percent of the agencies do not have a basic cybersecurity plan in place.

Ms. NORTON. Yes, well, that is really helpful, Mr. Belcher. I am really interested in this issue.

You spoke about cyberattacks that already have involved transit agencies in cities like New York, and places like Massachusetts, Pennsylvania, Vancouver. Now, I represent the District of Columbia. Many Members of Congress and their staff use transit agencies here, so these cyber effects could have very specific and harmful effects on Congress itself.

Can you discuss how the attacks have impacted average citizens?

Mr. BELCHER. Sure.

Ms. NORTON. For example, have these disruptions, and the huge increase, a 186-percent increase in ransomware attacks on the transportation sector, generally, shown us the attack on the average person using transportation?

Mr. BELCHER. Yes, in a number of ways. One example is at SEPTA, which had a major ransomware attack last year, or earlier this year. SEPTA was forced to shut down its public communication system, so it was not able to communicate with its customers for almost 2 months, digitally.

A large percentage of its customers utilize mobile applications to determine when their bus or their train was going to arrive, and how to access it, and they pay for it with a mobile application. They couldn't do that any longer. Many customers go and look on a digital screen to see when their bus is going to arrive. They couldn't do that any longer. They had to go back to paper schedules, and so they were forced to do that. So that is one example.

A second example is that, when a transit agency has to pay out a ransom, which many of them do, first of all, they may be insured once. Once they pay out a ransomware, the likelihood that they are going to get insurance a second time is highly unlikely. So, that is going to increase the cost of operations. So, there are a variety of ways that people are impacted.

And then, third, it can impact the operations. The main things we are concerned about right now are not the things that you would think about, in terms of, like, the movie, "Speed." That is what we all think about, is something is going to take over, and take over a bus, or take over a train autonomously. That is not why CEOs stay up at night—they are worried about somebody taking over PII, the customers' or the employees' personal information, or the operating system. And those are the things that hackers are getting a hold of and that impact passengers.

Ms. NORTON. Well, thank you very much, Mr. Belcher.

I next call on Mr. Gibbs.

Mr. GIBBS. Thank you, Madam Chair.

Mr. Kessler, I want to ask some questions here about the maritime industry. Is it inherently more difficult protecting IT communications systems that are both worldwide and require ship-to-shore communications?

Mr. KESSLER. Are you asking if it is harder to secure those?

Mr. GIBBS. Well, I am trying to understand the complications of when you have got a shipping company that is worldwide, that has ship-to-shore communications, do they establish firewalls in their land base to the ships and just how does all that relate, and how vulnerable are they to cyberattacks, I guess.

Mr. KESSLER. Well, they are as vulnerable as any other remote communications.

One of the mechanisms that are used widely to talk to ships is by VSAT, very small aperture terminals. And there have been any number of studies and demonstrations, particularly at the hacker conferences, about the fact that, when the communication is coming back down, it is not directed at a ship, or even a place on Earth. It is going to a total footprint on Earth, and that makes it very easy for people to intercept those communications, which are, in a large way, unencrypted.

And so again, the demonstrations at the hacker conferences have shown all sorts of very interesting communications coming between ships and back to shipping headquarters, or just in internet access for passengers that are just sending emails that are also invariably unencrypted. So that is one of the unique communications problems we have on ships.

Certainly, the ships themselves are using firewalls. What I believe we are going to see ongoing, as we get more and more autonomous vessels and remote-controlled vessels, is the fact that, if I am able to remotely access a vessel in order to provide control, it is naive to believe that nobody else could somehow also take over that communication.

Furthermore, when I get fully autonomous vessels, that means we are going to have to change the collision regulations or the maritime rules of the road. For example, you are required to have a lookout on board a vessel. Well, if I have a fully autonomous vessel, I can't have a lookout. So instead, what I am going to do is have a whole bunch of cameras, and they are going to be remotely monitored. That will suffice for my lookout.

Well, again, if I can remotely access the cameras, then it would be naive to believe that nobody else could break in and look at the cameras, possibly change the contrast setting on a camera so that the camera is now blind.

Mr. GIBBS. OK, let me——

Mr. KESSLER. So those are some of the issues——

Mr. GIBBS. Let me—yes, let me just interrupt you, I am running out of time. Autonomous vessels, that is more in the future a little bit.

But I also was concerned—we had the malware attack on Maersk in 2017. Can you tell us what specific steps maybe have been taken by the shipping industry to mitigate future attacks?

And have we been more vulnerable with the crisis of the supply chain, with all the ships being idled and backlogged?

Mr. KESSLER. Well, very quickly, Maersk, of course, was whacked quite hard by a ransomware attack for which they were not a target. They were merely susceptible. And I believe that that was, though, a wakeup alarm for the maritime industry.

However, as I said in my testimony, there were at least a dozen well-known attacks in 2020 and 2021 that were directed at the maritime industry. There have been at least two maritime entities that have been hit by two ransomware campaigns during that period of time. So, while the awareness has gone up, and there has been positive responses, it seems that it continues to be an ongoing problem.

Mr. GIBBS. So, we haven't really gotten any satisfactory solutions to address it? Still kind of really vulnerable, is that what——

Mr. KESSLER. I think that the satisfactory solutions have not been implemented, and some of those things have been actually mentioned with some of the other sector speakers, as well.

A lot of it is awareness training for everybody in the MTS, because so many of these attacks occur because humans are socially engineered.

Mr. GIBBS. OK.

Mr. KESSLER. But at the same time, I would like to say we have to stop throwing our hands up in the air and saying, "oh my goodness, it is the users," because that implies that we are giving the users secure systems, to begin with, that the people are somehow screwing up.

The fact is we are using operating systems that are not secure. We have applications that are not secure. And you only have to look at the number of patches that are coming out constantly to demonstrate that we are working with systems that are not as secure as they should be, which gives the users not really a chance.

Mr. GIBBS. Thank you very much. I yield back my time. Thank you.

Ms. NORTON. I now recognize Mr. Larsen for 5 minutes.

Mr. LARSEN. Thank you, Madam Chair.

My first question is for Mr. Stephens, if you could prepare, Mr. Stephens.

The U.S. aviation sector is very complex. It is made up of various entities and stakeholders responsible for different aspects of it. Have you considered how the complexity of the U.S. aviation system, though, then makes that system more vulnerable to cyberattacks, or less vulnerable because of the complexity?

How do you approach that?

Mr. STEPHENS. Oh, that is an excellent question, Congressman. In a way, I think it makes it more vulnerable, and here is why. I will give you an example.

The MTA attack that was mentioned earlier, it affects New York, it could create delays. It can create some safety risks. But it doesn't impact, maybe, the metropolitan transportation system in San Francisco. However, a cyberattack in New York at JFK, or one of the other major airports in that area, would very well not only impact, because of the connectivity, the airport in San Francisco, but across the globe, potentially. So, it is much more global, I think, in scope and approach.

Also, I think you have so many interdependent pieces. You have air traffic control systems, particularly the shift from terrestrial-based air traffic control management to satellite-based air traffic control management with NextGen. There are significant issues with the interference and cyber hacking, potentially, of signals and satellites that create the position awareness for those aircrafts and for controllers to be able to control those aircraft.

In my previous life I was an air traffic controller in the Air Force, and I will tell you being able to have positive control in everything in your airspace is of paramount importance, for obvious reasons. So, for those reasons I do believe that there is greater complexity because there are more interoperating systems, and there is a much broader landscape to cover, geographically speaking.

Mr. LARSEN. Does the FCC's decision on 5G, where the aviation sector expressed concerns about the size of the buffer between midband wasn't wide enough to protect aviation, do you see that as an additional vulnerability, or is that a separate issue for the aviation sector?

Mr. STEPHENS. I see that as an additional vulnerability. Anything that potentially impacts the safe navigation in our airspace, whether it is from 5G, or whether it is interference with global positioning satellites, or any other type of malicious intrusion or unintentional intrusion becomes a huge issue. It is a force multiplier.

And our colleagues from the maritime space and the surface transportation, they are all dealing with the same things. However, it is a little bit different when you are cruising at 500 miles per hour and 40,000 feet. You don't have that much room for error. And that isn't being said to minimize the situation with any of the other represented sectors. However, the consequences of error in aviation, potentially, are significantly greater. So, anything that impedes the safe flow in that airspace is a huge issue that we all have to make sure that we are coordinating on.

Mr. LARSEN. Yes, thank you. I want to shift to Ms. Samford, please, if you could prepare, just to ask you about the Incident Command System for Industrial Control Systems, and the model for the National Incident Management System. You discussed applying that in private-sector response, mainly.

But is that system adaptable to all industries? Is it a template you can just pick up and put down? Or do you anticipate, within the transportation sector, it would have to be modified industry by industry?

Ms. SAMFORD. That is a wonderful question, and thank you for it, Congressman Larsen.

Incident Command System is used globally. It was recently endorsed by the United Nations, so it is really a model. It is a framework that sits on top of existing plans. So, it is really industry or sector agnostic.

Mr. LARSEN. Yes, OK. I am not sure the U.N. endorsement would please some of the Members in the U.S. House, but that is fine.

Back to Mr. Stephens briefly, then. I have got 30 seconds, total. How can Congress incentivize the aviation sector to address cybersecurity issues? Are there specific points that we ought to do, other than what you have mentioned in your testimony?

Mr. STEPHENS. I think there are some specific things, Congressman. Very quickly, in the interest of time, I think there needs to be more investment, first of all. If you look at the TSA proposed guidance out there that requires all of these different things, they are good things. They are headed, notionally, in the right direction. But without investment, without developing the capacity and capability and workforce, they are just prescriptions that can't really be met.

When you see one airport, you have only seen one airport. They are different in size and scope and resources. So, every airport that is a commercial airport wouldn't be able to achieve that. So, if I had to give you one thing, it would be more focused investment, and talent development, as well as resources to meet any prescriptions that are set down from Congress or TSA.

Mr. LARSEN. Thank you very much.

Ms. NORTON. Next, I call on Mr. Webster for 5 minutes.

Mr. WEBSTER. Thank you, Madam Chair.

Dr. Kessler, my first question is to you. You mentioned the unique—maybe the unique—problems with autonomous shipping. You mentioned one example, and that was a lookout. Are there other things that would be unique—and maybe bring on new hazards and so forth, as far as cybersecurity—to the area of autonomous shipping?

Mr. KESSLER. There are some things with the autonomous vessels, but that also actually impact the nonautonomous vessels.

Autonomous vessels, of course, are going to be highly reliant on position navigation and timing systems, which is to say GPS. They are also highly reliant on situational awareness systems, such as the automatic ID system that allows vessels that are in proximity to identify themselves to other vessels in terms, not just of location, but also, of course, heading, rate of turn, destination, and speed, all that kind of stuff. I mean much more than, for example, radar would give you. Those systems are also highly unsecure.

Mr. Stephens referred to a little bit about the importance that aviation has for GPS. Maritime also has the same reliance, and that reliance, once we get into the near-coastal waters, is particularly important. As an example, if I can somehow spoof your GPS signal, and make you go off course by 100 meters or so in the open ocean, well, that is not good, but it is not terrible. If I cause you to go 100 meters off course in Kill Van Kull, as you are going into the Port of New York and New Jersey, that is a big problem, because I can now block the entire port. So that is one of the issues that we have.

The situational awareness system that I mentioned, AIS, also is not terribly secure, and can be easily spoofed. And we have seen some—you know, the more egregious demonstrations of that in the Black Sea during the NATO exercises last June.

But again, going back to the autonomous vessels, it is not just the lookouts, it is also the entire—being able to control the vessel. And if I can get something to go off course, obviously, that is, I think, a big potential problem with those vessels.

Mr. WEBSTER. Thank you very much.

Mr. Stephens, can you tell me, at Tampa International Airport, I guess you had mentioned that there have been great strides made, as far as cybersecurity. But on the other hand, you picked up some strides on the other side, from attacks and so forth. Can you elaborate on that any more?

Mr. STEPHENS. Congressman, yes. What I will tell you is that most airports, particularly your large hub airports, which are your 30 largest by traffic, passenger traffic airports, are under attack constantly. We at Tampa International probably defend about 3 million malicious cybersecurity attempts at our network every year.

And while we, here at Tampa International, have done a pretty good job by most standards, we have adopted the NIST standard, and we also have adopted aspects of another standard called COBIT. We still are looking at making sure—how can we harden our network? How can we train our employees to recognize these threats and attacks?

And the problem with cybersecurity defense: we have to be right almost 100 percent of the time. The bad guys don't have to be right all the time. They have to be able to get at us one good time, and you can really disrupt some things.

So, in summary, it is just an enormous, enormous challenge out there. The good thing is, though, that we don't do it alone. Everything, from CISA to TSA to the FBI and all of our partners, there is great information sharing and exchange, as Mr. Farmer alluded to in the rail industry. And we do the same thing in aviation by mandate.

So, we are not strangers to mandatory information sharing. Again, as I stated before, it is the nature and the quality of what we share that is really going to make the difference.

Mr. WEBSTER. USF has—out of the university system, the University of South Florida has been one of the designated cybersecurity hotspots. Are they part of your team, too?

Mr. STEPHENS. That is a great question. We do a lot of work with the cybersecurity groups around here, particularly coming out of USF. They hold a fantastic conference. We send some of our folks to that conference to participate. But again, I think we can do even more, maybe getting them involved in more tabletop exercises, and things of that nature. But we do participate with those local groups such as USF.

Mr. WEBSTER. Thank you very much. I yield back.

Ms. NORTON. I now recognize Mr. Carson for 5 minutes.

Mr. CARSON. Thank you, Madam Chair. I really appreciate it.

As a former law enforcement officer who worked at our Indiana Intelligence Fusion Center, I am always concerned about making sure that information sharing is strong, and I know how critical it is for Federal officers to share timely and detailed information with local and State partners.

Tell us, what is working well? What needs to be improved? And what do you recommend to improve the flow of information to strengthen cybersecurity for transportation, and even infrastructure?

Mr. KESSLER. Well, if I can say a few words about maritime—and I will keep this short—there is a very strong reporting requirement, at least within U.S. waters, and possibly even with all U.S.-flagged vessels, the few that we have, that they report on any safety issue to the U.S. Coast Guard.

We are only now really beginning to view cybersecurity as a safety issue. And so, while the mechanism in place—at least, again, in maritime and U.S. waters—to provide information to the Coast Guard, we need to have some better reporting structure and requirements for those cybersecurity issues to get reported up. There is a lot of work being done that all of the ports in the United States need to have a facility security plan, and now they have to have a cybersecurity amendment to that plan. So, the process is moving, albeit a little bit slowly.

Mr. BELCHER. I would say, from the transit perspective, there is a lot of communication that comes from the major transit associations, particularly APTA. They have a number of committees that communicate with their members, both large and small, a lot of standard development.

AASHTO also has a committee that works largely with the smaller and rural transit associations. So, there is a lot of communication in that regard.

And then TSA works closely with those associations.

And I think what you are starting to see is greater engagement by this administration in cybersecurity. And as a result, you are starting to see greater and greater engagement by the administration, both—obviously, from DHS, but now even at the Department of Transportation level with the industry. And that is something that is new.

Mr. CARSON. Thank you——

Mr. FARMER. Tom Farmer, if I could, sir.

Mr. CARSON. Oh.

Mr. FARMER. On the point of information sharing, what is working well among sectors in transportation is cross-sector sharing through the different information sharing and analysis centers for aviation, oil and natural gas, for public transportation, the railway network that we manage. And that has been very helpful in organizations understanding what others are seeing in transportation, from a cybersecurity perspective, and that gives insight.

If you are considering attackers, they likely haven't gone after one transportation entity. They are likely going among several to try to find opportunities. And so that sharing of indicators of cybersecurity concern can be very valuable for our awareness.

I think, importantly for the Cybersecurity and Infrastructure Security Agency, it is those sorts of signals that can help them determine whether what is happening is indicative of a pattern, of trends of a potential developing threat that merits attention. So that [inaudible] is working very well.

And there is a group that the TSA Administrator has appointed called the Surface Transportation Security Advisory Committee. It is a direction that Congress gave in the TSA Modernization Act of 2018, and it comprises representatives of each of the surface transportation modes: security support experts, State and local government representatives. And that committee earlier this year made 18 unanimous recommendations to the TSA Administrator, all of which he has accepted. Four of them focus on cybersecurity information sharing, with the aim of building this early notification network of sharing among sectors of what they are seeing, so that their colleagues can understand what the potential threats are. Thank you.

Mr. CARSON. Thank you. I yield back, Madam Chair.

Ms. NORTON. The gentleman yields back. I call on Mr. Massie for 5 minutes.

Mr. MASSIE. Thank you, Madam Chairwoman. I find this hearing somewhat terrifying. It is based on the premise that Federal involvement in ensuring cybersecurity in the private sector is either necessary or sufficient. It is not either of those things. And so, I am worried.

I mean, asking this committee to come up with standards for platforms in cybersecurity is a little bit like asking my cattle to write a term paper on one of Shakespeare's works. I mean, we are just not qualified to do it, and I am going to include myself in that. I have an undergraduate degree in electrical engineering and computer science from MIT. All that qualifies me to do is to know what I don't know. And I am terrified at what we don't know.

If some legislation comes out of this—and maybe it is already written, probably already written—if it is going to be written, it is going to be written by the vendors, who continuously fail to protect the assets of the Federal Government and the private sector.

And so, with that, I want to ask Mr. Kessler, can you tell us what a zero trust architecture solution is, and why that might have advantages over some of the other architectures in the context of cybersecurity?

Mr. KESSLER. Well, actually, there were a number of things that you said that—since your background—well, I didn't go to MIT, but—matches mine.

So, the zero trust architecture, it is basically, in my view, a relatively recent buzzword for trying to put together the idea that I start out with not trusting any entity with whom I communicate. And so, trust has to be designated. And it is a way of controlling access, not only to the fact that you and I can communicate, but, in fact, what we are going to communicate about, what you have access to. And again, I don't give you access to anything except that which I have specifically given you access.

However, you mention a point that I would like to say a few words about.

Mr. MASSIE. What—OK. If I have time at the end, I will allow you to do that.

Mr. KESSLER. OK, all right.

Mr. MASSIE. The zero trust architecture, is it possible to build that on top of, say, a Microsoft operating system?

Mr. KESSLER. I believe you can, at the application level. I will keep it there. Yes, I believe you could.

Mr. MASSIE. OK. I believe you can't, because if you are using the Microsoft operating system, you are getting updates from a vendor that you implicitly have to trust, or else the operating system does not work.

You are also getting an operating system that you can't audit. No audit is possible. Microsoft would not give you that level of access to know that—if you have a platform.

But I will allow you the application itself might be zero trust, and I think that was your answer. You are, obviously, more knowledgeable in this than me. I am just trying to point out to everybody else that everything underneath of that application cannot be trusted, because you can't audit it.

And so, I want to go on and just say, Mr. Belcher, you talked about the vast unwashed, and you were shocked that a CEO of a transit company didn't know how to secure a Zoom meeting. Would you be willing to put $1 million in bond, and we hire a hacker, and see if you can protect a Zoom meeting?

Mr. BELCHER. No.

Mr. MASSIE. OK, I wouldn't, either, because, from a directed, focused attack, it is really not even possible to guarantee that.

Ms. Samford, you use the words "consistency," "interoperability," "uniform," and "coordinated." Every hacker is getting excited when they hear that. It is like every castle has the same defense. And by the way, you have to trust the vendor, so it is like every castle's guard at the gate doesn't work for the people inside the castle, it works for somebody else, and they all use the same secret knock. And so, you could get in the door by trusting this vendor. And so, the hackers love these words "consistency," "interoperability," "uniform," and "coordinated." This is what allows them to hack not just 1 person on any given day, but 10,000 companies on any given day.

I am running out of time. I would suggest that, if Congress has any role here in mandating anything, it would be to have audits, and audits that are not written by the vendors, audits that are third-party audits that test—penetration testing of these systems. Otherwise, if you let vendors audit themselves, it is not going to work.

And with that I will yield back, and if somebody gives me more time I would love to go on.

[Laughter.]

Ms. NORTON. The gentleman's time has expired. I now recognize Mr. Payne for 5 minutes.

Mr. PAYNE. Thank you, Madam Chair.

Mr. Belcher, under the Rail Safety Improvement Act of 2008, Congress mandated that all Class I railroads and commuter and intercity passenger rail providers install Positive Train Control systems. Positive Train Control systems work to prevent unsafe movements and accidents by using an information network to regulate trains' positions. However, information networks can be vulnerable to bad actors, and must have adequate cybersecurity protections.

How should freight railroads and commuter and intercity passenger rail providers best protect these critical systems, and what consequences could result from a cyber incident of PTC systems?

Mr. BELCHER. Well, I think Mr. Farmer is probably better qualified to respond to that question than I am——

Mr. PAYNE. OK.

Mr. BELCHER [continuing]. Given his background.

Mr. PAYNE. All right. Mr. Farmer?

Mr. FARMER. Yes, sir, excellent question. Positive Train Control is a safety overlay to our operations. And I think what is significant here is, as opposed to many of the industrial control systems that we have seen hacked, a lot of them are older systems, not designed with cyber threats in mind. PTC has been specifically designed with cyber threats in mind.

And in particular, through the Rail Information Security Committee, which I referenced earlier in testimony, a concerted effort was devoted to coordinating with the National Laboratory, Lawrence Livermore National Laboratory, to do the sort of work that has been referenced a number of times in this hearing, to look at how the system was designed, to take the view of an adversary, to conduct penetration-type activity, to determine where potential vulnerabilities might be, and enable, as the development process proceeded, those matters to be addressed with effective cybersecurity measures.

Built into PTC you have, in particular, network segmentation, advanced encryption, short-term access authorizations for moving trains, all of which are designed to narrow the possibility that, one, a breach can happen; or secondly, if it does, that it can spread beyond the limited site in the network.

So that has been a concerted effort, and developed with cyber threats in mind, with support of Government through the National Laboratory, and through the proactive information-sharing work we do with CISA and TSA. Thank you.

Mr. PAYNE. Thank you.

And Mr. Farmer, good cyber hygiene is very important to protect against potential consequences that you just articulated. As chairman of the Railroads, Pipelines, and Hazardous Materials Subcommittee, I have a responsibility to ensure that freight railroads meet the evolving threat of cyberattacks.

Your testimony makes it clear that AAR opposes TSA's security directives. What assurances can you give this committee that freight railroads have taken the steps necessary to deal with a cyberattack targeting these critical systems?

Mr. FARMER. Well, the assurance is demonstrated in the experience of what we do in the industry, experience that is well-known to our partners in Government.

I mentioned earlier the committee that we have focused on cybersecurity more than two decades in duration. That group convenes twice monthly. It is an effective forum for sharing information on cybersecurity concerns, and on effective practices to mitigate risk.

The sorts of sound, fundamental measures that are taken across our industry include training for users on networks, drills of that training to make sure that the learning is tested and evaluated, exercises conducted within the railroad, conducted with TSA through its intermodal security training exercise program, and a national-level industry exercise we hold every year, where we take actual cyber incidents that have happened in other industries, and posit what would we do in the railroad industry if faced with similar situations.

And that gets into the key measure here, which is the well-developed preparedness and incident response plans that railroads maintain and constantly exercise, constantly refine, based on the assessments we do, based on what we learn, in particular from our interaction with Government on the nature of the evolving threat. Thank you.

Mr. PAYNE. Thank you.

And Madam Chair, I yield back the balance of my time.

Ms. NORTON. The gentleman yields back. I now recognize Mr. Perry for 5 minutes.

Mr. PERRY. Thank you, Madam Chair.

Mr. Belcher, your testimony explains that even the transition to electric buses brings with it a whole new level of cyber exposure and other security risks not previously anticipated. Given the majority's push to electrify everything without regard to the consequences, this statement may fall on deaf ears. But I think it is important to ensure everyone here knows what you mean by that statement.

Can you tell us how much greater is the cyber exposure in an electric bus fleet, relative to a diesel bus fleet?

Mr. BELCHER. Well, it simply creates a new threat vector in the sense that any time you add a new opportunity, a new digital connection, you create a new opportunity for an adversary to access your network.

Mr. PERRY. So, are you talking about things like the ability to degrade batteries remotely, cause fires, manually take over controls of the vehicle, that kind of thing?

Mr. BELCHER. Yes, you have created an opportunity to access the network. But——

Mr. PERRY. So——

Mr. BELCHER. But you are talking about sophisticated companies that are far more sophisticated, and that are building in protections into their bus systems and into their networks.

So, I think, while there are risks that come with that, new risks that we never thought about, these are sophisticated companies that are building in cybersecurity protections, as they develop these new technologies.

Mr. PERRY. But would you also say, then, I mean, based on that, yes, they are building in protections, but haven't computer companies and automation companies built in security protocols all along, but yet they have still been breached over and over and over again?

Mr. BELCHER. One hundred percent. We would be far safer if we were still running diesel buses that were not connected to anything, and that had no digital connections to anything.

Mr. PERRY. Right, OK. So, your testimony cites the 2020 Mineta Transportation Institute report on cybersecurity in the transit sector extensively. This report presents some pretty damning conclusions. As you noted, the 2020 MTI report concludes that, for many transit agencies, internal resources for cybersecurity are scarce. And you go on to cite reports finding that 43 percent of the agencies do not believe they have the resources necessary for cybersecurity preparedness.

To me, this raises a legitimate question about what exactly the taxpayer is getting back for the tens of billions of dollars per year that the FTA provides to transit agencies, and the nearly $90 billion we have given them in the past 2 fiscal years.

I mean, if transit agencies have failed to invest in protecting their cybersecurity systems, and have failed to do regular maintenance and upkeep, leaving more than $100 billion in state-of-good-repair backlog, both allegedly due to lack of resources, what in the hell are they spending their money on?

Mr. BELCHER. You know, that is——

Mr. PERRY. Yes, I guess that is probably not a fair question. Let me ask you this——

Mr. BELCHER. It really isn't a fair—yes, OK.

Mr. PERRY. I think the answer to that question might be a result of section 13(c) of the Urban Mass Transportation Act providing for employee protective arrangements, or agreements that effectively provide labor union leadership veto power over any potential Federal grants to their employer, which gives union leadership unparalleled negotiating leverage to force transit agencies to cave in to their demands.

This requirement is largely, in my opinion, responsible for the steep decline in transit worker productivity after it was enacted in 1964, despite the fact that nearly every other industry saw significant productivity increases.

It is also a significant contributing factor to the sector's uniquely high labor cost, as a percentage of operating cost, and massive, unfunded pension liabilities.

Given this background, would you agree that section 13(c) needs to be either repealed or, at the very least, significantly reformed so that transit operators are able to invest necessary resources to protect from physical and cyber threats?

Mr. BELCHER. I have no opinion on that.

Mr. PERRY. All right. How about the authors of the report emphasize the FTA should require transit organizations adopt and implement minimum cybersecurity standards prior to receiving Federal funding, where do you stand on that?

Mr. BELCHER. I agree.

Mr. PERRY. There you go. Thank you, Madam Chair, I yield the balance.

Ms. NORTON. The gentleman yields. I now call on Mr. Carbajal for 5 minutes.

Mr. CARBAJAL. Thank you. Thank you, Madam Chair.

Mr. Stephens, you highlight the importance of cybersecurity information sharing and communication. You also highlight how information sharing between the Government and the private sector has not been as effective as it could be, because it is voluntary.

What should be considered when thinking of legislation regarding mandatory cybersecurity information sharing and communication between the Government and the private sector?

Mr. STEPHENS. Thank you, Congressman, for that question.

One of the things—I would start from this perspective. Before legislation is struck, I think there has to be robust dialogue with the entities or the sectors that are going to be regulated. Sometimes moving too quickly to get something out significantly creates more obstacles, and more bureaucratic redtape, and impairs the cybersecurity preparedness of certain agencies, as many of us have spoken about.

To that end, though, a voluntary structure where there is no enforcement is relatively meaningless. You have to have some mechanism for enforcement. So, it is not a one-size-kind-of-fits-all approach. It is a holistic approach that, I think, our Federal Government has to take towards cybersecurity.

I will give you a primary example. Under FISMA, which—CISA is responsible for reviewing all of the Federal agencies, right? The vast majority of them have received D's. So the question becomes, if we can't—under FISMA, which has been struck some time ago—police the cyber hygiene of our own Federal agencies, it is a very difficult hurdle to then create mandates that are not attainable for other covered sectors. So, involvement with those covered sectors and getting really solid advice and perspective before those things come out is important.

And I will finish with this. Again, going back to the TSA proposal, for example, there was a 24-hour time reporting requirement under that proposed guidance. Most entities who have cyber incidents cannot begin to even do analysis on anything with respect to a cyber incursion in order to be able to meet that requirement, versus what is happening in the Department of Defense under the National Defense Authorization Act is a 72-hour requirement.

So, in short, I think that, while mandatory reporting requirements are great, it is what do we report and how do we report those things.

Mr. CARBAJAL. Thank you very much.

Dr. Kessler, you are an educator on the topic of cybersecurity at the U.S. Coast Guard Academy, and I am interested in your insight into the importance of cybersecurity training programs to strengthen our defenses.

Your recent report, "Raising the Colors," highlighted the need for industry-recognized certification in both information technology and operational technology fields, and the creation of cybersecurity training programs by the Coast Guard and the Department of Transportation.

With the support of the Department of Energy, the Department of Homeland Security, as well as the State Department and international organizations as vital to cybersecurity improvements, could you discuss the need for standardized training and certification in the Nation's cyber defenses?

Mr. KESSLER. Thank you very much for the question. I think we need to have certain standardization, so that everybody is at least getting the same baseline understanding and is on the same page of what it is we are trying to protect. I think it is incredibly important to recognize through this, and particularly as you are all considering legislation.

I agree, again, with what Mr. Stephens just said about working closely with stakeholders. The solution to cyber is not solely a technology solution. I will pull out an old quote that says anyone who thinks their technology can solve their problems doesn't understand technology and doesn't understand their problems.

If people are a big part of the problem, then people have to be a big part of the solution, and technology can't save them. Because people who don't know what they are doing can always get around the technology. So that is why the training is so incredibly important.

And there does need to be a certain global aspect to it, since the ships are going everywhere, and coming from everywhere, and can carry malicious software and viruses from port to port.

And so, again, the training has to be on the technology level, so that we have the appropriate number of technologists in the field, as it has already been discussed, that we are way short on the number of cybersecurity practitioners. But essentially, today everybody has become a cybersecurity practitioner, since we are all carrying around multiple devices that we need to secure.

Mr. CARBAJAL. Thank you. I am out of time.

I yield back, Madam Chair.

Ms. NORTON. The gentleman yields back. I now recognize Mr. Davis for 5 minutes.

Mr. RODNEY DAVIS. Thank you, Madam Chair, and thank you to all of the witnesses today. I would like to start my questioning with Mr. Farmer.

Mr. Farmer, do your members usually subscribe to more of a centralized cybersecurity operation at their specific railroads, or is it more decentralized?

Mr. FARMER. What you have with railroads is, through the headquarters elements you have cybersecurity expertise through chief information security officers, specialists in cybersecurity, well-trained personnel on the cybersecurity staff who, notably, participate in a training program hosted by Idaho National Laboratory, which looks at networks from a red-team perspective, and allows them to conduct penetration operations and learn what the adversary is looking to accomplish.

So, in that sense, what you have is probably something akin to my experience in the Air Force: centralized control, but decentralized execution, in terms of allowing the experts to apply their skills in ensuring network cybersecurity posture is maintained.

Mr. RODNEY DAVIS. So, the decentralized portion of your response there is indicative of—do you believe it is easier for a cybersecurity criminal to hack a more centralized system that is just in one location, versus a system you just described, that many of your members use?

Mr. FARMER. I think the key on what is easier for an adversary to hack comes down to the network architecture, and that is where the emphasis placed by railroads on ensuring network segmentation and on strong controls for access, those efforts, are vital. So, it is not so much whether it is a single point versus multiple points, it is more along the lines of how are you designing the network architecture, and putting in your layered cyber defenses in a way that creates opportunities to detect, disrupt, and prevent adversaries from inflicting harm.

Mr. RODNEY DAVIS. It just seems to me that it would be easier for our adversaries to go after systems that are uniquely intertwined at all levels, rather than decentralized, which I seem to—I guess I am understanding your response to say that you do have somewhat of a decentralized approach for possible redundancy issues and security issues.

What would you recommend we do, when it comes to transportation systems at the Federal level, when we certainly rely upon much more of a top-down approach when it comes to other systems in place?

What can we do to copy this more decentralized approach, and thus make it more secure?

Mr. FARMER. Well, I think your point on redundancy is exceptionally well taken. A lot of effort devoted in the industry to establishing backups, backups for programs and files, backups for operational control systems. And so, you have multiple options, should one component be adversely impacted, for the operation to continue.

I think what we have seen, particularly over the past several months, in terms of cyber intrusions, as you see in the CISA advisories on these events, this reference to highly sophisticated threat actors employing very well-developed tactics that reflect a great deal of understanding of networks, and I think there are two challenges that come into play there.

One is, in many cases, these are referred to as "supply chain vulnerabilities," where the adversary has determined, has identified the vulnerability present in a particular software application, and done the necessary surveillance of a network to exploit it. And CISA frequently recommends that railroads, other critical infrastructure organizations engage with their suppliers, and we do that in the industry through a dedicated group with our key suppliers.

But there is a key element, in terms of what Congress can do, I think, that merits attention, and that is one of the CISA recommendations is you should be getting from your supplier is a software bill of materials. And essentially, that is the delineation of all the software elements in the vehicle, equipment, device that you have procured, so that you, as the end user, know what software is included, and what versions are present. So, when these issues come up with these supply chain vulnerabilities and you need to know quickly, am I affected, the software bill of materials gives you the means to do that sort of reference.

And the second question that comes up is, are we doing enough, in terms of deterrence? We have talked a great deal in this hearing about network defense, and that is vital. But the concern that we have in the private sector is, in contrast to mitigating terrorism risk, which entailed a great deal of effort internationally in intelligence and military operations, the adversary's boldness, particularly of these past several months, with these highly sophisticated attacks, indicates they are not getting a deterrent message. And that is part of an effective strategy. Thank you.

Mr. RODNEY DAVIS. OK, I thank you. I would like to yield my remaining time to Mr. Burchett.

Thank you, Madam Chair.

Mr. BURCHETT. Thank you, Chairlady, and I yield the time that Representative Davis gave me to Thomas "The Hitman" Massie.

Mr. MASSIE. If there is any time remaining, I would like to allow Mr. Kessler——

Ms. NORTON. There really isn't.

[Laughter.]

Ms. NORTON. You will have to wait for someone else to yield, because all of that time has now expired.

Mr. MASSIE. Yes, Madam Chairwoman.

Ms. NORTON. And I am forced to——

Mr. BURCHETT. I am sorry, Chairlady, for that disruption. I have not had my Mountain Dew this morning. I apologize.

[Laughter.]

Ms. NORTON. All right. I now recognize Mr. Stanton for 5 minutes.

Mr. STANTON. Madam Chair, thank you so much for recognizing me. I want to thank Chairman DeFazio for holding this important hearing, I want to thank each of the witnesses here today for providing important testimony on this critically important issue that is growing in concern.

Cyberattacks against our water systems have become more frequent, sophisticated, and dangerous. Back in February a hacker gained access to the Oldsmar water treatment facility in Florida. Their goal was to increase the level of sodium hydroxide, otherwise known as lye, in the drinking water. While Oldsmar was lucky that the facility's operator was at his computer, and watching the hacker's attempts in realtime, the results, if they had been successful, could have been seriously harmful to residents and businesses who rely on that water for drinking water.

Approximately 90 percent of our country's public water supplies, and 80 percent of the wastewater utilities are small, and serve fewer than 10,000 people. The hack at Oldsmar demonstrates the vulnerability of small systems, and the challenges they face in preparing for and responding to these threats, compared to larger water systems. These systems have smaller budgets, limited resources, sometimes only a small number of employees to handle a significant amount of work. A cyberattack is just one more challenge they confront, so they must be strategic in how they approach this constantly evolving threat.

Mr. Sullivan, you mentioned in your testimony that Boston Water and Sewer Commission, where you are the chief engineer, you suffered from a ransomware attack last year. What do you believe are the lessons learned from that attack, and one that I described in Oldsmar, for other water and wastewater utilities, particularly small, rural, and Tribal systems, where they might not have as much access to staff with cyber expertise or financial resources?

Mr. SULLIVAN. Well, thank you, Congressman. We have been working many years to build up our cyber preparedness, along with most of your large water systems and wastewater systems.

The problem we had was this, it was the human element. One of our staffers allowed an email, a phishing email, and he opened it up, and he did not report that there was nothing there when he opened it up. What happened there is some malware got into our system [inaudible] and it sat, and—it sat for over a month, because we were able to trace it back later. The human element here is our biggest weakness. And we know that. We have got all kinds of systems. Our firewalls are secure. We are stopping things every day. We are getting attacked every day.

The cybersecurity awareness, a culture of awareness in every system, is the most important thing we need to do. And that is, we need to get to training. Many of these small systems are recognizing, they are struggling with making sure we get pure water out there, we are struggling with the new regulations of contaminants. The wastewater group, same thing. We struggle with producing the product that we are required to do, and many of the small ones may have IT systems that they don't even know how they run. They hired someone, they came in, a miracle occurred, all of a sudden you could operate from home, and life was good.

They don't have the awareness, and that is what we are trying to do through the ISAC, is continually remind people, "Pay attention, read these"—we work with CISA, et cetera—"Read all these reports, make sure you are doing this." But they don't have the resources to hire people to check everything else, and that is one of the major hurdles we have——

Mr. STANTON. Yes.

Mr. SULLIVAN [continuing]. Because we do have 50,000 water systems and 16,000 wastewater systems.

Mr. STANTON. You mentioned ISAC, the Water Information Sharing and Analysis Center, which was established, of course, 10 years ago to provide water utilities with critical information on threats, both physical and cyber-related, along with best practices for preventing and responding to those attacks.

I mentioned earlier Tribal communities, and challenges that the water systems in Tribal communities face. I want you to address that. What specific outreach or work has ISAC done with our Tribal communities? And if not, do you have plans to reach out to our Tribal communities to make it a part of its work?

Mr. SULLIVAN. The ISAC is a subscription service. We have over 400 members that cover much of the Nation. But we also have the States. The States are part of the ISAC. They get all our information, so that the States, through their resources, can reach out to smaller systems, the Tribals, et cetera.

We are asking for additional resources to have the subscriptions for everyone, every water and wastewater systems paid for so, that we can reach everyone, and give them the help they need to—we want to be able to take these threats, and boil them down to what it means for each size system, so that they can look at them, and they don't have to read these——

Mr. STANTON. All right.

Mr. SULLIVAN [continuing]. Lengthy documents.

Mr. STANTON. I am out of time, but my polite request is that maybe ISAC will reach out to those Tribal communities and the water systems there. It is so critically important that we provide clean water to our Tribal members, and often they don't have the same resources as others, but they have the same needs for their community. So, my request is that ISAC see what they can do to better reach out to our Tribal communities in Arizona, and around the country.

Thank you, I yield back.

Ms. NORTON. I now recognize Mr. Babin for 5 minutes.

Dr. BABIN. Thank you, Madam Chair. I am so glad we are having this hearing today for this committee to weigh in on the issue of cybersecurity in the transportation and critical infrastructure space. It is a great responsibility, and one that we should all take very seriously.

It is also very timely. Just yesterday the Director of CISA told the House Homeland Security Committee that “ransomware has become a scourge in nearly every facet of our lives, and it is a prime example of the vulnerabilities that are emerging, as our digital and our physical infrastructure increasingly converge.” She went on to say that, “The American way of life faces serious risks.” She is right.

Internet attacks are a full-fledged standard feature of our modern life. Hardly even a day passes anymore without a media story coming out about a cyber threat or an attack. These threats are disruptive, they are costly, potentially life-threatening. All of us saw what happened with the Colonial Pipeline breach last May, and how that attack led to gas shortages and interrupted supply chains.

There is certainly a legitimate and appropriate role for the Federal Government to play in protecting the American people in our companies and businesses against theft, espionage, and cyberattacks. No question. This is a fight for our national security. However, cyber intrusions are very hard to track. We have got to be extraordinarily careful, as lawmakers, that we don’t meddle in something that we don’t properly understand, and unintentionally cause bloated regulation, or stifle innovation with overly burdensome requirements that don’t truly secure our infrastructure.

Any policy we push forward has got to be aggressive, but consistent with our Nation’s founding principles, meaning that we provide for the common defense, while at the same time protecting civil liberties and the free economic economy. A former Director of National Intelligence, and my former Texas colleague and friend, John Ratcliffe, said that we need to attribute these attacks, and either to overtly or covertly retaliate against those responsible, creating deterrence for the future.

I could not agree more. There has to be a downside for these enemies. And inflicting appropriate pain for their attacks is not only justified, but I think absolutely necessary. And if our long-term strategy to cyber criminals is to just pay the ransom and hope for the best with cyber insurance, we will certainly lose to our foes in this new battlefront.

So, my question to all of you—and I will open this up to anyone who would like to answer this—what are commonsense steps that we, as lawmakers, can take to help the private sector better protect themselves, and better report cyber threats to the proper Government entities without infringing on people’s civil liberties or the free market?

I would open that up, please.

Mr. BELCHER. Well, I will jump in. I think one of the key things that organizations can and should do to protect against ransomware is to make sure that they keep adequate logs, data logs. And that is one of the things you see, particularly with small, smaller, or less sophisticated organizations. And if you are keeping adequate data logs, you can go back and recreate everything that happened prior to the hack. And that way you can avoid having to pay a ransom. And that is the best way that you can manage against ransom attacks.

And so anything that Congress can do to encourage that—I am not saying that you mandate data logs. It is good hygiene, it is something that trade associations should be encouraging, and should be providing guidance on, and it is something that we should all be pushing for, because it is the best thing that you can do to mitigate against ransomware, because it is happening every day.

Dr. BABIN. Thank you. Anyone else?

Ms. SAMFORD. Yes, sir, thank you. And I think that it is an excellent question. Thank you, Congressman Babin.

I always tell owners and operators there are a few top things that they can do. Number one is to have a complete asset inventory. You can't protect what you don't know about.

The second is to understand if you have direct exposure to the internet. I think that Congress would be very frightened if they were to examine the number of critical infrastructures that have industrial control systems that remain directly connected to the internet. That is an immediate and direct source.

If I were Congress, if I were in that position, I would direct all designated critical infrastructures within the United States to ensure that they do not have any devices directly connected. That would immediately eliminate tons of exposure and risk.

And lastly, I would like to redirect and go back to the point on ICS4ICS in that every single local fire department, every emergency services, even our military, it is the way that we mobilize to respond to events.

Out of all of the nationally declared disaster types, cyber is the only one that is not mandated currently to follow Incident Command System. I can tell you that being prepared and being able to mobilize the private sector, which is where 85 percent of your response resources will come from in the event of a nationwide attack, you will want a system like ICS to integrate. By no means does having a common framework for a response increase our risk or our threat. Those threats and risk are already there. All it does is give us an advantage over the enemy in effectively bouncing back from those attacks.

Dr. BABIN. Thank you very much, and my time is out, and so I will yield back.

Mr. STANTON [presiding]. Thank you so much. The next Congressmember will be Congressmember Carter.

Mr. CARTER OF LOUISIANA. Thank you, Mr. Chairman. My district recently suffered through one of the most intense hurricanes to ever make landfall in the United States. Hearing about the dangers threatening our systems through cyberattacks, I can't help but be concerned about what would happen if bad actors took advantage of a natural disaster to launch a cyberattack.

According to a recent article on the topic, natural disasters can set the stage for cyberattacks. Security experts say that they are not aware of any major cyberattacks against a State or local government during a natural disaster, but that is only a matter of time, if we are not careful to prepare for these things. And if a hacker launched a disruption to coincide with a natural disaster, that could greatly hamper first responders, hospitals, utilities, Government agencies. According to the National Association of State Chief Information Officers, this is a real threat.

So, I ask this question of you, Mr. Sullivan. Municipal water systems in many areas have to cope with threats of physical damage from natural disasters. I shudder to think what would happen if a cyberattack occurred in the near proximity to a natural disaster. Can you share your thoughts with me on that, and do you think that any local systems should train and practice for responding to a dual-threat scenario like this?

Mr. SULLIVAN. Certainly. First, the ISAC was formed because of the events of 9/11. And for the first 10 years, we spent all of our time talking about physical threats and natural hazards, and how to make sure you can get your systems up and running. And cyber wasn't really in the forefront at that time, because there were no major threats for us on cyber.

So we have been training people on natural hazards all along, how to do it, how to get yourself back up and running. We all have emergency response plans. The AWIA that Congress passed a couple of years ago required all systems serving 3,300 and more services to look at our natural hazards plan and our cybersecurity plans. And we have to self-certify that we looked at them and we have an emergency response plan.

So, I would say that most of your systems are definitely capable of getting up and running. Now, they can't run with the cyber. A lot of times communications are down, et cetera. They will place people at the plants, and they can manually run them. Most of our plants, although they are highly technologically run, can be run manually. We are able to run them that way. So, we are——

Mr. CARTER OF LOUISIANA. Let me ask you, what do you think Congress could do to make these types of trainings possible and accessible to local governments?

Mr. SULLIVAN. Well, there is a lot of training going on. EPA just ran some yesterday with CISA. We are working—American Water Works Association has put out much training. And all your water and wastewater national organizations have the training available.

The problem is a lot of the smaller systems don't know about it. We haven't been able to reach them to come in and get the training, and that is where the ISAC is trying to expand its reach, so that we can give them informed messages, informed information of training for them, their size, and how they can get available. So——

Mr. CARTER OF LOUISIANA. And maybe this is something that, through this committee, Mr. Chair, we could utilize our resources to enhance the availability or knowledge to local governments of this resource. Obviously, it is a threat that could be devastating. And having the preparation and training could really go a very long way.

Do any of the other panelists have any thoughts on how Congress could better help industries protect against cyberattacks occurring around or during or after natural disasters?

Mr. FARMER. Representative Carter, if I could, please?

Mr. CARTER OF LOUISIANA. Yes, please.

Mr. FARMER. Thank you. One of the important areas to emphasize, in terms of the emergency preparedness, is the level of deployment of resources in advance of the storm, so that the response and recovery effort happens immediately, as soon as safe conditions allow.

I think a good point was made earlier about the ability to maintain the capability to conduct manual operations. That is part of how we operate in the railroad industry. In the event there is an electrically or cyber debilitating environment, trains can continue to move under manual procedures. We can also relocate dispatch centers from impacted areas to others. And as I mentioned earlier, a key facet of our cyber defense and depth is having backup capabilities and backup files.

I think the point that you are getting to, though, gets to a broader question of how does private sector across sectors cooperate with Government, and what can we be focusing attention on? I think there are two elements there.

One is, what are the sorts of cyberattacks that would be most impactful, whether they are actually happening now or not, looking forward to that potential. What we deal with now are people looking to exploit the fact that there is a response going on, and that there is going to be businesses trying to come into an area, and you have a lot of fraud attempts. But what could be done, positing a potential scenario?

And then, secondly, then working through the Critical Infrastructure Cross-Sector Council, through CISA, through FEMA in developing a collective approach to try to address that problem.

I think the last aspect gets to a point that was raised in an earlier question. And that is, there has to be some deterrent aspect to our cybersecurity strategy. Adversaries need to understand there are limits.

Mr. STANTON. Thank you very much.

Mr. CARTER OF LOUISIANA. I think I am out of time. I yield back. Thank you.

Mr. STANTON. All right. Thank you very much, Representative Carter. Next up will be Congressmember Weber.

[Pause.]

Mr. STANTON. Congressman Weber, are you there?

If not, we will move to Congressman LaMalfa.

Mr. LAMALFA. Thank you, Mr. Chair. I appreciate the opportunity here today, and for witnesses that have gathered online for our information here.

So, when we look at the—yes, I know, a lot has been covered so far in the hearing today. But with the issue of cybersecurity and, I guess, my more acute interest in how that would be on small water systems and rural water systems. And you know, in California, we do have several water districts that distribute water to agriculture, but also they do have hydroelectric power as part of their system, as well.

So, the smaller districts have a bigger struggle probably coming up with the resources to compete, and have the best cybersecurity capabilities that might come against them from China or other terrorism activities.

Let me pose to Mr. Sullivan.

The Water Information Sharing and Analysis Center serves districts of all types, all sizes. You had noted some that were quite small, with 2,000 residents, or we can shift to agriculture that aren't necessarily residents, but also indeed very important in water delivery for what they do.

Could you touch on—if you have already, my apologies, but what are some of the simplest, fastest, lowest cost protections we could be emphasizing and starting with to help secure those districts, especially in a time we have so much unrest and potential for mayhem like that, and in an already stressed economy and stretched water situation like we see in California?

What are some of the things that they could be doing very cost effectively, and quickly, and efficiently to tighten up their cybersecurity?

Mr. SULLIVAN. Well, right off the bat, EPA has a great site that will list all the things they need to do.

But what is really important is make sure they don't have their operational technology, their SCADA control systems tied into their information systems. It is so easy to get into an information system, either through the human nature, or they can just hack into it through an email, et cetera. But if you can separate those two right off the bat, you——

Mr. LAMALFA. Separation, sir, a better separation, not having—we heard stories about having the same access codes and everything for the—so you want to have just a greater separation between the two?

Mr. SULLIVAN. Yes, I want to separate all the pumps and everything else that are run by technology, separate them from your information systems, where—your email, your—all your other systems. That is a very basic tenet. And if you can do that, you really secure the ability for someone to control your pumping stations, shutting yourself down, overloading your stations, adding chemical where it shouldn't be added. That is critically important, because many of the small systems have embraced technology so that they can go home at night, and these systems self-operate. And it is so important that they separate those.

But the data available, it is out there. EPA has done an incredible job. We work with the Water Sector Coordinating Council, DHS, EPA, our sector leader. All this information is out there. They just don't know where to go to get to it. And that is the key that we need to get more of.

The rural water has riders, they go out and they educate everyone, but keeping updated is important. If everyone thinks that 5 years ago they took a review of their systems and life was good, and they haven't looked at it again, they have got to look at it again. It is ever changing. This whole security issue is ever changing.

Mr. LAMALFA. Five years is a very long time, yes, yes.

Mr. SULLIVAN. An extremely long time. And we did that, we had a big emphasis, we pushed it, and everyone thought they were all taken care of. And now we have these additional threats daily.

Mr. LAMALFA. So, when we are talking small districts with, you know, not huge budgets with—if it is rural delivery or agricultural delivery, do you see that it is going to be affordable? Is it going to require a lot of staff, or a lot of upgrades and technology and equipment? Or is it something that can be piggybacked onto existing systems, if they are halfway modern?

Mr. SULLIVAN. I think it could be piggybacked. It is $100 to join the WaterISAC if you are a system below 3,300, $100 a year. There are 40,000 of them, though, and that is one of the problems. They just don't have that $100, or they don't know that they need this——

Mr. LAMALFA. Do you have confidence, sir, that the larger entities like—well, the State of California, for example, right in my backyard is the Orville Dam and the spillway that broke apart, you remember that story from a few years ago. Do you think the large ones, like States, are doing what they need to do on 1960s technology to upgrade those, so that they can keep control of their spillway gates and other aspects of their water control systems?

Mr. SULLIVAN. I think the larger systems are in very good shape. They are quite aware, because of the association of the CIOs talking to each other. So, I think there has been a lot of that going on.

What happens is the medium and small, and they have so many other things tearing apart. Most of your water and sewer operators in the country aren't computer literate. They hire people to come in and set up the systems for them. So, they are not quite aware of what we are all talking about all the time. The big ones are. We have whole departments dedicated to that.

Mr. LAMALFA. Thank you. Thank you, I appreciate it. I yield back.

Mr. STANTON. Thank you very much. Next up will be Congressmember Lynch.

[Pause.]

Mr. STANTON. Congressman Lynch, are you on?

If not, next will be Congressmember Malinowski.

[Pause.]

Mr. STANTON. Congressman Malinowski?

How about Congressmember Kahele?

[Pause.]

Mr. STANTON. Congressmember Williams?

Ms. WILLIAMS OF GEORGIA. I am here.

Mr. STANTON. Thank you so much. It is your turn.

Ms. WILLIAMS OF GEORGIA. Thank you, Mr. Chairman. The topic of today's hearing is one that is personal to me and my constituents.

I know how critical it is to invest in cybersecurity, because my district learned the hard way just 3 years ago. In 2018, a vicious cyber ransom attack devastated the city of Atlanta. Residents of the Fifth Congressional District couldn't pay their water bills, police departments lost investigation files, the courts lost legal documents, and it took millions for the city to recover. Our Atlanta airport is owned by the city of Atlanta, and luckily we only had to shut down our Wi-Fi for the duration.

What happened in Atlanta is a lesson to be learned from. We need to ensure that we are prepared for any future cyberattacks. And as a Member of Congress, I am dedicated to ensuring what happened to Atlanta won't happen again.

Ms. Samford, what are the contemporary challenges that State and local governments face today in confronting cybersecurity challenges?

And what more can Congress do to assist them, and ensure information sharing between the private sector and Government, so we can prepare for and mitigate cyber threats?

Ms. SAMFORD. Great. Thank you, Congresswoman Williams, and that is an excellent question.

I think the main thing, honing in on the private sector, I think, coordination and response aspect, is that specifically what you would like me to touch on, is that private-sector interaction?

Ms. WILLIAMS OF GEORGIA. Yes.

Ms. SAMFORD. Thank you. In particular, for the private sector, there is no real way for the private sector currently to hook into existing emergency management practices. So, I am sure that you are very familiar with Atlanta. You probably have an Atlanta emergency operations center. And your emergency responders come in there, the different groups from the city of Atlanta, water, wastewater, your energy companies, your electric utilities, they all come in there, and support through what are called emergency support functions, ESFs. This is part of the Incident Command System structure that I was speaking of earlier.

There needs to be a better mechanism for the private sector to be trained on what Incident Command System is, what their role would be in a disaster, in terms of integrating with the Government, and then they can actually have representatives that are sitting there in that EOC, ready to integrate into your response efforts and reporting up through your incident commanders through the city of Atlanta.

So that would be one recommendation: training of the private sector, right? We can start on a voluntary basis and see where that gets us. And secondly, have them take their existing response plans—no one is telling them to get rid of what they have. We don't want them to do that. We just want them to learn the overarching Government framework that every other first responder is using, so that cyber can stop treating itself as something special and get with the program with the rest of the way that the emergency response communities behave. And that way we can begin to form coordinated responses together.

Ms. WILLIAMS OF GEORGIA. Thank you, Ms. Samford.

And Mr. Belcher, in your testimony you highlighted that only 60 percent of transportation agencies have a cybersecurity preparedness program in place. What are the most critical additional resources that Congress can provide to ensure that all transportation agencies are in a strong position to protect themselves from cyberattacks?

From agencies that have programs currently in place, what are some of the best practices that agencies should be sure to adopt?

Mr. BELCHER. So, I think the first thing that agencies need to do is that they need to do an assessment of their cyber maturity. Every agency has some level of cybersecurity protection, whether they know it or not. Cybersecurity protection comes with your Microsoft 360 system. You have got some level of cybersecurity protection. And then many of your more sophisticated systems also have protections in them.

But many of the operators really don't understand what they have. So, you have to understand what you have to understand what you need.

So, the first thing you need to do is to do an assessment, and then you need—as Ms. Samford was talking about, is to understand—is to then—to bring that into an enterprise system, and to treat cybersecurity as just another—it becomes another risk. It is another—you know, and you need to manage it as a risk, as one of the many risks that you manage, so that it becomes a way of doing business, and it becomes part of the culture of the business.

Most of the threats are coming—or most of the hacks are coming not at the IT level, but they are coming through the users, and through phishing, through—and like—and I think I keep hearing that I am about to be——

Ms. WILLIAMS OF GEORGIA. Yes, Mr. Belcher——

Mr. BELCHER. Got you.

Ms. WILLIAMS OF GEORGIA [continuing]. We are running out of time.

Mr. BELCHER. OK.

Ms. WILLIAMS OF GEORGIA. And before I yield back, Mr. Stephens, I would like to just get some better ideas on how we can address the unique cybersecurity challenges of major airports, with Atlanta being the busiest airport in the country, soon to be in the Nation. We are coming back, you all. But I would love to get some written comments on how we can better prepare in Atlanta, as you discussed what was happening down in Tampa.

Mr. STANTON. Thank you very much for——

Ms. WILLIAMS OF GEORGIA. Thank you, Mr. Chairman, and I yield back.

Mr. STANTON. Thank you. We will ask for a written response to that question.

Next up will be Congressmember Van Duyne.

Ms. VAN DUYNE. Yes. Thank you very much, Mr. Chairman. I would like to relinquish my time to Congressman Thomas Massie.

Mr. MASSIE. I thank the gentlelady from Texas.

Ms. Samford, I wanted to give you a chance to answer my concerns about consistency, interoperability, uniformity, and coordinated systems.

But before that I want to highlight something really important you said to one of my other colleagues. You talked about the microcontrollers and embedded processors that are connected to the internet that a lot of users don't even know present security vulnerabilities.

Just for my colleagues, this is like if you bought a coffeemaker, or an icemaker, or a dishwasher, and it is connected to the internet when you get it home for your convenience. Those things can be security vulnerabilities. But within a sewer system, for instance, or a pipeline, they might have things connected to the internet for remote monitoring.

So, can you talk about that, Ms. Samford, about how you advise your clients, and what to do with those things?

Ms. SAMFORD. Sure, and thank you, Congressman Massie. It is a really good question. And what we see a lot of—and I don't know that it is specifically with the programmable logic controllers that PLCs—in many cases, those lack the ability to directly communicate out to the internet, but they certainly could talk through something else. What we see a lot of are what are called human-machine interfaces, HMIs. To your point about someone remote accessing in, they would be remoting in to that engineering workstation, or HMI, to see what is going on on that plant floor.

In many cases, if you go to a website right now called Shodan.io, you can see tens of thousands of HMIs directly connected in the United States and the U.K. and Australia, globally. They are everywhere. And this main point of exposure is that right now I could go to the login screen of this HMI, and, if I am successfully able to log in—say, if the user name is "admin" and then the password is "admin," or if I am just using a password cracker, I can get into that system within a matter of minutes or hours. And once I am there, I can see other devices that are on that network, because it is the HMI, and it tells me that. And I can move laterally to do whatever I need to do.

So, I always tell people, please have an up-to-date asset inventory, know what you have so that you can protect it. And secondly, make sure that nothing is talking out directly to the internet.

Mr. MASSIE. Thank you very much. And did you—I didn't give you a chance earlier to respond to my concerns about consistency, interoperability, uniformity, and coordination. I am worried that that—and sometimes that makes it easier for the hackers to hack multiple systems at once.

Ms. SAMFORD. I definitely understand and respect your concerns. I think that it is a credit to you to understand the nature of how hackers can work.

Sometimes—I can tell you that the system that I am talking about, they have already gotten in, they have already performed the attack. So, the response structure, the only thing it gives us, is the ability to more effectively work with our local, State, and Government officials. And I am not asking that this be mandated at this point, but I am saying that it is really good training. It is how every single fire department responds. It is how, if someone was injured, the ambulance would show up. It is using the same system.

So, I would liken it to—I wouldn't say that we would suggest that having all firefighters trained in the country to be able to work together and respond somehow contributes to terrorist attacks. We don't see that correlation. So, we are not seeing that data to suggest that risk at this time. But I understand your point.

Mr. MASSIE. Yes, I was more concerned about, like, the updates that happen, and such as that.

Mr. Kessler, you had a couple of things you wanted to talk about, and we ran out of time. And also, if you could throw into that group—you talked about the pros and cons of having a human in the loop. It is not always a bad thing to have a human in the loop, I would say. And could you talk about—I will give you the remaining time.

Mr. KESSLER. Well, I mean, humans are in the loop, one way or another, either the human user with the hands at the keyboard, or the designer of the system.

So, I wish more of my grad students had been like you, Congressman Massie.

So, I used the ICS for decades. I was 25 years on the ambulance in my hometown in Vermont, as a volunteer ambulance. And so, cyber differs in this way. So, I need an organized structure to do my defense. But, as an EMT, I would walk into somebody's house, and I was always reminiscent of the saying "No battle plan survives first contact with the enemy." I know how I am going to respond.

The problem in cyber with having any static response, or automated response to an attack is, if I can figure out what your static response is going to be, I own you because I can make you respond when I want you to respond, and I know how you will respond, because too many of the cyber systems are not built defensively to take into account that there is an intelligent actor causing the problem.

Mr. STANTON. Thank you——

Mr. KESSLER. Too many of our systems by engineers, of which I am one, are designed to fail, thinking nature is our enemy. And I understand [inaudible] what is going to happen, but I am not building a system——

Mr. STANTON. All right——

Mr. KESSLER [continuing]. [Inaudible] other people.

Mr. MASSIE. Thank you.

Mr. STANTON. Thank you.

Mr. MASSIE. I yield back.

Mr. STANTON. Thank you. Next up will be Congressmember Johnson of Texas.

Ms. JOHNSON OF TEXAS. Thank you very much. Let me express my appreciation for this hearing, and the urgency of dealing with the issue.

Five years ago, in my Dallas-based congressional district, cyber hackers breached the Dallas Area Rapid Transit computer system, targeting customer communication and business processing tools. Just last year, hackers stole Trinity Metro's data in Fort Worth, knocking out the Metro's phone lines and entire booking system. And although not specific to the transportation industry, electronic records were hacked at the Dallas Independent School District in September, allowing the hackers to gain access to the names, addresses, telephone numbers, Social Security numbers, and medical information. While just last month, the Dallas-based company of Neiman Marcus notified 4.6 million customers that information associated with their online accounts had been stolen. Disheartening stories like this play out week after week in the United States and across the globe.

So first I want to ask Mr. Belcher.

Mr. Belcher, much of the Nation's infrastructure is owned and operated by the private sector. What controls and procedures do you recommend synthesizing and strengthening regarding cybersecurity in the private sector and the Government partnership?

Mr. BELCHER. Well, the good news is, many of the hacks that you talked about in the public sector in the Dallas-Fort Worth area have been moved to private-sector vendors.

Transit agencies now, for the most part, do not handle the records of private riders, the financial records. Those are typically handled by financial institutions now, because those financial institutions are far better able and capable to handle those records under a specific regime that has been established, and they are able to protect those records far better than public transit agencies are.

And really, at this point, only the largest public transit agencies do it on their own, because of that. And so, I think we have gotten a lot smarter. And I think, in the public transit arena, public transit agencies are continuing to try to push off as much as they can into the private sector, which itself is becoming much more sophisticated than the public agencies are.

Ms. JOHNSON OF TEXAS. How do we transition to all-inclusive security monitoring and tracking of information technology and operational technology systems to protect against these cyberattacks and breaches, and the alertness to enact immediate incidence response?

Mr. BELCHER. Well, you are never going to be able to track everything, and that is the challenge. You have to try to stay ahead, and you have to be able to be responsive. But you are never going to be able to catch everything.

We now have systems that you can employ at the various levels of your stack that can track what is going on, and that can identify breaches. And every major system, whether it is an OT, an operational technology system, or an IT system, an information technology system, do have those systems in place.

And again, we pick up the vast majority of the hacks that occur. It is the ones that slip through which are the ones that we read about. So, we are getting better at discovering, and at preventing them from occurring, and we have to continue to up our game, and continue to get better.

I think what we are seeing, though, and I think what you have highlighted, is that, especially in the public sector, we are just not very sophisticated, and we are underresourced, and we need all the help we can get. And so, we need to work with Congress, with the Federal Government, and with the private sector to elevate the game at all levels. Because if we don't work together, we are going to continue to see the kinds of breaches that you have talked about.

Ms. JOHNSON OF TEXAS. You touched on my last question. What amount of funding do you believe Congress should provide——

Mr. STANTON. Well, I think we are out of time, Congressmember.

Ms. JOHNSON OF TEXAS [continuing]. To assist individual transit agencies like the Dallas Area Rapid Transit with increasing their cybersecurity programs?

Mr. STANTON. Maybe we can get that answer in writing. We are out of time, Congressmember Johnson.

Ms. JOHNSON OF TEXAS. Thank you, I yield back.

Mr. STANTON. Thank you so much. Next up will be Congressmember Balderson.

Mr. BALDERSON. Thank you, Mr. Chairman. Thank you all for being on today. My first question is directed to Mr. Farmer.

Mr. Farmer, you noted in your testimony that the rail industry security plan does not just sit on a shelf, occasionally taken down, and dusted off. Rather, it is a living document elevated and enhanced continuously. It is great to hear how importantly the rail industry takes cybersecurity.

It has also become obvious over the last several months just how delicate our supply chain is. Mr. Farmer, can you discuss the impact that a breach or a hack on just one Class I railroad could have on our supply chain?

And then a followup to that would be what ripple effects would we see if a Class I railroad had to shut down operations, even if just for a few days?

Mr. FARMER. So, the question posits that the impact is one for which the response capability would not be adequate to sustain operations.

I think the key point to make there is the entire basis of our cybersecurity program is to ensure the protection of the operations from breaches, to contain any breaches that occur, so that we are not facing a situation where the entire railroad network has to be shut down.

And the key point here that came up in an exercise we held at the Naval War College—the Naval War College invited representatives of numerous critical infrastructure sectors to an exercise in July 2016, and it focused on operating a debilitated cyber environment. And we had participation by one of our major freight railroads. And a key point made by its chief information officer was, so long as I can communicate, I can continue to move trains.

I think, for us, we have the ability to fall back onto manual operations, if necessary, backup systems. So, the whole thrust of what we are doing is to ensure we don't find ourselves in a situation where that sort of shutdown happens, by keeping in the layered defenses and the depth of operational capabilities, even down to manual, and continuing to move trains as safe conditions allow.

Mr. BALDERSON. Thank you. A followup to that, Mr. Farmer, you recommended future cybersecurity legislation should direct the CISA to establish consistent standards for software bills of materials from vendors and suppliers. Can you expand on why this is important in preventing cyberattacks?

Mr. FARMER. Yes, sir. So, a common theme, a recurring theme in the high-profile attacks that have garnered such attention, particularly in the first portion of this year, first several months, was the supply chain vulnerability type attack. Again, that is where an adversary has identified what is called a zero-day vulnerability and exploits it.

And so, some of the major attacks that have been perpetrated with alleged involvement by nation-state actors have followed this model. SolarWinds is one example.

The software bill of materials gives the end user an ability to understand fully what software applications and what versions are on any of the vehicles, equipment, devices, systems they employ. CISA strongly recommends that end users have these bills of materials.

The challenge is there is no consistency in their being provided. And when they are provided, there is no consistency to ensure they are fully thorough and accurate. And there is an opportunity here for CISA to define standards so that end users can quickly act upon reported vulnerabilities, scan their networks using these software bills of materials as a reference point, and make any security patches to preclude the potential for exploitation.

Mr. BALDERSON. Thank you very much. Great answer. My next question is for Mr. Stephens.

Mr. Stephens, thank you for being here today. I understand that Tampa International Airport is designated as a large hub. But can you speak on the differences between the threats or vulnerabilities faced at large hubs and the cybersecurity issues facing small or medium hubs?

Mr. STEPHENS. Congressman, thank you for that question. The threats are, at their very basic nature, the same. The impacts are different. So, when you are talking about large hub airports, particularly airports where there are a lot of connections, we are more of an O&D, so, we don't do a lot of connecting activity.

But the Dallas-Fort Worth Airport, Los Angeles, all those types of airports have a different threat profile, because attacking them becomes a much more preferred target if you are trying to create injury, if you are trying to create disruption. Smaller airport systems here in Florida like, say, Gainesville or some of the other smaller airport systems, the primary driving factor or interest there would perhaps be data or information from employees or other vendors.

So those are the major distinctions. It is the desirability from a bad actor of the target, based on the scope and the size and the damage that they want to do.

Mr. BALDERSON. All right. Thank you very much.

Mr. Chairman, I will yield back my remaining—well, I am almost done. Thank you, Mr. Chairman.

Mr. STANTON. Thank you. Next up will be Congressmember Johnson of Georgia.

[Pause.]

Mr. STANTON. Congressmember, I think you are muted right now.

[Pause.]

Mr. STANTON. Congressmember Johnson of Georgia?

[No response.]

Mr. STANTON. Congressmember, I think you are muted right now. Can you unmute?

[Pause.]

Mr. STANTON. All right. We will come back to you, Congressmember Johnson. Next up will be Congressmember Auchincloss.

[Pause.]

Mr. STANTON. Congressman Malinowski?

Mr. JOHNSON OF GEORGIA. Mr. Chairman, I am ready to go. It's Hank Johnson.

Mr. STANTON. Thank you very much, Congressman Johnson.

Mr. JOHNSON OF GEORGIA. Thank you, Mr. Chairman, for holding this hearing, and thank you to the witnesses for your time and testimony.

The information age has radically changed our critical infrastructure landscape. Earlier this year, cyberattacks on SolarWinds and Colonial Pipeline demonstrated the emerging threat of cyber warfare from state and nonstate actors. However, the cybersecurity field is beset by a dire shortage of specialists, especially among Americans of color and women.

We, as a Congress, must act now to provide young Americans equitable access to cybersecurity training. The future of our national security depends on it.

Mr. Belcher, this fall I introduced H.R. 5593, the Cybersecurity Opportunity Act, with Senator Ossoff, a bill which aims to create a pipeline of diverse cybersecurity workers by investing in research and training at historically Black colleges and universities and minority-serving institutions.

You have served as the CEO of the Telecommunications Industry Association, and president and the CEO of the Intelligent Transportation Society of America. So, I assume you have encountered issues regarding cybersecurity, workforce shortages, and diversity.

A 2021 study estimates that the national cybersecurity workforce is made up of 14 percent women, 9 percent Black Americans, and 4 percent Latino Americans. Can you discuss the importance of diversity goals, as they apply to cybersecurity-related positions in transportation and other critical infrastructure?

Mr. BELCHER. Yes. I think it is a much bigger issue than just cybersecurity. It is an issue that is playing out in all of transportation and all of engineering.

Shawn Wilson, the secretary of transportation from Louisiana, who is now the new AASHTO chair, has made that one of his preeminent goals. He is also the incoming vice chair of TRB. And so, there are leaders in the transportation community who have made that a significant priority.

The interesting thing about—the only thing that I can add is it has—finding women and people of color for technology positions has been a significant issue in the industry for a long time. It is becoming harder, but it is becoming even harder because it is becoming difficult to find people, in general, for these positions.

And so, what we are seeing now is—I am seeing my clients contracting those positions out. Where they would normally have hired in-house, they are now no longer able to find higher in-house positions. So, transportation organizations now are going to contractors and filling the positions with contractors. And it becomes even harder, then, to fill those positions, to try to fill them with STEM-type individuals. It has become even more challenging, not less challenging.

Mr. JOHNSON OF GEORGIA. Thank you.

Mr. BELCHER. So, I applaud you for your legislation.

Mr. JOHNSON OF GEORGIA. Well, thank you, and we hope it will make a difference.

Dr. Kessler, you have had extensive academic experience teaching computer technology education at some of the top engineering programs in America. Can you address how a more diverse cybersecurity workforce would benefit your specific infrastructure sector, and what steps you might advise private industry in your sector to consider to improve diversity in regard to cybersecurity positions?

Mr. KESSLER. Well, I have a couple of comments. First of all, I, too, applaud your legislation.

I would observe that one of the problems keeping an appropriate number of all of our citizenry, but particular people of color and women, is not at the college level. It is at the K through 12 level. I believe that too many individuals—and again, particularly women and particularly people of color—are socialized out of STEM by sixth grade. So, it is laudable, but late, in 12th grade to say, "You should go study STEM at college," because they haven't been prepared.

I have found that diversity of background gives me diversity of thought, and that is what I need to build a cyber defense. Because to build a cyber defense, I need to think like my attacker. The same thought leadership, if you will, that got me my problems are not going to get me my solutions, so I need to have that diversity of thought.

So, is that addressing, I think, what you are asking?

Mr. JOHNSON OF GEORGIA. Yes, it does. And I thank you for your comments.

Mr. Belcher, according to the 2020 MTI report presented in your testimony, 81 percent of responding transit agencies felt they were prepared to manage and defend themselves against cybersecurity threats. However, only 60 percent had an actual preparedness program, while 47 percent failed to audit their cybersecurity program at least once a year. What requirements should the Federal Government enforce, so that cybersecurity safety is adhered to at these transit agencies?

Mr. BELCHER. Well, if you look at the conclusions of the study, I think that the conclusions kind of lay them out. I think there are some basic requirements.

I think that agencies should be required to have a cybersecurity response plan in place.

Mr. JOHNSON OF GEORGIA. Thank you. I believe my time has expired, and I yield back.

Mr. STANTON. Next up will be Congressmember Stauber.

Mr. STAUBER. Thank you, Mr. Chair. Cyberattacks are a serious and evolving risk that affect transportation and infrastructure matters across this committee's jurisdiction. The Committee on Transportation and Infrastructure's jurisdiction includes 5 of the 16 sectors of cybersecurity which include our transportation systems, Government facilities, water and wastewater systems, dams, and emergency services.

The Nation's critical infrastructure is comprised of both public and private-sector assets. However, within this committee's jurisdiction, cybersecurity requirements in the private sector are mainly voluntary. Like other industries and the Federal Government, the transportation sector is facing a critical shortage of cybersecurity personnel, which has impacted the ability to protect, detect, and respond to cyberattacks effectively.

Simple steps regarding basic training, consistent cybersecurity hygiene, and periodic exercises could go a long way in protecting

America's transportation infrastructure. As the technology that enables America's infrastructure becomes even more complex and increasingly integrated, cybersecurity threats and vulnerabilities will continue to multiply.

My question is for Mr. Farmer.

Mr. Farmer, we have heard from several industries expressing concern over potentially duplicative and conflicting cyber reporting requirements to various Government agencies. Is this a concern for railroads? And if so, what steps could Congress consider to better harmonize such reporting across the Government?

Mr. FARMER. So, that is an excellent question, and it gets into two applications. One is what is being imposed by requirements, and then what is being done under cooperative efforts initiated by industries with partners in Government.

For requirements, a railroad with a cybersecurity incident could find itself having to meet a TSA regulation from 2009 under the rail transportation security rule that requires reporting of significant security concerns of requirements to report to the Department of Transportation. If the transport involves DoD supplies, requirements to report the DoD components. And then, with the planned security directives, a separate reporting requirement to the Cybersecurity and Infrastructure Security Agency.

The concern there, obviously, is multiple reports on the same matter going to different organizations, and the confusion that can result.

Another key concern in this area, as has been noted previously, is the short timeline envisioned by both of the TSA—the current regulation and the pending security directive. And that is a 24-hour period. And as has been detailed, it is often very difficult in that short time window to complete the analysis that helps an organization understand whether they are dealing with a significant cybersecurity concern.

So we have—our view is this area can be readily addressed through a collaborative process, based on what we have heard a lot about today, in terms of the reporting that is already taking place by our industry, in the water sector, the transit sector, oil and natural gas sector, all of these industries have created information-sharing analysis centers or, in our case, the Railway Alert Network.

And the focus is on taking what we are experiencing, what we are seeing, conducting analysis, and getting reports that—again, using the standard that Jen Easterly has set, as Director of cybersecurity at the Cybersecurity and Infrastructure Security Agency, provides the Government with signals, not noise, to aid their analytical efforts.

And I think, if there is an area where Congress' action is vitally important, it comes down to two points.

One, the Cybersecurity Information Sharing Act of 2015 should be fully implemented, and it is not. That will create the conditions—it specifically authorizes the kind of information sharing we are talking about within sectors, across industries, between industry and Government. It also provides protections that remove impediments to timely flow of useful information.

And the second element is we have got to close the gap on analysis. A lot of reporting goes into Government, but it doesn't often come back in terms of the sort of cybersecurity information products transportation organizations need. It has to be focused on transportation. What does this activity mean to transportation organizations? What should they do about it, in terms of some of the measures you laid out on cybersecurity actions to narrow their risk profile?

Thank you.

Mr. STAUBER. Well stated. That was a very defined answer.

And my time is running short here. Mr. Chair, I yield back.

Mr. STANTON. Thank you. Next up will be Congressmember Malinowski.

Mr. MALINOWSKI. Thank you, Mr. Chair. I wanted to address some questions to Mr. Sullivan, and because I am, in particular, very concerned about the water sector's vulnerability to cyberattacks.

Most of us here are familiar with what happened in Oldsmar, Florida. I think other Members raised that case, when an intruder took control of an engineer's screen at a waterplant, and dialed up the levels of sodium hydroxide. And thankfully, it was noticed. The disaster was averted. But as former CISA Director Chris Krebs has noted, after the attack, that the vulnerabilities in the Oldsmar plant, as he said, are probably more the rule than the exception.

There are a lot of things that need fixing here, and we have heard about a number of them throughout the hearing today. Municipalities need more funding, more in-house technical expertise, better cyber hygiene practices, and more. And the Federal Government can and should help with these things.

But it is also my view, at least, that the Federal Government should also have a bit more visibility into these breaches when they are discovered, that we shouldn't be relying, as we do today, on voluntary reporting.

So, Mr. Sullivan, you noted in your testimony that your organization, WaterISAC, created a step-by-step, 15-point document to help water and wastewater utilities with cybersecurity challenges. We took a look at that document, and there is some very useful, actionable information in there. I am grateful to the help you are providing to utilities.

But the language on reporting of incidents particularly caught my eye. In the document you urge utilities and other sector stakeholders to report incidents and suspicious activity to your analysts at WaterISAC, and you further note that, as a private nonprofit, WaterISAC is not subject to public records law, further preserving the security of your report. Again, sort of emphasizing the privacy of this information.

So, I wanted to ask your views. And I think the chairman of the committee asked a number of others on the panel this question before. What are your views on creating mandatory reporting requirements for municipalities for certain types of cyber incidents?

Mr. SULLIVAN. Well, mandatory can work. First of all, what we have seen is that it was way too short a time. We struggled, and we are pretty good at our IT. We struggled over the first 24 hours to find out what we were dealing with. So, if we do go to mandatory, we have got to go 72 hours, and maybe not the full report in 72, but reporting in 72 and then being able to follow up a couple of weeks later, because it took us 3 weeks to figure out exactly what happened.

Mr. MALINOWSKI. Right.

Mr. SULLIVAN. As far as the mandatory, we then have to explain to everyone what is an incident. And as I described earlier, we have so many water systems that, although they have cybersecurity protocols, et cetera, I am not sure everyone understands an incident.

So, we have to be very careful. The water sector would definitely work with Congress to help identify what triggers an incident, or else every time something goes wrong, we are just going to be flooding a market under the mandatory, because we are so used to standards in the water and wastewater. You will get a lot of information, much of which may be useless. So, we need to be very careful what we call mandatory.

But that is the only way we are going to get it. WaterISAC struggles to get people to report to us what is going on out there, so that we can share that information and others can learn from it. We constantly ask our members what went on, what happened, so that we can take that information—take your name out of it, and we will call it a utility in the Northeast, we will call it a utility in America—and to share the information so we can all learn. It is the only way we are going to figure out what is happening in our sector.

Mr. MALINOWSKI. That makes sense. And, I mean, it would—it is fair to assume that there probably have been other Oldsmar-like intrusions that we just don't know about, right, because we don't have mandatory reporting.

Mr. SULLIVAN. I would say there definitely were other problems that have occurred that weren't reported, because they really didn't need to be, or they didn't realize they were a cyber intrusion.

Mr. MALINOWSKI. Got it, good. Thank you so, so much. I look forward to working with you on this, and I yield back my time.

Mr. AUCHINCLOSS [presiding]. The gentleman yields. The Chair recognizes the gentlelady from Puerto Rico, Miss González-Colón.

[Pause.]

Mr. AUCHINCLOSS. Miss González-Colón?

[No response.]

Mr. AUCHINCLOSS. The Chair recognizes Mr. Burchett.

Mr. BURCHETT. Thank you, Mr. Chairman. I yield time sufficient to Thomas Massie.

Mr. MASSIE. I thank the gentleman from Tennessee for yielding me more than zero seconds this time.

Mr. Farmer, you spoke about something, a best practice, what should be a best practice—but I think it is underutilized and underappreciated—that you learned from consulting with the Naval War College about operating in a degraded or debilitated digital communications environment. It is my hope—and you mentioned that you looked at how you could go to manual systems in those times.

Also, I think a lot of people need to be doing that as a best practice at waterplants, or pipelines, or sewer plants. I think that is something that they should follow, and look to, and even look at possible parallel analog systems. It is very hard to hack an analog system, but everything has gone to digital now.

And could you just tell us a little bit more about that part of your process, or what you learned from the Naval War College?

Mr. FARMER. The Naval War College exercise, sir, brought together representatives of numerous critical infrastructure sectors, including some represented in the work of the committee in this hearing. It was an initiative where the military wanted to do a focused exercise on a scenario involving an activity by China that necessitated naval deployment, and looking at, logistically, what would it take to get all the resources to deploy a naval task force, and how would that work in a debilitated cyber environment.

And a key question that came up over and over again is, well, just how much operations could be retained if the information technology systems were not as available as we are used to them being prevalent. And for the rail industry, there were repeated points made along the lines I referenced earlier. Essentially, as long as communication could be made in some way to get the train crews engaged, to get the trains organized, typically for the military deployments is that priority, we could continue to operate. It would not be as efficient as normal, but we could continue to get trains to destination and, with a priority to the military shipments, get the items from forts to ports for deployment.

Beyond that exercise, we had a—during the 2017–2018 period, where we participated with Transportation Command and Northern Command in a forts-to-ports analysis, where they were looking at how the military deploys from its installations to ports and coastal areas, and what are the logistics there. And that work involved a great deal of sharing of information by our industry on both our physical security, planning and preparedness, and response measures, and on the cyber side, as well, and so a very good partnership with military components, in terms of ensuring we are able to support their operations in situations where they need to get equipment and people—sorry, mostly equipment—to ports for transport overseas.

Mr. MASSIE. Well, I surely hope that any legislation that comes out of Congress doesn't force you into a system that assumes that you will always be operating in a secure cyber environment. And so, I am glad to hear that you have at least tested what would happen in that instance, and you are going to look like a prophet later, if they go back and look at this hearing, if they have somehow forced you into a completely digital solution that is not segmented. That was another thing that you mentioned that I think is a really smart thing that you—that one hack on your system wouldn't imply the whole system was hacked. I think that is also a good best practice that I hope will come out of this.

Part of the problem we have—and this is ironic—is our Federal procurement standards sort of bake in vulnerabilities. I don't know exactly what is available in the executive branch, but in the legislative branch, if you wanted to buy a zero-trust system that ran on Linux, you couldn't do it, because there is interoperability requirements with the Microsoft systems, which have—by the way, a lot of these commercially available, widely deployed systems have the requirement that the end user is not at the root level.

The end user is not the root user, the actual root user is the vendor. And they have convinced the end user that it is in their best interest to let them send real-time updates. “We can make you more secure if we can identify a threat somewhere else, and then update your system without you hitting yes or no on the screen. Just let us go ahead, at the root level, and update your system, and we can make you safer if you allow us to do that.” Well, that is not always the case, and that is the vulnerability that oftentimes makes a small exploit turn into a giant one.

So, Mr. Kessler, I think you are wise to encourage and solicit diversity of solutions from your students, and I wish we had more diversity of solutions allowed into procurement policies.

And I yield back.

Mr. BURCHETT. Mr. Chairman, my intellect is so much superior to Thomas Massie’s, that is why I had him deliver those questions, so that the average citizen could understand them. And I yield back the remainder of my time.

Mr. AUCHINCLOSS. The gentleman yields. The Chair recognizes himself for 5 minutes.

I want to continue to pull on the thread of water infrastructure. We know that our water infrastructure in the country needs serious improvement. In Massachusetts alone, we have got between $10 to $15 billion of a maintenance backlog for water potability and riverine and littoral resilience.

I submitted four projects to the House Appropriations Committee requesting funding for critical water projects in Massachusetts. And, unlike Boston, which has the scale and the scope to have a sophisticated IT component to its water and sewer public works, these towns are small, and they don’t necessarily have those kinds of resources, and have the ability to have that type of expertise on standby.

So, in addition to making investments in water potability itself, we need to be making investments in securing that critical infrastructure from cyberattacks.

Mr. Sullivan, the Boston Water and Sewer Commission, where you are the chief engineer, as you said, has suffered from a ransomware attack last year. And in your testimony you noted that, because the business network was segregated from the control system, there was never any threat to public or environmental health.

And just to give you a sense of the divergence, in terms of Boston’s scale and some of the towns in my district, Norton, which is a town that recently launched a new, $11 million water treatment plant in February 2020 that has been exceptionally effective, that has a base of about 20,000 residents. Boston has a base of about 675,000 residents, so two orders of magnitude here, almost.

Has the Boston Water and Sewer Commission been able to communicate with these smaller Massachusetts entities about best practices, should they be attacked, or even been able to form a collaborative regional working group, so that there is some sort of umbrella protection from the bigger cities?

Mr. SULLIVAN. Well, we work with all the Massachusetts—through the Mass WARN system, should something come up. But we recommend to them that they actually join the WaterISAC, because you get national exposure.

It is difficult sometimes, when an entity as large as ours is talking, and we talk about, "You should buy this, buy that," and the smaller towns go, "How are we going to afford it, and who is going to run it?" So, it is better that they go to a national one, who has like-size utilities, where we can put them in touch with them, and they can communicate on the same level how they took care of it, because we do operate in different levels of scope.

The treatment systems are all the same. It is the size of the system, and whether it is fully automated, or whether you have a 24/7 operator watching the screen, as Oldsmar did. I mean, they happened to be lucky. They watched the screen, and it was moving because someone got in on their system.

The other problem we have with some of the smaller systems is they want to tie into the internet, so they can use things like TeamViewer, which was at Oldsmar, so that they can operate these remotely. During COVID, it was one of the biggest things: How can I run my automated plant remotely?

So, we have got to get away from that. We have got to get them down to a much securer system that is run where the OT is totally separate from the IT. And we do talk to the different communities, and we are always open. But again, we try to refer them to someone of like size who has had the same problems.

Mr. AUCHINCLOSS. So, if I could recapitulate what you are saying here, it is—you would encourage them to join WaterISAC, you would encourage them to separate—or to not permit a remote operation, to require onsite operation.

Any further recommendations that you would give to smaller towns, IT departments in particular?

Mr. SULLIVAN. Well, one of the other problems is, in small towns, the IT department may reside at the townhall, and not necessarily with the water or wastewater department. And so, they communicate occasionally, but they don't really live the IT issues. And that we see in many of the small towns, it is part of city government, town government.

And I am not aware exactly how the Norton system is set up, if there is even an IT expert working for the water department. Many times, it is someone released to them from the town. So, I would need to look into it.

Mr. AUCHINCLOSS. Mr. Sullivan, I appreciate the answers and the work that you are doing to ensure the resilience of our water infrastructure in Massachusetts.

The Chair yields the balance of his time, and the Chair recognizes the gentlelady from Puerto Rico, Miss González-Colón.

[Pause.]

Mr. AUCHINCLOSS. The Chair recognizes Mr. Guest.

Mr. GUEST. Thank you, Mr. Chairman.

To our panel, Congress has tasked CISA, the Cybersecurity and Infrastructure Security Agency, as the lead agency in both protecting our cyber and defending against any cyber threats and cyberattacks. I would like, if the panel would, to please provide any information, any insight with your interaction with CISA, the benefits that they have provided, and any shortcomings that you see that may exist between CISA's interaction and the interaction with your industry or your particular company.

[Pause.]

Mr. KESSLER. Since nobody else is jumping in, I will jump in.

The interactions that I have had with CISA actually have been primarily through Coast Guard colleagues who are doing tours at CISA. I think CISA has started to take a lead role with Coast Guard in some of the protections in ports. I think they have done a really good job at trying to get the word out and take that role.

I have also some colleagues in the energy field, who are doing some work with CISA.

The work that I have seen from CISA and the output from the agency seems to be appropriate. You know, there is always more that we can do. I think that is one of the recurring themes here. But I think they have done an excellent job, and I don't really have anything I would point to right now and say that they are deficient.

Ms. SAMFORD. This is Megan Samford. I am happy to comment on that, as well.

I applaud Department of Homeland Security and CISA, actually. I think that they have a tremendous mission. I think that their scope is one of the largest that the Federal Government has.

It has been my experience that, especially when dealing with vulnerability handling and coordination, the entity—I think the name has changed now, but it used to be known as ICS–CERT out in Idaho. Despite any company I have worked with over the past decade, I have been able to call that team, and we have been able to work through issues. They have always been at the ready.

Mark Bristow, who currently leads their hunting team there, he is also an advocate. He is one of the other four people that are currently credentialed as an incident commander for cyber under the FEMA system.

They believe the construct can work. They do a really good job at templating exercise material response plans. In many cases, I think that these materials are underutilized, or the private sector simply isn't educated on. If the private sector were more educated on the resources available through CISA, I think that we would see greater utilization of that agency. But I hold them in very high regard.

Can agencies improve? Yes, of course. But my interactions with that entity have been very good.

Mr. GUEST. And Ms. Samford, let me follow up on it just a little bit. You talked a little bit about the raising awareness, the education of CISA. What can Congress do to make sure that we are educating our businesses, educating our key industries on, first, the existence of CISA, because I think many people have never heard of CISA. If you are not in the homeland security realm, CISA is just another acronym, and you have no idea what it stands for.

But with the recent cyberattacks that we have seen, and the threats of growing cyberattacks, whether that be criminal elements, rogue nations who are using cyberattacks to—either espionage, ransomware—what can we, as Congress, do to better educate?

Because what we want people to do is we want them to be aware of CISA, of what the benefits CISA has to offer when there is an attack. We would like for them then to report that to CISA, so that we can investigate and try to go forward.

And so, do you have any thoughts on what we can do to, again, improve that awareness of this agency?

Ms. SAMFORD. Sure, thank you. Thank you, and that is a great question.

I believe that any public show of support for CISA and its efforts, I think that that is a tremendous deal.

I can tell you there was one program in particular that I think CISA and Department of Homeland Security have been especially successful at since the Department was stood up, and that is the Protective Security Adviser program.

The Commonwealth of Virginia—I was actually working in the Governor's office of Tim Kaine at the time, but Virginia was the first State to have a pilot program for protective security advisers, and now every State has at least one protective security adviser.

But this individual, that is exactly what their job is, is they go out to the designated critical infrastructures, and they do physical security site assessments. And now I understand that CISA has cybersecurity advisers that accompany the protective security advisers. And so, they are kind of two in a box, visiting these infrastructures, wastewater treatment facilities, you name it, and they are talking about the different programs that CISA can offer to them.

So, I think any public show of endorsement for these programs and CISA and the direct interaction with the private sector is definitely appreciated at all levels.

Mr. GUEST. Thank you, Mr. Chairman——

Mr. AUCHINCLOSS. The gentleman's time has expired.

Mr. GUEST [continuing]. I am over time, I yield back.

Mr. AUCHINCLOSS. Thank you, the gentleman yields, and that concludes our hearing.

I would like to thank each of our witnesses for your testimony today. Your comments were informative and helpful.

I ask unanimous consent that the record of today's hearing remain open until such time as our witnesses have provided answers to any questions that may be submitted to them in writing.

I also ask unanimous consent that the record remain open for 15 days for any additional comments and information submitted by Members or witnesses to be included in the record of today's hearing.

Without objection so ordered.

The committee stands adjourned.

[Whereupon, at 1:19 p.m., the committee was adjourned.]

SUBMISSIONS FOR THE RECORD

Prepared Statement of Hon. Frederica S. Wilson, a Representative in Congress from the State of Florida

Thank you, Chairman DeFazio for today's hearing.

Gaps in the transportation sector's ability to defend, detect, and respond to cybersecurity incidents threaten residents of Florida and the nation at large.

For example, the cyberattack on the Oldsmar water treatment facility had the potential to contaminate drinking water for 15,000 Florida residents.

Improving cybersecurity needs to be a top priority through strong industry and governmental partnerships and effective standards to avert attacks on facilities and systems, such as the Turkey Point Nuclear Generating Station located in South Florida.

In addition, we must take actionable steps to increase our cybersecurity workforce and work to make these jobs accessible for all communities.

I look forward to working with my colleagues and the private sector to enhance our nation's cybersecurity preparedness, increase the cybersecurity workforce, and protect citizens.

With that, I have a few questions.

Appendix

QUESTION FROM HON. EDDIE BERNICE JOHNSON TO SCOTT BELCHER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, SFB CONSULTING, LLC, ON BEHALF OF MINETA TRANSPORTATION INSTITUTE

Question 1. Mr. Belcher: What amount of funding do you believe Congress should provide to assist individual transit agencies, like Dallas Area Rapid Transit, with increasing their cybersecurity programs?

ANSWER. Most transit agencies do not currently have the necessary funding to effectively begin addressing their cybersecurity needs. Unfortunately, there is not a specific amount that each transit agency should receive because each transit agency is unique and is at a different level of cyber maturity. Factors that should be considered when determining how much an individual agency should invest in cybersecurity preparedness include the risk and threats posed to the organization and the risk tolerance of the organization. At a minimum, transit agencies should have an understanding of the cyber risk and threats posed to their organization, and have assessed their current cyber risk program based on their risk tolerance. This resulting understanding of cyber risk should be factored into the agency's business continuity planning and incident response plans. If a transit agency has not taken these steps, then funding should be provided to help with these fundamentals. The understanding of cyber risk will also inform an estimate of the agency's immediate and long-term capital needs. As a start, Congress should provide funding for each agency to conduct a cyber risk assessment and integrate its assessment into its business continuity planning and incident response plans. These basics would then enable each agency to effectively convey their needs for additional resources for an ongoing cyber risk program to effectively mitigate and manage their identified cyber risk.

QUESTION FROM HON. FREDERICA S. WILSON TO SCOTT BELCHER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, SFB CONSULTING, LLC, ON BEHALF OF MINETA TRANSPORTATION INSTITUTE

Question 2. Mr. Belcher: In your testimony, you mentioned that "one of the key foundations for cybersecurity programs across any industry comes from the National Institute of Standards and Technology."

a. Why is this agency's cybersecurity framework important and how can it be improved?

ANSWER. The foundation for much of the United States' cybersecurity efforts, including those of the Department of Homeland Security (DHS) and U.S. Department of Transportation (U.S. DOT), is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST Framework). NIST is a non-regulatory agency: it has no authority to dictate the use of any particular standard. However, when there is a matter of public good that depends on establishing a standard, NIST convenes relevant public and private stakeholders to develop a standard, as they have done in the face of cybersecurity threats.

In February 2014, NIST released the NIST Framework for Improving Critical Infrastructure Security in response to Presidential Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[1] which called for a standardized security framework for critical infrastructure in the United States. It is not a how-to guide for cybersecurity; rather, it is a framework designed to help a wide range of organizations assess risk and make sound decisions about prioritizing and allocating resources to reduce the risk of compromise or failure among their systems.

[1] Barack Obama. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, 78 FR 11737, February 19, 2013, https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

For any industry or organization to leverage the NIST Framework, customized implementation is required in ways that are not necessarily obvious from the document. An entire industry has emerged of cybersecurity practitioners, software tools, consultants and advisors that leverages the NIST Framework as its basis for delivering services to its customers. For the transportation sector to effectively leverage the wares of this growing industry, it too must support the use of the NIST Framework.

QUESTIONS FROM HON. COLIN Z. ALLRED TO SCOTT BELCHER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, SFB CONSULTING, LLC, ON BEHALF OF MINETA TRANSPORTATION INSTITUTE

Question 3. Mr. Belcher, in your testimony you mentioned the importance of cybersecurity preparedness and support for cybersecurity programs, as well as possibly using both a carrot and stick approach to ensure that public and private entities are using the necessary resources. What carrots and sticks do you recommend? And what minimum cybersecurity standards do you believe every transit company, both public and private, should adopt?

ANSWER. In the Mineta Transportation Institute (MTI) study entitled "*Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*,"[2] my colleagues and I provide a number of recommendations that fall into each category. In the "carrot" category, we recommended that:

- Congress should increase formula grant funding to transit agencies to ensure that they have sufficient resources to meet the minimal cybersecurity standards established above
- Congress should increase funding to DHS and U.S. DOT to develop and promulgate a set of minimal cybersecurity standards and tools and to help with their promotion
- DHS and U.S. DOT should provide technical guidance to transit agencies on the collection, retention, and assessment of system logs
- The American Public Transportation Association (APTA), working with other stakeholders, should develop a clearinghouse for cybersecurity best practices, in particular for small and medium transit operations
- APTA, working with other stakeholders, should create minimum guidelines for cybersecurity audits
- APTA, working with other stakeholders, should develop model cybersecurity contract language for agencies to integrate into their vendor contracts
- APTA, working with other stakeholders, should develop a model incident response plan, business continuity plan, continuity of operations plan, crisis communications plan, and disaster recovery plan that can be tailored to meet the needs of public transit organizations of varying sizes and needs
- APTA, working with other stakeholders, should continue to develop cybersecurity training modules and certificates

In the "stick" category, we recommend that:

- Congress should ensure through its oversight powers that U.S. DOT and DHS work together to improve cybersecurity preparedness within the Transportation Systems Sector (TSS)
- DHS and U.S. DOT, the TSS co-sector specific agencies for transit, working with input from APTA and other industry organizations, should promulgate a set of minimum cybersecurity standards
- The Federal Transportation Administration (FTA), working with DHS, should create an attestation program, whereby transit CEOs are required to attest that their organization has met the minimum cybersecurity standards established above prior to receiving federal funds
- FTA, working with DHS and other relevant federal agencies, should require that transit agencies either outsource management of payment data to Payment Card Industry (PCI)-compliant vendors, or require that their CEO attest that they are PCI-compliant prior to receiving federal funds

Question 4. Mr. Belcher, in your testimony you also mentioned the different agencies that provide cybersecurity preparedness support or guidance. In the transportation space, these agencies include the National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), DOT,

[2] Mineta Transportation Institute, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf

Homeland Security and TSA as critical cybersecurity players. While some of these agencies do not have regulatory authority, are there any concerns with having so many different agencies responsible for leading different cybersecurity efforts?

ANSWER. On February 12, 2013, the White House released Presidential Policy Directive 21 outlining the federal government's responsibility to strengthen the security and resilience of U.S. critical infrastructure against both physical and cyber threats.[3] The Directive established that DHS and U.S. DOT share responsibility for the TSS. In sharing this role, the DHS's and U.S. DOT's responsibilities include:

- Collaborating with critical infrastructure owners and operators
- Coordinating with state, local, tribal, and territorial entities to implement the directive
- Providing, supporting, or facilitating technical assistance and consultations to identify vulnerabilities and help mitigate incidents in the sector

While there are multiple agencies providing guidance in this space, it was not until December 2021, that TSA issued Transportation Security Directive 1582–21–01, "Enhancing Public Transportation and Railroad Cybersecurity"[4] applying to Public Transport/Public Rail owners and operators and required that they:

- Designate a cybersecurity coordinator
- Report cyber incidents to CISA within 24 hours of detection
- Complete a vulnerability assessments of their networks; and
- Develop a cybersecurity incident response plan based on security issues discovered

The FTA was part of the deliberations that led to the release of this Transportation Security Directive. I believe that this is the beginning of the new Administration's approach to cybersecurity and is likely to be the first of a series of Security Directives and/or regulations. I believe that working together, the TSA and the U.S. DOT as co-leads for this TSS, are the appropriate bodies to issue any mandatory requirements for the transit industry. Combined, they have a thorough understanding of appropriate cybersecurity protective measures and an in-depth understanding of the industry.

Question 5. If so, which of these agencies should take the lead and what kind of restructuring should occur?

ANSWER. See answer above.

QUESTION FROM HON. FREDERICA S. WILSON TO MEGAN SAMFORD, VICE PRESIDENT, CHIEF PRODUCT SECURITY OFFICER–ENERGY MANAGEMENT, SCHNEIDER ELECTRIC, ON BEHALF OF THE INTERNATIONAL SOCIETY OF AUTOMATION GLOBAL CYBERSECURITY ALLIANCE

Question 1. Ms. Samford: Thank you so much for your testimony. I agree with your position that a bipartisan effort is necessary to effectively implement the Incident Command System for Industrial Control Systems at scale.

a. Please explain the importance of private and public sectors working together to effectively manage cyber incidents.

ANSWER. The ICS4ICS program is creating Incident Command System capabilities that will enable private companies of various sizes to improve their response to cybersecurity incidents, especially those with Operational Technology and Industrial Control Systems. It will also create a consistent process for the US Department of Homeland Security to interface with, and support responses in the private sector. Today, no such process exists to ensure common terms, processes, and tools. The following critical infrastructure sectors heavily depend on Industrial Control Systems for their operations: chemical, energy, and pipelines; water and wastewater; critical manufacturing; dams; transportation including streetlights, aviation, and public transportation; and buildings that support hospitals, government agencies, and private companies. 85% of the critical infrastructure of the United States is owned and operated by private companies. The remaining 15% are owned and operated by local, state, tribal, and federal government agencies. ICS4ICS is based on an informal public-private partnership with FEMA and DHS who have contributed significant capabilities and resources to the ICS4ICS program.

[3] Barack Obama, Presidential Policy Directive-21, Washington, D.C.: The White House, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[4] Transportation Security Agency, Transportation Security Directive 1582–21–1, Washington, D.C., Enhancing Public Transportation and Railroad Cybersecurity, effective December 31, 2021, https://www.tsa.gov/sites/default/files/sd-1582-21-01__signed.pdf.

ICS4ICS membership is continuing to expand rapidly with 700 individuals currently on our distribution list. ISAGCA has funded this private sector effort to develop ICS4ICS but will not be able to meet the funding needs as the program expands. ICS4ICS was developed by leveraging FEMA and DHS capabilities, processes, and tools. Currently, ICS4ICS is focused on Type 3 (single-company, single-site/asset) incidents. The program will be expanded in 2022 to address Type 2 (single-company, multiple sites/assets) incidents. ICS4ICS will not be able to address nation-wide incident (Type 1) without a formal public-private partnership. DHS CISA currently provides information about cyber-attacks and will need to expand their coordination role in a nation-wide attack impacting an entire critical infrastructure sector or possibly multiple sectors. ICS4ICS will enable public and private parties to work together more easily because they will have common terms, processes, and tools. ICS4ICS will also enable public and private companies to establish mutual aid agreements through credentialling of ICS4ICS staff based on roles and by having a common methodology.

QUESTION FROM HON. COLIN Z. ALLRED TO MEGAN SAMFORD, VICE PRESIDENT, CHIEF PRODUCT SECURITY OFFICER–ENERGY MANAGEMENT, SCHNEIDER ELECTRIC, ON BEHALF OF THE INTERNATIONAL SOCIETY OF AUTOMATION GLOBAL CYBERSECURITY ALLIANCE

Question 2. We often only hear or see reporting on the most well-known attacks against larger companies like Colonial Pipeline, but smaller businesses and companies are potentially more vulnerable to attacks than larger companies. Ms. Samford, what additional resources should the federal government provide to smaller businesses?

ANSWER. The federal government should recommend the use of the FEMA Incident Command System to the private sector, and in particular, smaller businesses because it will greatly aid in helping them create incident response plans, common terminology, as well as a framework for working with the federal government when they need support. FEMA has numerous Incident Command Systems tools, templates, and training that can be leveraged by public and private sector small or large. The ICS4ICS tools and templates could be added to the FEMA site and customized for small businesses. The DHS Control System Exercise Package could be leveraged as a model to create an ICS4ICS Exercise Package for small businesses. Some of the ICS4ICS tools and templates should be updated to address the needs of small businesses and align with the DHS Exercise Package for small businesses. A registry could be established for parties willing to provide mutual aid which would likely significantly benefit small businesses who don't have the procurement staff to create these types of agreements. FEMA classroom training course information could be widely shared with small businesses which would allow them to participate for free when extra seats are available.

QUESTION FROM HON. FREDERICA S. WILSON TO THOMAS L. FARMER, ASSISTANT VICE PRESIDENT–SECURITY, ASSOCIATION OF AMERICAN RAILROADS

Question 1. Mr. Farmer: Thank you for your testimony. I want to applaud the collaboration of railroads in their efforts to strengthen cybersecurity. I am the current sponsor of a rail safety resolution that is introduced every year. And even though it focuses on collisions, in 2022, a cybersecurity element may be needed. In your testimony, you mention that TSA directives are unnecessary and can undermine the work the rail industry has done over the last 20 years.

a. You indicate the benefit of a collaboration between government and the rail industry. How would government mandates erode the benefit of this collaboration, especially if these mandates would protect this critical industry?

ANSWER. Representative Wilson: Thank you very much for your commendation of the collaborative efforts that railroads maintain, and strive continuously to enhance, to protect networks and assure safe and resilient operations. As your question indicates, the railroads value collaboration not only among freight and passenger railroads, but also with other transportation modes, other industries, and government agencies.

Our unwavering focus is on assuring timely access to assessments, analyses, and reporting on cyber threats and incidents to inform vigilance; and on having the capability to detect cyber-attacks and prevent breaches. It is vital that railroads be flexible and nimble to counter an ever-evolving threat.

AAR's general concern with government mandates is that they potentially undercut the railroads' efforts to be prepared for cyber-attacks. Government mandates inevitably alter the nature and quality of the interaction between government and industry. The priority shifts from what can be attained collaboratively for cybersecurity enhancement to complying with the terms of the mandates—what actions are expressly required and whether the covered organization has implemented all mandated measures.

Regarding the recent security directives, AAR's cyber team worked tirelessly with the TSA and other federal stakeholders to make significant revisions to shape the directives into what they are today:

1. designate a cybersecurity coordinator;
2. report cybersecurity incidents to CISA within 24 hours;
3. develop and implement a cybersecurity incident response plan to reduce the risk of an operational disruption; and,
4. complete a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems.

AAR does not object to the substance of these mandates. As a matter of fact, the railroads are already substantially in compliance. However, the process by which the mandates was issued was not ideal. The public notice and comment period used to promulgate federal regulations would have afforded ample time and opportunity to address these matters and produced a stronger outcome overall. Railroads take cyber threats seriously. We value our productive work with government partners to keep the rail network safe from cyber and physical threats—as we have done for decades and will continue to do for many more.

QUESTIONS FROM HON. FREDERICA S. WILSON TO MICHAEL A. STEPHENS, GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT FOR INFORMATION TECHNOLOGY, HILLSBOROUGH COUNTY AVIATION AUTHORITY, TAMPA INTERNATIONAL AIRPORT

Question 1. Mr. Stephens: Thank you for your testimony. Adopting a non-voluntary cybersecurity mitigation strategy can be effective in preventing attacks on airports, airlines, and critical aviation information systems.

a. Please explain the significance and need for implementing a non-voluntary, baseline cybersecurity standard to best protect the aviation industry.

ANSWER. As attacks and threats become more prevalent and damaging, we cannot afford as a nation for our critical infrastructure sectors to experience a catastrophic event before we

The current posture for many critical infrastructure entities is to be often reactive rather than proactive when mitigating cyber risks—for example, delaying essential mitigation activities such as patching and updates. This reactive posture is usually not because of lack of willingness but is often due to low prioritization or financial constraints. The reactive post, in my opinion, also occurs because there is often no oversight or requirement to do so. However, I believe that we are at an inflection point where this is no longer acceptable. The most apparent benefit of mandatory standards is that they incentivize entities to actively implement the necessary measures, processes, and policies for an improved security posture, thereby reducing the risk of an entity getting breached. If a breach occurs, it significantly increases the chances that the entity will be better prepared with incident responses and continuity plans to minimize damage and mitigate risks.

Question 2. Mr. Stephens: You state that "closing the human factors gap is a critical and integral part of a successful and effective cyber resilience strategy," and suggest a uniform standard that establishes a minimum baseline training requirement.

a. What would an ideal baseline standard look like from your perspective?

ANSWER. It is my opinion that standards currently exist that airports and key aviation sector stakeholders can easily adopt that to enhance their cybersecurity preparedness and resiliency. These standards include guidance that focuses on "human factors," such a reoccurring awareness and preparedness training related to cyber threats. As discussed during the hearing, the NIST standard and the COBIT 5 standard offer excellent opportunities for airports to build robust threat mitigation and cybersecurity programs.

It is important to note that airports are very different with respect to their organization and operations. Therefore, a one-size-fits-all approach would be highly inadvisable, and I believe, ineffective. The TSA and the FAA can begin to more actively encourage airports to adopt and implement a standard of the airport or stakeholders' choice as a component of their System Security Plan. Airport stakeholders should be given the flexibility to adopt standards and mitigation measures that best fit their unique structures and risks.

QUESTION FROM HON. COLIN Z. ALLRED TO MICHAEL A. STEPHENS, GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT FOR INFORMATION TECHNOLOGY, HILLSBOROUGH COUNTY AVIATION AUTHORITY, TAMPA INTERNATIONAL AIRPORT

Question 3. Mr. Stephens, as the government puts more focus on cybersecurity preparedness measures, how do you suggest that we incentivize private companies to address cybersecurity issues in the aviation sector?

ANSWER. I believe that, where appropriate, incentives are often the preferable path to adopting and accepting cyber security standards as opposed to mandates in the aviation sector. A few areas where I believe there is an opportunity are the Federal grants process. Entities that have demonstrated greater preparedness, whether through the adoption or implementation of cyber standards, could potentially be given more significant consideration. Grant programs such as the FAA's programs on workforce development, AIP program, or other grant programs for safety and security enhancements are potential starting points.

Moreover, cyber requirements should be embedded into the procurement process where Federal funds are involved over a certain dollar threshold. This would potentially incentivize private sector entities who wish to do business with airports to focus on cybersecurity preparedness measures. Another incentive could come in the form of limiting liability for cybersecurity breaches under current law in exchange for implementing certain baseline standards.

QUESTIONS FROM HON. FREDERICA S. WILSON TO JOHN P. SULLIVAN, P.E., CHIEF ENGINEER, BOSTON WATER AND SEWER COMMISSION, ON BEHALF OF THE WATER INFORMATION SHARING AND ANALYSIS CENTER

Question 1. Mr. Sullivan: Thank you for your testimony. You highlight that there is no statutory requirement for wastewater systems to take an "all-hazards" look at potential threats, including cyber risk. Furthermore, you discuss the development of a wastewater sector program, like the EPA's oversight of drinking water.

a. What legislative approach to federal oversight of wastewater systems would you recommend, and how would it incorporate cybersecurity?

ANSWER. While WaterISAC takes no position on the federal regulation of the cybersecurity practices of wastewater systems, my testimony notes that America's Water Infrastructure Act of 2018 (P.L. 115–270) requires drinking water utilities, under the oversight of EPA, to periodically take an "all-hazards" look at potential threats, including risks to "electronic, computer, or other automated systems." Subject matter experts have noted that Congress could consider extending this same requirement to the nation's wastewater systems, directing them to similarly make periodic evaluations of their cybersecurity posture. While some assistance may be necessary to help small wastewater systems complete this task, other wastewater systems—such as those that are part of joint utilities with drinking water systems—could likely fulfill this requirement fairly easily. This would also serve to put both drinking water and wastewater systems on equal regulatory footing, in terms of physical and cybersecurity requirements, thus providing the entire water sector with a consistent baseline on which to build any future security policies.

Question 2. Mr. Sullivan: A Water Sector Coordinating Council survey found that nearly 40 percent of respondents did not have cybersecurity as part of their risk management plans; many of them were smaller water and wastewater systems that lack the funding and expertise.

a. What can be done to provide these smaller systems with resources and technical assistance to make cybersecurity a meaningful part of their operations?

ANSWER. One of the most effective things the federal government can do to help small water and wastewater systems improve their cybersecurity posture is to offer voluntary technical assistance and financial aid to connect these small systems with best practices and information sharing resources that are available in the water sector. For example, my testimony notes that the recently enacted Infrastructure Investment and Jobs Act authorizes a new Department of Energy program that aims to improve the cyber resilience of utilities in the bulk power sector. Specifically, the new program will facilitate the delivery of technical assistance and work to expand participation in the Electricity Information Sharing and Analysis Center, which is WaterISAC's counterpart in the electricity sector. I believe a similar EPA program, focused on offering cybersecurity technical assistance to small water and wastewater systems, while also supporting the membership of these systems in WaterISAC, could greatly increase the cyber awareness of water systems from coast to coast. This, in turn, will help the operators of these systems become aware of the threat landscape, protect themselves against cyber attacks, and implement measures that make their water systems less vulnerable.

Question from Hon. Garret Graves to John P. Sullivan, P.E., Chief Engineer, Boston Water and Sewer Commission, on behalf of the Water Information Sharing and Analysis Center

Question 3. Earlier this year we saw that impact of a hack into a water system in Oldsmar Florida (near Tampa), with the hacker increasing the amount of sodium hydroxide (lye) in the water by a factor of more than 100 (FYI sodium hydroxide is the main ingredient in liquid drain cleaners like Drano®, in smaller quantities it tempers the water's acidity).

During the first reconciliation markup and on the floor, I offered an amendment which would have authorized $50 million for an EPA grant program to help municipalities keep their systems secure. This amendment was not adopted by the committee or by the full House.

Do you think that this amendment would have been helpful to safeguard drinking water from hackers?

Answer. While I am not familiar with the specific details of that amendment, water and wastewater systems would certainly benefit from additional EPA aid to keep their systems secure against threats from cyberspace and elsewhere. In fact, two provisions included in the recently enacted Infrastructure Investment and Jobs Act would make progress toward this goal. Sections 50107 and 50205 of that new law authorize respective drinking water and wastewater utility resilience and sustainability programs at EPA to help utilities undertake projects to protect against cyber threats, extreme weather events, and other natural hazards. Funding these and similar programs to increase water and wastewater system preparedness to a range of threats would certainly help all utilities become more secure.

Question from Hon. Frederica S. Wilson to Gary C. Kessler, Ph.D., Nonresident Senior Fellow, Atlantic Council

Question 1. Dr. Kessler: Thank you so much for your testimony. You highlighted the significant uptick in cyberattacks targeting the Maritime Transportation System. This is a very important issue to me because PortMiami is located in South Florida. I agree that a focus on mitigating cyber risks should not only target threats, but also vulnerabilities.

a. You stated that a critical defensive tactic is related to intelligence sharing. Why is information sharing so important for defending against cyberattacks and ensuring that all organizations, regardless of size, can safeguard themselves?

Answer. Thank you, Congresswoman Wilson, for this question. We address this issue in the Atlantic Council report, as Recommendation #3, one of the high priority responses that we believe will elevate the effectiveness of cybersecurity practices. It is an issue near and dear to my heart.

Information and intelligence sharing works on at least a couple of levels. First, the Maritime Transportation System (MTS) has at least the same cyber issues as all other users of computers and technology. Given all of the cyber issues that are common to everyone, then it just makes sense to openly share known vulnerabilities in software and hardware. These efforts are already largely in place with programs such as MITRE's Common Vulnerabilities and Exposures (CVE) database, NIST's National Vulnerability Database (NVD), and periodic cybersecurity warnings from CISA and vendors.

Within the MTS, we can be more open in sharing particular threats against our industry and computer systems specific to maritime. Indeed, sharing actual case studies of attacks that have occurred and the lessons learned would be very valuable to the entire community.

There are those who opine that openly sharing vulnerabilities informs the Bad Guys and does not give vendors enough time to fix the problems. I would observe that historically, for at least the last 30 years on the public Internet, the attacker community has always been better informed than the target community. Keeping vulnerabilities secret from potential victims while waiting for vendors to create a patch leaves a lot of systems unaware, unarmed, at risk, and unable to take any potential protective measures on their own.

Secondly, while I believe that we need to focus on cyber vulnerabilities, we also need to be cognizant of all threats directed at us. By way of example, if I was the Port of Miami, I would be interested in any and all threat intelligence directed at anything related to my organization's operation, including threats against:

- The MTS, in general;
- Ports, in general, or my port, in particular;
- Any ship or shipping line doing business in my port;
- Any inter-modal carrier with a presence at my port;

- The U.S., Florida, Miami-Dade County, or the City of Miami;
- Any port personnel, officers of the Miami-Dade Seaport Department, or any other officials or officers associated with PortMiami (all identified, by the way, in the port's Annual Report, available online); or
- Industry meetings, particularly those related to port operations.

The community of attackers—and the attackers do communicate and share information—is very informed and have bad intentions. Potential victims need to be armed with as much information as possible in as timely a fashion as possible.

Please let me know if I can provide any other information or clarification.

THE EVOLVING CYBERSECURITY LANDSCAPE: FEDERAL PERSPECTIVES ON SECURING THE NATION'S INFRASTRUCTURE

THURSDAY, DECEMBER 2, 2021

HOUSE OF REPRESENTATIVES,
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
WASHINGTON, DC.

The committee met, pursuant to call, at 10:04 a.m. in room 2167 Rayburn House Office Building and via Zoom, Hon. Peter A. DeFazio (Chair of the committee) presiding.

Members present in person: Mr. Larsen, Mr. Carson, Mr. DeSaulnier, Mr. Carbajal, Mr. Stanton, Ms. Davids of Kansas, Mr. Auchincloss, Ms. Strickland, Ms. Newman, Mr. Graves of Missouri, Mr. Crawford, Mr. Perry, Mr. Rodney Davis, Dr. Babin, Mr. Bost, Miss González-Colón, Mr. Balderson, Mr. Stauber, and Mr. Burchett.

Members present remotely: Mr. DeFazio, Ms. Norton, Ms. Johnson of Texas, Mrs. Napolitano, Mr. Cohen, Ms. Titus, Ms. Brownley, Mr. Payne, Mr. Lynch, Mr. Malinowski, Mr. Allred, Mr. García of Illinois, Mr. Delgado, Mr. Lamb, Ms. Bourdeaux, Ms. Williams of Georgia, Mr. Carter of Louisiana, Mr. Gibbs, Mr. Massie, Mr. Katko, Mr. Graves of Louisiana, Mr. Rouzer, Mr. Weber, Mr. Mast, Mr. Fitzpatrick, Mr. Johnson of South Dakota, Dr. Van Drew, Mr. Guest, Mr. Nehls, Ms. Van Duyne, and Mrs. Steel.

Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

Peter A. DeFazio
Chairman

Katherine W. Dedrick, Staff Director

Sam Graves
Ranking Member

Paul J. Sass, Republican Staff Director

NOVEMBER 29, 2021

SUMMARY OF SUBJECT MATTER

TO: Members, Committee on Transportation and Infrastructure
FROM: Staff, Committee on Transportation and Infrastructure
RE: Full Committee Hearing on "The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure"

PURPOSE

The Committee on Transportation and Infrastructure will meet on Thursday, December 2, 2021, at 10:00 a.m. EST in 2167 Rayburn House Office Building and via Zoom, to hold a hearing titled "The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure." The Committee will hear testimony from Mr. Cordell Schachter, Chief Information Officer (CIO), Department of Transportation (DOT); Mr. Larry Grossman, Chief Information Security Officer (CISO), Federal Aviation Administration (FAA); Ms. Victoria Newhouse, Deputy Assistant Administrator for Policy, Plans, and Engagement, Transportation Security Administration (TSA); Rear Admiral John W. Mauger, Assistant Commandant for Prevention Policy, U.S. Coast Guard (USCG); Mr. Kevin Dorsey, Assistant Inspector General for Information Technology Audits, DOT Office of Inspector General (DOT OIG); and Mr. Nick Marinos, Director of Information Technology and Cybersecurity, Government Accountability Office (GAO).

BACKGROUND

CYBERTHREATS TO THE U.S. TRANSPORTATION AND INFRASTRUCTURE SECTORS

Cyberattacks are a serious and evolving risk that affect transportation and infrastructure matters across T&I's jurisdiction. Cyberattacks can result in tremendous financial damage, destruction of infrastructure assets, and even death.[1] They impact governments, businesses, and individuals alike and have been growing in number and sophistication.[2] This hearing is the second of two full committee hearings on cybersecurity of the nation's infrastructure.[3] The first hearing was held in November 2021 and featured testimony from industry stakeholders and cybersecurity experts.[4] As discussed in the November hearing, cyberattacks on the nation's critical infrastructure—about 85 percent of which is owned and operated by private enti-

[1] Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," (February 2018), available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf; Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, (October 14, 2018), available at https://tech.industry-best-practice.com/2018/10/14/the-untold-story-of-notpetya-the-most-devastating-cyberattack-in-history/

[2] Id.

[3] House Committee on Transportation and Infrastructure, "The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure,"(December 2, 2021), available at https://transportation.house.gov/committee-activity/hearings/the-evolving-cybersecurity-landscape-federal-perspectives-on-securing-the-nations-infrastructure; House Committee on Transportation and Infrastructure, "Hearing: The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure," available at https://transportation.house.gov/committee-activity/hearings/the-evolving-cybersecurity-landscape-industry-perspectives-on-securing-the-nations-infrastructure

[4] Id.

ties[5]—can cause significant harm to the public. However, many private entities, as well as federal agencies, have not taken the necessary steps to prevent, prepare for, respond to, and recover from cyberattacks.[6] During the Committee's November hearing, witnesses discussed challenges that hamper infrastructure operators' preparedness and resilience, such as a shortage of qualified information technology staff, a lack of appropriate cybersecurity awareness training, and insufficient technical expertise.[7] Responsibility for cybersecurity of the nation's infrastructure is shared among many entities, including the federal government, state and local entities, and public and private infrastructure owners and operators.[8]

This hearing will feature federal witnesses and focus on (1) actions the federal government is taking to address cybersecurity and preparedness of the transportation and infrastructure sectors, and (2) challenges agencies face in securing their own computer networks and the steps they are taking to address these challenges and to implement recent federal cybersecurity directives and other actions.

Federal Agencies with a Role in Transportation and Infrastructure Cybersecurity

In 2013, the federal government established a framework to guide the cybersecurity efforts of critical infrastructure owners and operators, which is set forth in the *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*.[9] The plan organizes critical infrastructure into 16 sectors and designates a federal department or agency as the lead coordinator—or sector risk management agency—for each sector.[10]

The agencies listed below serve as the federal interface for the prioritization and coordination of sector-specific security and resilience efforts, including for cybersecurity. These respective sectors are within the committee's jurisdictional purview.

Sector	Sector Risk Management Agencies
Government Facilities	General Services Administration Federal Protective Service (DHS)[11]
Transportation Systems	Department of Transportation U.S. Coast Guard (DHS) Transportation Security Administration (DHS)[12]
Water and Wastewater Services	Environmental Protection Agency[13]
Dams	Department of Homeland Security (DHS)[14]

[5] GAO, "The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report," (June 26, 2009), p. 1, available at https://www.gao.gov/assets/gao-09-654r.pdf

[6] See for example, testimony of Scott Belcher and John Sullivan at House Committee on Transportation and Infrastructure, "Hearing: The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure," available at https://transportation.house.gov/committee-activity/hearings/the-evolving-cybersecurity-landscape-industry-perspectives-on-securing-the-nations-infrastructure

[7] "Hearing: The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure," available at https://transportation.house.gov/committee-activity/hearings/the-evolving-cybersecurity-landscape-industry-perspectives-on-securing-the-nations-infrastructure

[8] The White House, PPD–21 Presidential Policy Directive—Critical Infrastructure Security and Resilience, (February 12, 2013), available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[9] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience, p. 3, available at https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[10] NIPP, 2013 at p. 9.

[11] Department of Homeland Security and General Services Administration, "Government Facilities Sector-Specific Plan," 2015, available at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf

[12] Department of Homeland Security and Department of Transportation, "Transportation Systems Sector-Specific Plan," 2015, available at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

[13] NIPP, 2013 at p. 11.

[14] Id.

Sector	Sector Risk Management Agencies
Emergency Services	Department of Homeland Security (DHS)[15]

The responsibilities of sector risk management agencies include:[16]

- Coordination with the Department of Homeland Security (DHS) and other relevant departments and agencies, and collaboration with infrastructure entities on the protection of critical infrastructure, including cybersecurity threats;
- Providing and facilitating technical assistance for sector owners and operators to identify threats and vulnerabilities, improve cyber defenses, and help mitigate cyber incidents; and
- Participation in Sector-Specific Coordinating Councils, Government Coordinating Councils, and other coordinating bodies for their sector.[17]

Information Sharing and Analysis Centers

In addition to the above-mentioned federal assistance for cybersecurity, private industry offers assistance through sector-specific Information Sharing and Analysis Centers (ISAC). The concept of ISACs was first promulgated in Presidential Decision Directive–63 (PDD–63), signed on May 22, 1998.[18] Today the National Council of ISACs recognizes 26 industry specific ISAC organizations.[19] Typically, ISACs are nonprofit organizations that share information about threats, vulnerabilities, and mitigation within their particular sector.[20] Some also provide awareness training and assistance in responding to cyber and other security incidents.[21]

For example, in the water sector, the Water Information Sharing and Analysis Center (WaterISAC) partners with various organizations, including the American Water Works Association, the Association of Metropolitan Water Agencies, and the National Rural Water Association.[22] WaterISAC also maintains close contact with government agencies to access sensitive and classified security information.[23] WaterISAC acts as an information clearinghouse and provides analysis and resources to its members to "support response, mitigation, and resilience initiatives."[24]

Federal Cybersecurity Preparedness and Internal Weaknesses

While the federal government supports private actors regarding cybersecurity in critical infrastructure, significant work is needed within federal government agencies to improve their own cybersecurity defenses. In March 2021, GAO identified ten critical actions needed to address major cybersecurity challenges.[25] The ten urgent needs fell under four major cybersecurity challenges previously identified by GAO, specifically: (1) Establishing a comprehensive cybersecurity strategy and performing effective oversight; (2) Securing federal systems and information; (3) Protecting cyber critical infrastructure; and (4) Protecting privacy and sensitive data.[26]

The report also noted that establishing the Office of the National Cyber Director within the Executive Office of the President, as Congress did in early 2021, was "an essential step forward" towards addressing cybersecurity.[27] Further, the recently passed Infrastructure Investment and Jobs Act directed $21 million for initial fund-

[15] Id.

[16] Id. at pp. 9–10.

[17] Id. at p. 43.

[18] "About ISACs," National Council of ISACs, available at https://www.nationalisacs.org/about-isacs

[19] "About NCI," National Council of ISACs, available at https://www.nationalisacs.org/about-nci

[20] National Council of ISACs web site, available at https://www.nationalisacs.org/about-isacs

[21] For example, Aviation ISAC offers training and incident response analysis see: https://www.a-isac.com/aboutus; Maritime Transportation System ISAC offers training and threat alerts see: https://www.mtsisac.org/services

[22] Water ISAC web site, available at https://www.waterisac.org/about-us

[23] Id.

[24] Id.

[25] GAO, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," (March 2021), p. 9, available at https://www.gao.gov/assets/gao-21-288.pdf

[26] Id. at p. 8.

[27] Id. at p. i.

ing for this office, ensuring the federal government will be better situated to confront the nation's cyber threats and challenges.[28]

However, the GAO report also said, "critical risks remain on supply chains, workforce management, and emerging technologies" and pointed out that in December 2020, "GAO reported that none of the 23 agencies in its review had fully implemented key foundational practices for managing information and communications technology supply chains."[29] In May 2021, GAO received updates from six of the 23 agencies regarding actions taken or planned to address its recommendations.[30] However, none of the agencies had fully implemented the recommendations.[31]

The report also highlighted the fact that since 2010, "GAO has made nearly 80 recommendations to enhance infrastructure cybersecurity" and that "nearly 50" of those recommendations have not been implemented heightening the risk to the nation's infrastructure.[32] Overall, since 2010, GAO has issued more than 3,700 recommendations across the federal government, including DOT and its subagencies, that could improve the nation's cybersecurity.[33] In July 2021, more than 950 of those recommendations remained unimplemented.[34]

Department of Transportation (DOT)

DOT and its 11 operating administrations and other components rely on hundreds of information technology systems for uses as diverse as air traffic control operations, disbursement of billions of dollars in loans and grants, managing sensitive personnel data, and many other functions key to DOT's mission.[35] The DOT OIG has identified information security as a top management challenge for the Department and stated that addressing these weaknesses and strengthening controls is essential for protecting departmental information technology (IT) infrastructure and improving DOT's cybersecurity posture.[36] These recurring cybersecurity weaknesses have resulted in key systems being vulnerable to cyberattacks, takeovers, and data breaches.[37] In addition, in the DOT OIG's most recent Top Management Challenges report released in late October 2021, they found that DOT needs a "holistic approach with sustained focus and direction" to resolve 66 open recommendations the DOT OIG made in previous audits.[38] These recommendations are intended to help address 10,663 security weaknesses identified in DOT plans of actions and milestones.[39] The DOT OIG has also identified cybersecurity weaknesses at the component agencies within DOT. Specific problems the DOT OIG has identified include the following:

- *Federal Transit Administration (FTA).* In October 2021, the DOT OIG released a report on cybersecurity weaknesses of FTA's financial management systems that could affect FTA's ability to approve, process, and disburse COVID–19 funds.[40] Among the OIG's findings: FTA has failed to fix security control weaknesses identified since 2016; it lacks sufficient contingency planning and incident response capabilities; and it "does not adequately monitor the security con-

[28] Liz Carey, "Infrastructure Act Includes $20M for Office of National Cyber Director," Homeland Preparedness News, (November 9, 2021), available at https://homelandprepnews.com/stories/74682-infrastructure-act-includes-20m-for-office-of-national-cyber-director/

[29] GAO, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," (March 2021), p ii, available at https://www.gao.gov/assets/gao-21-288.pdf

[30] GAO, "Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risk," (May 25, 2021), p 15, available at https://www.gao.gov/assets/gao-21-594t.pdf

[31] Id. at p. 13.

[32] GAO, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," March 2021, p. ii, available at https://www.gao.gov/assets/gao-21-288.pdf

[33] GAO, "Our Testimony to Congress on Efforts to Secure Oil and Gas Pipelines Against Cyberattacks," (July 28, 2021), available at https://www.gao.gov/blog/our-testimony-congress-efforts-secure-oil-and-gas-pipelines-against-cyberattacks-video

[34] Id.

[35] DOT OIG, "DOT Top Management Challenges FY 2022," (October 27, 2021), available at https://www.oig.dot.gov/sites/default/files/DOT%20FY%202022%20Top%20Management%20Challenges.pdf

[36] Id.

[37] Id.

[38] Id.

[39] Id.

[40] DOT OIG, "FTA Does Not Effectively Assess Security Controls or Remediate Cybersecurity Weaknesses To Ensure the Proper Safeguards Are in Place To Protect Its Financial Management Systems," (October 20, 2021), available at https://www.oig.dot.gov/sites/default/files/FTA%20Financial%20Management%20Systems%20Security%20Controls%20Final%20Report__10-20-21__REDACTED.pdf

trols provided by or inherited from DOT's common control provider."[41] The DOT OIG found that 139 of 269 security controls were not tested or implemented but reported as satisfied by FTA officials, for instance, increasing the exposure of FTA's financial management systems to outside threats.[42] The DOT OIG made 13 recommendations to correct these and other weaknesses and FTA has concurred with all of these recommendations.[43]

- *Federal Motor Carrier Safety Administration (FMCSA).* FMCSA regulates and oversees the safety of commercial vehicles. In October 2021, the DOT OIG issued a report showing their investigators had exploited vulnerabilities in web servers at FMCSA that allowed them to gain unauthorized access to the agency's network.[44] The agency also failed to detect the DOT OIG's placement of malware on their network.[45] DOT OIG investigators were able to gain access to 13.6 million unencrypted records with personally identifiable information.[46] The DOT OIG estimated that if malicious actors had obtained this information, it could have cost FMCSA up to $570 million in credit monitoring fees.[47] FMCSA did not detect the breach, in part because it did not use required automated detection tools and malicious code protections.[48] The DOT OIG also found that FMCSA does not always remediate vulnerabilities as quickly as DOT policy requires, putting FMCSA's network and data at risk for unauthorized access and compromise.[49] FMCSA concurred with DOT OIG's 13 recommendations and considers these issues "resolved but open pending FMCSA's completion of" its planned actions.[50]
- *Federal Aviation Administration (FAA).* In August 2021, the DOT OIG released a report on FAA's efforts to categorize its high-impact information systems.[51] The report found that until recently, the agency's air traffic organization had never properly categorized its high-impact security systems, although these systems provide safety-critical services.[52] In addition, it found, "FAA lacks formalized policies and procedures for selecting and implementing high security controls for its high-impact systems and continues to develop mitigations for security risks."[53] The DOT OIG further found that FAA has not completed a required gap analysis to comply with federal standards for its 45 high-impact systems "and is essential for determining whether the organization's security and privacy risks have been effectively managed."[54] Finally, the report said, "FAA has not yet mitigated the risk that the NAS [National Airspace System] could be vulnerable to threats as the Agency works to implement high security controls, because it has not fully implemented enterprise security initiatives designed to protect NAS assets."[55]
- *Aviation Cyber Initiative (ACI).* ACI is an interagency collaboration between FAA, the Department of Homeland Security (DHS), and the Department of Defense (DOD) that was informally established in 2016.[56] Its objectives include identifying and analyzing cyber threats and vulnerabilities, engaging with aviation stakeholders to help reduce cyber risks, and seeking opportunities to improve risk mitigation.[57] Its charter was finally approved in 2019, when 10 prior-

[41] Id.

[42] Id.

[43] Id.

[44] DOT OIG, "FMCSA's IT Infrastructure Is at Risk for Compromise," (October 20, 2021), available at https://www.oig.dot.gov/sites/default/files/FMCSA%20IT%20Infrastructure%20Final%20Report__10-20-21%20REDACTED.pdf

[45] Id.

[46] Id.

[47] Id.

[48] Id.

[49] Id.

[50] Id.

[51] DOT OIG, "FAA Is Taking Steps to Properly Categorize High-Impact Information Systems but Security Risks Remain Until High Security Controls Are Implemented," (August 2, 2021), available at https://www.oig.dot.gov/sites/default/files/REDACTED%20Final%20Report%20on%20FAA%20System%20Security%20Re-Categorizations.pdf

[52] Id.

[53] Id.

[54] Id.

[55] Id.

[56] DOT OIG, "FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities," (September 2, 2020), p. 1, available at https://www.oig.dot.gov/sites/default/files/FAA%20Aviation%20Cyber%20Initiative%20Final%20Report%5E09-02-20.pdf

[57] DOT Office of Inspector General, "FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities," (September 2, 2020), p. 1, available at https://www.oig.dot.gov/sites/default/files/FAA%20Aviation%20Cyber%20Initiative%20Final

ities were set for 2019 and 2020. The DOT OIG found, however, that ACI has only implemented three of those priorities.[58] In addition, according to GAO, the FAA has not developed mechanisms to monitor and evaluate cybersecurity issues that are raised in ACI coordination meetings and FAA's "oversight coordination activities are not supported by dedicated resources within" the FAA's budget.[59] GAO declared in a report it released in October 2020: "Until FAA establishes a tracking mechanism for cybersecurity issues, it may be unable to ensure that all issues are appropriately addressed and resolved. Further, until it conducts an avionics cybersecurity risk assessment, it will not be able to effectively prioritize and dedicate resources to ensure that avionics cybersecurity risks are addressed in its oversight program."[60] In addition, GAO found more broadly that "FAA has not (1) assessed its oversight program to determine the priority of avionics cybersecurity risks, (2) developed an avionics cybersecurity training program, (3) issued guidance for independent cybersecurity testing, or (4) included periodic testing as part of its monitoring process."[61]

United States Coast Guard (Coast Guard or Service)

The aging and underinvested status of the Coast Guard's cyber systems and IT infrastructure is at a crisis point as was highlighted during a Subcommittee on Coast Guard and Maritime Transportation hearing on November 16, 2021.[62] The Coast Guard has historically struggled with IT modernization, and Commandant Karl Schultz has made it a priority in what the Coast Guard calls its "Tech Revolution."[63] The Tech Revolution road map outlines strategic goals, including modernizing cybersecurity and cyber resilience.[64] Currently, the Coast Guard primarily operates on 1990s-era hardware and software, running the risk of critical failures even before its resilience can be challenged by cyber incidents.[65] In February 2020, for instance, the Commandant stated that the Coast Guard's IT infrastructure was at the "brink of catastrophic failure" and highlighted the immediate need for $300 million in IT spending to modernize the Coast Guard's technological landscape.[66]

In its 2015 *Cyber Strategy*, the Coast Guard explained that in the digital age, their overall mission to ensure the safety, security, and stewardship of the nation's waters cannot effectively be met without the Coast Guard maintaining a robust and comprehensive cyber program.[67] In 2021, working in close collaboration with DHS, DOD, government partners, foreign allies, and the maritime industry, the Coast Guard released its *Cyber Strategic Outlook*, an update to its cyber strategy to improve protection of the Marine Transportation System (MTS).[68] The strategic outlook focused on three efforts: (1) Securing resilient information technology and operational technology networks to support all Coast Guard missions; (2) Employing frameworks, standards, and best practices in prevention and response activities to

%20Report%5E09-02-20.pdf; *See also* FAA, "Aviation Cyber Initiative (ACI)" available at https://www.faa.gov/air__traffic/technology/cas/aci/media/documents/aci.pdf

[58] Id.

[59] GAO, "AVIATION CYBERSECURITY: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," GAO–21–86, (October 2020), available at https://www.gao.gov/products/gao-21-86

[60] Id.

[61] Id.

[62] House Committee on Transportation and Infrastructure, "Hearing: Rebuilding Coast Guard Infrastructure to Sustain and Enhance Mission Capability," (November 16, 2021), available at https://transportation.house.gov/committee-activity/hearings/rebuilding-coast-guard-infrastructure-to-sustain-and-enhance-mission-capability; James Ousman Cheek, "Changing Tides: Appraising and Supporting the Coast Guard's Role In Changing Seas," Consortium for Ocean Leadership, (November 2021), available at https://oceanleadership.org/changing-tides-appraising-and-supporting-the-coast-guards-role-in-changing-seas/

[63] Lauren Williams, "As the Coast Guard wrestles with aging IT, cloud is a long-term conversation," FCW (August 2018), available at https://fcw.com/articles/2018/08/03/uscg-it-progress-williams.aspx

[64] United States Coast Guard, "Tech Revolution: Vision for the Future," available at https://www.dcms.uscg.mil/Portals/10/CG-6/roadmap/C5i-roadmap-FINAL-v6.pdf

[65] Connie Lee, "BREAKING: Coast Guard Releases New 'Tech Revolution' Road Map," National Defense, (February 2020), available at https://www.nationaldefensemagazine.org/articles/2020/2/20/coast-guard-releases-new-tech-revolution-roadmap

[66] Jackson Barnett, "Coast Guard wants a 'tech revolution' to dig itself out of IT from the '90s," Fed Scoop (February 2020), available at https://www.fedscoop.com/coast-guard-tech-revolution-plan/.

[67] Coast Guard, "United States Coast Guard Cyber Security Strategy" (June 2015), p. 10, available at https://www.dco.uscg.mil/Portals/10/Cyber/Docs/CG__Cyber__Strategy.pdf?ver=nejX4g9gQdBG29cX1HwFdA%3d%3d

[68] Coast Guard, "United States Coast Guard Cyber Strategic Outlook," (August 2021), p. 4, available at https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf

identify and manage cyber risks to the MTS; and (3) Projecting advanced cyberspace capabilities in and through the operating environment enabling the Service to fight and win across all domains.[69]

The MTS includes waterways, shorelines, ports, shipyards, facilities, bridges, and other infrastructure throughout the United States, facilitating $5.4 trillion of economic activity every year, representing about a quarter of U.S. gross domestic product.[70] Over the past year, high-profile cyberattacks into U.S. networks have included crippling attacks on maritime infrastructure like the one that hit the Port of Kennewick, Washington, in November 2020.[71] The port refused to pay a $200,000 ransom to cybercriminals who hijacked their computer systems cutting off emails and other IT systems.[72] Email systems were restored by the end of the month, but it took longer to restore other compromised computer systems.[73]

As the sector risk management agency responsible for protecting the MTS under DHS's designated critical infrastructure sectors, the Coast Guard designated its Captains of Port to "lead governance by promoting cyber risk management, accountability, and the development and implementation of unified response plans." [74] The Coast Guard also intends to "refine cybersecurity incident reporting requirements and promote information sharing to improve the ability of owners and operators to prepare for, mitigate, and respond to threats to maritime critical infrastructure." [75]

Under the 2021 *Cyber Strategic Outlook*, the Coast Guard intends to conduct offensive cyber operations to deny or degrade adversaries' ability to plan, fund, communicate, or execute their own cyber operations.[76] To enable that capability, the Coast Guard seeks to establish an offensive Cyber Mission Team, interoperable with DOD cyber forces and DHS, and requested funding for continued cyber force development as part of its fiscal year (FY) 2022 budget request.[77] Supplementing a Coast Guard Maritime Cyber Readiness Branch that already consists of three defensive Cyber Protection Teams, administrative and policy legal challenges remain for the Coast Guard's future cyber operations capability.[78]

Federal Emergency Management Agency (FEMA)

In February 2021, DHS modified two existing FEMA Preparedness Grant programs to require recipients to spend at least 7.5 percent of their awards on improving their cybersecurity.[79] This requirement was added to State Homeland Security Program (SHSP) grants, which received $415 million in FY 2021 , and Urban Area Security Initiative (UASI) grants, which received $615 million in FY 2021.[80] State and local recipients of these grants can use the funding to conduct cybersecurity training and planning, cybersecurity risk assessments, and improve their critical infrastructure's cybersecurity.[81] In addition, in FY 2021, when FEMA's Port Security Grant Program (PSGP) offered $100 million in assistance to state and local governments, applicants were slated to receive a 20 percent increase in their scores for addressing Cybersecurity National Priority Areas.[82] PSGP is part of a broader FEMA effort to help protect transportation infrastructure against potential terrorist attacks.[83]

[69] Id. at p. 7.

[70] Id. at p. 3.

[71] Tri-City Areas Journal of Business, "Cyberattack Hobbles Port of Kennewick," (December 2020), available at https://www.tricitiesbusinessnews.com/2020/12/port-cyberattack/

[72] Id.

[73] Id.

[74] Coast Guard, "Cyber Strategic Outlook," p. 7.

[75] Id. at p. 28.

[76] Coast Guard, "Cyber Strategic Outlook," p. 32.

[77] Kimberly Underwood, "Coast Guard Embarks on Cyber Offense," AFCEA, (October 2021), available at https://www.afcea.org/content/coast-guard-embarks-cyber-offense

[78] Doubleday, "Coast Guard looks to plug digital holes," Federal News Network, August 4, 2021, available at https://federalnewsnetwork.com/cybersecurity/2021/08/coast-guard-looks-to-plug-digital-holes-in-maritime-infrastructure-under-new-cyber-outlook/

[79] FEMA Press Release, "DHS Announces Funding Opportunity for $1.87 Billion in Preparedness Grants," February 25, 2021, available at https://www.fema.gov/press-release/20210225/dhs-announces-funding-opportunity-187-billion-preparedness-grants

[80] Id.

[81] Id.

[82] FEMA—Port Security Grant Program Frequently Asked Questions, "Fiscal Year 2021 Port Security Grant Program," (February 25, 2021), available at https://www.fema.gov/sites/default/files/documents/FEMA_FY2021-PSGP-FAQ_02-18-21.pdf

[83] Id.

Environmental Protection Agency (EPA)

The EPA provides several cybersecurity services to state and local governments to help protect wastewater facilities.[84] These services include an online briefing to help state's assess cyber risks, a cybersecurity incident action checklist, training and response exercises, a Water Sector Cybersecurity Technical Assistance Provider Program to train state and regional water sector technical assistance providers, an online Vulnerability Self-Assessment Tool, and tools for the development of a tabletop exercise for cybersecurity incidents.[85]

Transportation Security Administration (TSA)

As a component agency of DHS since its creation in November 2001, the TSA states its mission is to "protect the nation's transportation systems to ensure freedom of movement for people and commerce."[86] In a constantly changing threat environment, TSA now prepares for cyber-related events like physical threats, as expressed in its 2018 TSA Cybersecurity Roadmap.[87] The roadmap provides the framework for how TSA can operate in the cyber environment, ensuring the protection of its data and information technology systems and ensuring the protection and resilience of the Transportation Systems Sector.[88] In line with that framework, TSA has moved to mandate certain protections and incident reporting requirements in response to recent cyberattacks.[89]

In addition to addressing longstanding cybersecurity vulnerabilities in the nation's private pipeline system, TSA must also address its own cyber weaknesses that increase the vulnerability of the nation's pipelines. In July 2021, GAO highlighted that additional pipeline-related weaknesses remain in TSA's internal policies.[90] These weaknesses include (1) incomplete information in TSA's pipeline risk assessments used to prioritize pipeline security reviews; and (2) aged protocols for responding to pipeline security incidents that TSA had not revised since 2010.[91] TSA officials concurred with GAO recommendations in this area and anticipate updating their policies and guidelines over the next year.[92] As TSA considers future directives mandating private sector action related to critical infrastructure, it is incumbent on TSA to maintain maximum credibility by fixing and updating its own cybersecurity policies and processes quickly and thoroughly.[93]

In October 2021, the Department of Justice (DOJ) announced that DOJ may seek substantial fines on government contractors or companies that receive federal funds when they fail to follow TSA cybersecurity standards by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.[94]

[84] EPA, "EPA Cybersecurity Best Practices for the Water Sector," available at https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector

[85] Id.

[86] TSA, "Mission," available at https://www.tsa.gov/about/tsa-mission

[87] TSA, "TSA Cybersecurity Roadmap 2018" (November 2018), p 2, available at https://www.tsa.gov/sites/default/files/documents/tsa__cybersecurity__roadmap__adm__approved.pdf#:~:text=TSA%E%2%80%99s%20mission%20responsibilities%20include%3A%20%281%29%20securing%20its%20own,in%20coordination%20with%20DHS%20to%20secure%20its%20cyberspace

[88] Id.

[89] DHS, "DHA Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," (May 2021), available at https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators; see e.g., Holland and Knight, "TSA's Pipeline of Cybersecurity Requirements," (August 2021), available at https://www.jdsupra.com/legalnews/tsa-s-pipeline-of-cybersecurity-5827015/#:~:text=At%20a%202019%20joint%20congressional,against%20an%20evolving%20threat%20environment

[90] GAO, "TSA is Taking Steps to Address Some Pipeline Security Program Weaknesses," (July 2021), available at https://www.gao.gov/assets/gao-21-105263.pdf

[91] Id.

[92] Id.

[93] See, e.g., Michael Hudson, "What if the Threat Comes from Within? Federal Agencies Must Address the Risk," The Hill (June 2021), available at https://thehill.com/opinion/cybersecurity/557460-what-if-the-threat-comes-from-within-federal-agencies-must-address

[94] Gevena Sands, "TSA to impose cybersecurity on railroads and aviation industries," CNN, (October 2021), available at https://www.cnn.com/2021/10/06/politics/tsa-cybersecurity-mandates-railroad-aviation/index.html

Cybersecurity and Infrastructure Security Agency (CISA)

The CISA is a component agency of DHS and leads national cybersecurity and infrastructure security efforts.[95] CISA helps protect the federal government's computer networks and partners with stakeholders in the public and private sectors to help improve cybersecurity and resiliency.[96] CISA also offers various services to stakeholders, including infrastructure assessments and analysis, information sharing between the public and private sector, training and exercises, and coordination of situational awareness and response to national cyber incidents.[97]

However, CISA's actions in some areas have been criticized.[98] For instance, CISA is responsible for the safety, security, and resiliency of the more than 91,000 dams nationwide, 63 percent of which are privately owned.[99] Dams are vulnerable to cybersecurity threats.[100] In 2016, the DOJ charged seven hackers linked to the Iranian government with carrying out a coordinated large scale cyberattack against dozens of banks and a small dam outside New York City.[101] In September 2021, the DHS OIG evaluated CISA's oversight of the Dams Sector and warned, "when they fail, the effects create a cascade of water inundation and flooding to buildings and agriculture, loss of power, disruptions to transportation, and damage to communication lines."[102] The report found that CISA does not manage or evaluate its Dams Sector activities, does not coordinate or track its own Dams Sector activities, does not gather or evaluate performance information on Dams Sector activities, does not consistently coordinate and effectively communicate with FEMA and other external Dams Sector partners and stakeholders, and has not updated overarching critical infrastructure plans.[103] The agency concurred with the five recommendations the report made to improve CISA's oversight of the Dams Sector.[104]

CHRONOLOGY OF RECENT FEDERAL GOVERNMENT ACTIONS ON CYBERSECURITY

Obama Administration

- *Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity*. This EO was issued by President Obama on February 12, 2013,[105] and designed to improve critical infrastructure's ability to manage cyber risks.[106] The EO sought to foster information sharing, promote the adoption of cybersecurity practices, and tasked the National Institute of Standards and Technology (NIST) with working with the private sector to identify voluntary standards and industry best practices in order to develop a voluntary Cybersecurity Framework whose adoption would help organizations enhance their cybersecurity preparedness and lower their risk of falling victim to cyberattacks.[107]

[95] Brian E. Humphreys, "Critical Infrastructure: Emerging Trends and Policy Considerations for Congress," Congressional Research Service, July 8, 2019, available at https://www.everycrsreport.com/files/20190708__R45809__54416d7b2f43d41696e8e971832aea5fe96a9919.pdf

[96] CISA web site, "About CISA," available at https://www.cisa.gov/about-cisa

[97] CISA Services Catalog, p. 11, available at https://www.cisa.gov/sites/default/files/publications/FINAL__CISA%20Services%20Catalog%20v1.1__20201029__508__0.pdf

[98] Department of Homeland Security Office of Inspector General, "CISA Can Improve Efforts to Ensure Dam Security and Resilience," (September 9, 2021), pp. 5–10, available at https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-59-Sep21.pdf

[99] Id.

[100] Ryan Schoolmeesters, "Lessons Learned From Dam Incidents and Failures," Association of State Dam Safety Officials, (Undated), available at https://damfailures.org/lessons-learned/site-security-is-critical/

[101] "Seven Iranians Working for Islamic Revolutionary Guard Corps—Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," U.S. Department of Justice, (March 24, 2016), available at https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

[102] Id.

[103] Department of Homeland Security Office of Inspector General, "CISA Can Improve Efforts to Ensure Dam Security and Resilience," (September 9, 2021), pp. 5–10, available athttps://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-59-Sep21.pdf

[104] Id.

[105] Federal Register, "Executive Order 12636 Improving Critical Infrastructure Cybersecurity," (February 12, 2013), available at https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[106] The White House (Obama Administration), "Cybersecurity—Executive Order 13626," available at https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636

[107] The White House (Obama Administration), "Executive Order—Improving Critical Infrastructure Cybersecurity," (February 12, 2013), available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

- *Presidential Policy Directive (PPD) 21—Critical Infrastructure Security and Resilience*. This PPD was published in conjunction with EO 13636 on February 12, 2013, replaced an earlier PPD on critical infrastructure, and established a national policy on critical infrastructure security.[108] The PPD directed agencies to develop a situational awareness capability, understand the consequences of infrastructure failures, mature public-private partnerships, and update the National Infrastructure Protection Plan.[109]

Trump Administration

- *EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This EO was issued by President Trump on May 11, 2017 and designed to enhance "the security of federal networks and critical infrastructure." [110] Notably, the EO indicated that the president would hold agencies "accountable for managing cybersecurity risk to their enterprises." [111] It also empowered the DHS Secretary to serve "as the nation's key coordinator for all aspects of critical infrastructure security, including cybersecurity." [112]
- *EO 13833, Enhancing the Effectiveness of Agency Chief Information Officers*. This EO was issued on May 15, 2018, by President Trump and empowered agency chief information officers (CIOs) by increasing their scope of authority, especially regarding agencies' IT management.[113]
- *National Maritime Cybersecurity Plan to the National Strategy for Maritime Security*. Published in December 2020, this plan was meant to integrate cybersecurity into the National Strategy for Maritime Security (NSMS).[114] The plan committed to setting standards to mitigate risks in the maritime sector, promote information sharing, and build a cyber workforce.[115] The 2020 plan followed President Trump designating the Maritime Transportation System (MTS) [116] a "top priority" in the 2017 National Security Strategy.[117]
- *Cyberspace Solarium Commission*. This commission is a bipartisan and intergovernmental body created by the John S. McCain National Defense Authorization Act for Fiscal Year 2019 with the purpose to develop a strategic approach to defense against significant cyberattacks.[118] The Commission published its re-

[108] CISA, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," available at https://www.cisa.gov/homeland-security-presidential-directive-7; The White House (Obama Administration), "Presidential Policy Directive—Critical Infrastructure and Resilience," (February 12, 2013), available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[109] CISA, "EO 13636 and PPD 21 Fact Sheet," (March 2013), available at https://www.cisa.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf

[110] The White House (Trump Administration), "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[111] Id.

[112] National Security Archive, "President Trump's Executive Orders on Critical Infrastructure," available at https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-10-22/president-trumps-executive-orders-critical-infrastructure

[113] The White House (Trump Administration), "President Donald J. Trump is Enhancing the Effectiveness of Agency Chief Information Officers," May 15, 2018, available at https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-enhancing-effectiveness-agency-chief-information-officers/

[114] The White House (Trump Administration), "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security," (December 2020), available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf; Homeland Security Digital Library, "National Maritime Cybersecurity Plan Released," (January 12, 2021), available at https://www.hsdl.org/c/national-maritime-cybersecurity-plan-released/

[115] The White House (Trump Administration), "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security," (December 2020); Homeland Security Digital Library, "National Maritime Cybersecurity Plan Released," (January 12, 2021), available at https://www.hsdl.org/c/national-maritime-cybersecurity-plan-released/

[116] The Maritime Transportation System (MTS) includes the nation's waterways, ports, and land-side connectors, additional information available at https://www.maritime.dot.gov/outreach/maritime-transportation-system-mts/maritime-transportation-system-mts

[117] The White House (Trump Administration), "Statement from National Security Advisor Robert C. O'Brien Regarding the National Maritime Cybersecurity Plan," (January 5, 2021), available at https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-regarding-national-maritime-cybersecurity-plan/

[118] "Cyberspace Solarium Commission," available at https://www.solarium.gov/

port in March 2020 and was reauthorized in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.[119]

Biden Administration

- *Industrial Control Systems Cybersecurity Initiative*. This initiative, launched in April 2021, aims to improve the security of operational technology (OT) and industrial control systems (ICS) through the development and deployment of OT/ ICS cyber monitoring technologies.[120] The initiative also started a pilot program to improve cybersecurity of the electricity infrastructure, a "100-Day plan," with aggressive milestones, which is led by the Department of Energy, in coordination with CISA.[121]
- *Cybersecurity Sprints*. CISA began a series of cybersecurity-focused "60-day sprints" in April 2021, the first focused on ransomware, with the following sprints focused on the cybersecurity workforce, ICS resilience, transportation security, election security, and international partnerships.[122] The sprints aim to remove roadblocks, elevate existing cybersecurity efforts, and launch new efforts, with the first sprint on ransomware to include an awareness campaign and engagement with industry.[123] The 60-day sprints and the 100-day plan are part of the Biden Administration's increased focus on cybersecurity issues.[124]
- *EO 14028, Improving the Nation's Cybersecurity*. This EO was issued by President Biden on May 12, 2021,[125] and is intended to improve cybersecurity by modernizing the defense of federal networks by moving to secure cloud services and a zero-trust architecture, improving information sharing by removing contractual barriers, and strengthening response capabilities.[126] It also calls for the creation of a Cybersecurity Safety Review Board, modeled after the National Transportation Safety Board, that would examine significant cybersecurity incidents in order to help apply lessons learned from these incidents and improve the nation's cybersecurity defenses.[127]
- *TSA emergency security directives for the pipeline industry*. TSA issued two emergency security directives due to the May 2021 Colonial Pipeline ransomware attack.[128] The first, issued in May 2021, required pipeline companies to report cyber incidents to TSA and CISA, both part of DHS, and to name a cybersecurity point person; the second directive, issued in July 2021, required companies to develop an incident response plan for potential cyberattacks and implement specific mitigation measures to protect against ransomware attacks.[129]

[119] Id.

[120] Department of Energy, "Progress Report: 100 Days of the Biden Administration's Industrial Control Systems (ICS) Cybersecurity Initiative and Electricity Subsector Action Plan," (August 16, 2021), available at https://www.energy.gov/articles/progress-report-100-days-biden-administrations-industrial-control-systems-ics

[121] Id.

[122] Justin Katz, "Mayorkas announces cyber 'sprints' on ransomware, ICS, workforce," (March 31, 2021), available at https://fcw.com/articles/2021/03/31/mayorkas-cyber-sprints-speech.aspx; Jory Heckman, "DHS launching 60-day sprints ahead of upcoming executive order," (March 31, 2021), available at https://federalnewsnetwork.com/cybersecurity/2021/03/dhs-launching-60-day-cyber-sprints-ahead-of-upcoming-executive-order/

[123] DHS, "Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience," (March 31, 2021), available at https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience

[124] Id.

[125] Federal Register, "Executive Order 14028 Improving the Nation's Cybersecurity," (May 12, 2021), available at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[126] The White House, "Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," (May 12, 2021), available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

[127] Id.

[128] Ellen Nakashima, "TSA to impose cybersecurity mandates on major rail and subway systems," The Washington Post, (October 6, 2021), available at https://www.washingtonpost.com/national-security/rail-cybersecurity-dhs-regulations/2021/10/06/b3db07da-2620-11ec-8831-a31e7b3de188_story.html

[129] Ellen Nakashima and Lori Aratani, "DHS to issue first cybersecurity regulations for pipelines after Colonial hack," The Washington Post, (May 25, 2021), available at https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/; *See also*: DHS Press Release, "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," July 20, 2021, available at https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

- *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*. This memorandum was issued by President Biden on July 28, 2021,[130] and directed CISA and NIST to develop cybersecurity performance goals[131] and formally established the "Industrial Control Systems Cybersecurity Initiative."[132] The Initiative is a voluntary and collaborative effort between federal partners and critical infrastructure owners and operators to improve collaboration and increase the use of new cybersecurity technologies.[133] The Initiative was first launched earlier in April 2021 (see above) with the pilot program focused on the electricity subsector, with initiatives focused on the water and wastewater sector and the chemical sector to follow.[134]
- In October 2021, TSA announced plans for an additional *directive to address cybersecurity in the rail and aviation sectors*.[135] Reportedly, TSA will require higher-risk railroad and rail transit entities to report cyber incidents to the federal government, identify cybersecurity point persons, and put together contingency and recovery plans in case they become victims of cyberattacks.[136] For the airline industry, TSA will reportedly require critical U.S. airport operators, passenger aircraft operators, and all-cargo aircraft operators to designate cybersecurity coordinators and report cyber incidents to CISA.[137]
- The recently enacted bipartisan Infrastructure Investment and Jobs Act, (P.L. 117–58) provides approximately $2 billion "to modernize and secure federal, state, and local IT and networks; protect critical infrastructure and utilities and support public or private entities as they respond to and recover from significant cyberattacks and breaches."[138]

WITNESS LIST

- Mr. Cordell Schachter, Chief Information Officer (CIO), Department of Transportation (DOT)
- Mr. Larry Grossman, Chief Information Security Officer (CISO), Federal Aviation Administration (FAA)
- Ms. Victoria Newhouse, Deputy Assistant Administrator for Policy, Plans, and Engagement, Transportation Security Administration (TSA)
- Rear Admiral John W. Mauger, Assistant Commandant for Prevention Policy (CG–5P), U.S. Coast Guard (USCG)
- Mr. Kevin Dorsey, Assistant Inspector General for Information Technology Audits, Office of Inspector General (OIG), Department of Transportation (DOT)
- Mr. Nick Marinos, Director, Information Technology and Cybersecurity, Government Accountability Office (GAO)

[130] The White House, "Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure," (July 28, 2021), available at https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/28/background-press-call-on-improving-cybersecurity-of-u-s-critical-infrastructure/

[131] NIST, "White House National Security Memo Issued: NIST & DHS Developing Cybersecurity Performance Goals for Critical Infrastructure Control Systems," (July 29, 2021), available at https://www.nist.gov/news-events/news/2021/07/white-house-national-security-memo-issued-nist-dhs-developing-cybersecurity

[132] The White House, "Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure."

[133] The White House, "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems," (July 28, 2021), available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[134] Id.

[135] Ellen Nakashima, "TSA to impose cybersecurity mandates on major rail and subway systems," The Washington Post.

[136] Id.

[137] Maggie Miller, "TSA to issue regulations to secure rail, aviation groups against cyber threats," The Hill, (October 6, 2021), available at https://thehill.com/policy/cybersecurity/575580-tsa-to-issue-regulations-to-secure-rail-aviation-groups-against-cyber

[138] Public Law No. 117–58; Infrastructure Investment and Jobs Act, Congress.gov; White House Fact Sheet, "Top 10 Programs in the Bipartisan Infrastructure Investment and Jobs Act That You May Not Have Heard About," (August 3, 2021), available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/03/fact-sheet-top-10-programs-in-the-bipartisan-infrastructure-investment-and-jobs-act-that-you-may-not-have-heard-about/

Mr. DEFAZIO. The committee will come to order.

I ask unanimous consent that the chair be authorized to declare a recess at any time during today's hearing.

Without objection, so ordered.

As a reminder, please keep your microphone muted, unless speaking. Should I hear any inadvertent background noise, I will request the Member please mute their microphone.

To insert a document into the record, please email it to DocumentsT&I@mail.house.gov.

I am going to abbreviate my opening statement. I will put the full statement in the record, given the fact that you probably can't hardly understand me, and I am having trouble.

This is the second hearing. The last hearing was industry stakeholders, and we heard distressing and serious gaps, shortages of cyber personnel, a lack of even the most basic cyber hygiene practices, and a consensus among our witnesses that the Federal Government needed to help the private sector, which owns and operates 85 percent of the Nation's critical infrastructure, to defend itself from and respond to attacks.

The bill, H.R. 3684, will provide funding at the local, State, and Federal level to enhance the Nation's cyber resilience and response to cybersecurity incidents. It improves the National Highway System and other public transportation systems' cybersecurity preparedness capabilities, and it empowers the newly established Office of the National Cyber Director, the President's principal adviser on cybersecurity policy and strategy, to identify cybersecurity incidents and coordinate a Federal response. Those are noteworthy steps, but there is more to do.

Today we will hear from the Federal agencies responsible for transportation and other critical infrastructure, and their efforts to help private industry.

We have, for the most part, relied upon a voluntary approach to protecting assets, choosing not to mandate standards for cybersecurity audits or exercises. In contrast, in other areas where private sector assets have the potential to cause significant harm, the Government has established very robust requirements—that would be nuclear power, aviation, drinking water, wastewater, and others—to make them safer and more resilient.

But many of these industries relate to other critical industries, the private sector, and voluntary cooperation sometimes isn't enough. You have to spend a bunch of money on cybersecurity.

The leeches on Wall Street are going to say, "Hey, why are you spending all that money on cybersecurity? It is driving down your stock price. We want to see you just, you know, put the money in the bank." So there needs to be a little nudging here.

And then, of course, the cost of the incident far exceeds the investment they should have and would have made to prevent that incident, absent an absolutely catastrophic incident, but more basic incidents or ransomware, and all these other things that are rather routine.

So, I don't think that implementing basic cybersecurity standards, reporting requirements, and cybersecurity awareness training should be voluntary. It should be required. And public safety and the Nation's security depend upon these steps.

In the wake of the Colonial Pipeline cyberattack, the Transportation Security Administration mandated specific cybersecurity protections for pipelines to defend against ransomware and other attacks. Colonial had turned down a comprehensive audit before the event, which might have helped prevent the event. But it was voluntary, so they said no, thanks, we don't want to know about our vulnerabilities.

Last week, TSA issued basic cybersecurity enhancements for the aviation sector that will go into effect early next year, and I understand TSA intends to issue a security directive for passenger rail, high-risk freight rail, and the transit sector as early as today or this week. So, this is an appropriate time for this hearing.

Both the GAO and the Department of Transportation's Office of Inspector General, who we will hear from today, have made thousands of recommendations related to cybersecurity weaknesses at Federal agencies. Many of these recommendations remain unaddressed. Some of their more alarming findings find DOT's failure to implement a cybersecurity risk management strategy and weaknesses in FAA's approach to cybersecurity for avionics systems in commercial aircraft.

Similarly, the DOT IG has uncovered a range of cybersecurity deficiencies and deemed information security one of the Department's top management challenges. The OIG has found evidence of inconsistent software updates, lax enforcement of Federal cybersecurity requirements, and IT systems at DOT that are vulnerable to exploitation by hostile actors.

I look forward to hearing from our expert witnesses today on the best mitigation and potential solutions, so that we can look forward.

With that I recognize the ranking member, who hopefully has better control of his voice.

[Mr. DeFazio's prepared statement follows:]

Prepared Statement of Hon. Peter A. DeFazio, a Representative in Congress from the State of Oregon, and Chair, Committee on Transportation and Infrastructure

Last month, we heard from industry stakeholders and cybersecurity experts on the challenges they face in protecting our nation's transportation systems and critical infrastructure from cyberattacks. The testimony was troubling. Witnesses discussed serious gaps such as shortages of cybersecurity personnel and a lack of basic cyber hygiene practices. Notably, there was a consensus among our witnesses that more—not less—federal action is needed to help the private sector, which owns and operates an estimated 85 percent of the nation's critical infrastructure, defend itself from, respond to, and recover from cyberattacks.

Since our November hearing, Congress passed with bipartisan support and the president signed H.R. 3684, the Infrastructure Investment and Jobs Act. Along with other vital investments in our nation's infrastructure, this bill takes significant steps toward improving the cybersecurity of our nation's critical infrastructure. It provides funding at the local, state, and federal level to enhance the nation's cyber resilience and response to cybersecurity incidents, it improves the national highway system and other public transportation systems' cybersecurity preparedness capabilities, and it empowers the newly established Office of the National Cyber Director, the president's principal advisor on cybersecurity policy and strategy, to identify cybersecurity incidents and coordinate a federal response. These steps are noteworthy, but there is much more to do.

Today, we will hear from the federal agencies who are responsible for transportation systems and other critical infrastructure sectors about their efforts to help private industry address these cybersecurity gaps, as well as the challenges these agencies face themselves in protecting the government's own networks from cyberattacks.

In the cybersecurity realm, the federal government has largely permitted the private sector to take a "voluntary" approach to protecting their assets, choosing not to mandate cybersecurity standards, cyber audits, or cybersecurity exercises. In contrast, in other areas where private sector assets have the potential to cause significant harm, the government has established requirements to protect the public.

For example, nuclear power plants are subject to strict federal mandates on their operation. Commercial airlines must comply with federal reporting requirements regarding runway incursions and other safety-related mishaps. Drinking water utilities must report to the federal government if they detect spikes in lead or other dangerous chemicals that can harm the public. These requirements have not undermined these industries. In fact, they have made them stronger, safer, and more resilient.

Yet, when it comes to intrusions into the networks of a critical infrastructure entity, an intrusion that could damage critical components of an airplane, a train, an oil or gas pipeline, or a port facility, if that network belongs to a private company, up until now, the federal government has merely asked for "voluntary" cooperation. As we learned at our last hearing, an astounding 30 percent of public transit agencies failed to report known breaches to anyone. I expect the statistics in the private sector are far worse. In addition, the short-term financial implications of making a cyber breach public, possibly affecting a company's economic bottom line or shrinking a CEO's bonus, inhibits cybersecurity transparency, masking known vulnerabilities that should be quickly corrected.

Implementing basic cybersecurity standards, reporting requirements, and cybersecurity awareness training should not be voluntary—they should be required. The public's safety and the nation's security depend on these systems. While no single change can prevent every cyberattack, we need to raise the bar significantly and make cyberattacks on our systems much more difficult to accomplish.

The Biden administration has taken notable steps to address these issues holistically. They have issued orders and memoranda to encourage infrastructure owners and operators to increase their cybersecurity investments to minimize threats to all critical infrastructure sectors. In the wake of the Colonial Pipeline cyberattack, the Transportation Security Administration mandated specific cybersecurity protections for pipelines to defend against ransomware and other attacks, along with contingency and recovery plans. Last week, TSA issued basic cybersecurity enhancements for the aviation sector that will go into effect early next year and I understand TSA intends to issue a security directive for passenger rail, high-risk freight rail, and the transit sector as early as today. So, we appear to have scheduled this hearing quite well. In addition, last month, the Cybersecurity and Infrastructure Security Agency issued a binding directive that ordered federal agencies to fix known software and hardware vulnerabilities in their computer networks within six months. For those that care about the public's safety and the nation's economic and national security, these efforts—in both the public and private sectors—should not be controversial. They should be welcomed and supported.

Both the Government Accountability Office (GAO) and the Department of Transportation's Office of Inspector General (DOT OIG)—whom we will hear from today—have made thousands—literally thousands—of recommendations related to cybersecurity weaknesses at federal agencies. Many of these recommendations remain unaddressed.

Some of GAO's more alarming findings include DOT's failure to implement a cybersecurity risk management strategy and weaknesses in FAA's approach to cybersecurity for avionics systems in commercial aircraft.

Similarly, the DOT OIG has uncovered a range of cybersecurity deficiencies and deemed information security one of the department's top management challenges. The OIG has found, among other things, evidence of inconsistent software updates, lax enforcement of federal cybersecurity requirements, and IT systems at DOT that are vulnerable to exploitation by hostile actors.

I look forward to hearing from our government witnesses today. I expect them to explain the steps they are taking to address the cybersecurity issues that have plagued them for far too long and update us on the status of their efforts to work with private industry to address the cybersecurity threats that endanger us all. As our transportation systems and critical infrastructure assets—both public and private—evolve, we become more efficient and connected than ever, but we also create new opportunities for cyber villains. To improve our resiliency to these threats, we must work together and address them in a holistic manner.

With that, I recognize Ranking Member Graves for his opening statement.

Mr. GRAVES OF MISSOURI. Thank you, Mr. Chairman.

Before I give my statement, I do want to acknowledge your announcement that you are not going to be seeking reelection next term, and I want to commend you for your long and distinguished career, serving over three decades in the House of Representatives. I think that says a lot.

I have no doubt that you are going to finish out your term, and you are going to work just as hard as ever on behalf of your district and your constituents.

And I also believe that you and I agree that the Committee on Transportation and Infrastructure is one of the best and most important committees in Congress. And I know you will continue to work diligently to address the vital issues before this committee in the coming months.

I do wish you and your family all the best in your retirement.

Turning to today's hearing, we will continue an examination on cybersecurity challenges for the transportation and infrastructure sectors.

During our first hearing on this topic in November, we heard from the perspective of owners and operators of these critical assets about the steps that they have taken to improve their cybersecurity posture, the threats and risks that they still face, and the effectiveness of the Federal Government's cyber activities.

Now we will hear testimony from some of those Federal agencies themselves and learn how they are providing support to transportation and infrastructure operators in boosting their cybersecurity preparedness and response capabilities.

Stakeholders have expressed concerns about aspects of those Federal programs—for instance, the recent security directives from the TSA—and I hope we can get some answers on how to improve their implementation.

We also will hear today about how Federal agencies are protecting their own systems, their own data, and infrastructure from ever-changing cyber threats. I look forward to hearing from our witness panel about the cyber challenges that they have identified and examined for the Federal agencies under the committee's jurisdiction, as well as receive updates from those agencies on how they are rising to meet these challenges.

And I appreciate our witnesses joining us today and discussing how operators and Federal agencies can work collaboratively to improve the cybersecurity of our Nation's most critical transportation systems and infrastructure.

So, with that, I would yield back, and I look forward to it.

[Mr. Graves of Missouri's prepared statement follows:]

Prepared Statement of Hon. Sam Graves, a Representative in Congress from the State of Missouri, and Ranking Member, Committee on Transportation and Infrastructure

Thank you, Chair DeFazio.

For today's hearing, we will continue our examination of cybersecurity challenges for the transportation and infrastructure sectors. During our first hearing on this topic in November, we heard from the perspective of owners and operators of these critical assets about the steps they have taken to improve their cybersecurity posture, the threats and risks they still face, and the effectiveness of federal government cyber activities.

Now we will hear testimony from some of those federal agencies themselves and learn how they are providing support to transportation and infrastructure operators in boosting their cybersecurity preparedness and response capabilities.

Stakeholders have expressed concerns about aspects of these federal programs—for instance, the recent security directives from the TSA—and I hope we can get some answers on how to improve their implementation.

We will also hear today about how federal agencies are protecting their own systems, data, and infrastructure from ever-changing cyber threats. I look forward to hearing from our witness panel about the cyber challenges they've identified and examined for the federal agencies under the Committee's jurisdiction, as well as receive updates from those agencies on how they are rising to meet these challenges.

I appreciate our witnesses joining us today and discussing how operators and federal agencies can work collaboratively to improve the cybersecurity of our nation's most critical transportation systems and infrastructure.

Mr. DEFAZIO. [Addressing technical difficulties off the record.]

Oh, thanks for the kind words, Sam. I know that the committee will continue its great work, between your leadership and others on the committee.

With that I would like to move to recognizing the witnesses here today.

The first is Mr. Cordell Schachter, Chief Information Officer, DOT; Mr. Larry Grossman, Chief Information Security Officer, Federal Aviation Administration; Ms. Victoria Newhouse, Deputy Assistant Administrator for Policy, Plans, and Engagement, Transportation Security Administration; Rear Admiral John W. Mauger, Assistant Commandant for Prevention Policy, United States Coast Guard; Mr. Kevin Dorsey, Assistant Inspector General for Information Technology Audits, Office of Inspector General, Department of Transportation; and Mr. Nick Marinos, Director, Information Technology and Cybersecurity at the GAO.

With that, I would first recognize Mr. Schachter for 5 minutes. Mr. Schachter?

TESTIMONY OF CORDELL SCHACHTER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF TRANSPORTATION; LARRY GROSSMAN, CHIEF INFORMATION SECURITY OFFICER, FEDERAL AVIATION ADMINISTRATION; VICTORIA NEWHOUSE, DEPUTY ASSISTANT ADMINISTRATOR FOR POLICY, PLANS, AND ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY; REAR ADMIRAL JOHN W. MAUGER, ASSISTANT COMMANDANT FOR PREVENTION POLICY, U.S. COAST GUARD; KEVIN DORSEY, ASSISTANT INSPECTOR GENERAL FOR INFORMATION TECHNOLOGY AUDITS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF TRANSPORTATION; AND NICK MARINOS, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. SCHACHTER. Good morning, Chair DeFazio, Ranking Member Graves, and members of the committee. Thank you for the opportunity to testify before you today, and for your support of the Department of Transportation.

I am Cordell Schachter, Chief Information Officer. I am honored to be here with FAA Chief Information Security Officer Larry

Grossman, U.S. DOT Office of Inspector General Assistant Inspector General for IT Audits Kevin Dorsey, and officials from the U.S. Coast Guard, the Transportation Security Administration, and the Government Accountability Office.

I was appointed U.S. DOT's chief information officer on August 30th of this year. My testimony today is based on my observations and review of DOT records during my 3 months in this position. My testimony is also informed by my 26 years of service as a local government official in New York City, 13 years of that service as chief technology officer and CIO of New York City's department of transportation.

In between two tours of New York City government service, I worked 9 years for several multinational technology companies. I have also taught master's level courses in civic technology at New York University in New York City, and at St. Peter's University in Jersey City, New Jersey.

I believe U.S. DOT's cybersecurity program has improved the Department's information security posture, and we are on a path for continual improvement, according to Government best practices. U.S. DOT's executive ranks have many positions filled by professionals with the knowledge and the expertise of providing service directly to the public. This begins with Secretary Pete Buttigieg, Deputy Secretary Polly Trottenberg, and the leaders of many of our operating administrations or modes.

They have also held key elected and appointed leadership positions in cities and States solving problems, protecting citizens, and improving the quality of life of their constituents.

We now have before us one of the greatest opportunities to improve the quality of life for all Americans. We look forward to partnering with Congress and our sister Federal agencies to implement the landmark bipartisan infrastructure law.

On the same day that President Biden signed the law, he executed an Executive order to ensure, among other priorities, increased coordination across the public sector to implement it effectively. We commit to that goal. Our executive leadership teams' experience includes making improvements to systems while they continue to operate. Similarly, we will continue to improve our existing systems to make them more cyber secure while they continue to operate, so that they resiliently support DOT's operations and the American people.

I want to transparently acknowledge that we have multiple open audit findings from previous OIG and GAO cybersecurity audits. We respect and take seriously their assessments. I have designated cybersecurity improvement as the top priority for DOT's information technology organization, the Office of the Chief Information Officer. We have begun a series of cyber sprints to complete tasks and make plans to meet our Federal cybersecurity requirements, and implement best practices, including those from President Biden's Executive order for improving the Nation's cybersecurity.

The cyber sprints prioritize three areas: system access control; website security; and improved governance, oversight, and coordination across DOT. These priority activities address OIG and GAO findings.

DOT is actively working to meet its responsibilities to securely improve the Department's information technology infrastructure, while implementing our portions of the bipartisan infrastructure law.

We will also meet the challenge of continuously improving the cybersecurity of DOT information technology systems, while keeping those systems available for use.

We look forward to working with this committee, our agency partners, and the White House to strengthen and protect our infrastructure and systems.

Thank you again for this opportunity to testify. I will be happy to answer your questions.

[Mr. Schachter's prepared statement follows:]

Prepared Statement of Cordell Schachter, Chief Information Officer, U.S. Department of Transportation

Chair DeFazio, Ranking Member Graves, and Members of the Committee, thank you for the opportunity to testify before you today, and for your support of the Department of Transportation (DOT). I am honored to be here with Federal Aviation Administration (FAA) Chief Information Security Officer Larry Grossman, US DOT Office of Inspector General (OIG) Assistant Inspector General for IT Audits, Kevin Dorsey, and officials from the US Coast Guard, the Transportation Security Administration, and the U.S. Government Accountability Office (GAO).

I was appointed US DOT's Chief Information Officer, or CIO on August 30th of this year. My testimony today is based on my observations and review of DOT records during my 3 months in this position. My testimony is also informed by my 26 years of service as a local government official in New York City (NYC), 13 years of that service as Chief Technology Officer and CIO of New York City's Department of Transportation. In between 2 tours of NYC government service, I worked 9 years for several multi-national technology companies. I have also taught masters level courses in civic technology at New York University in NYC and at Saint Peter's University in Jersey City, New Jersey. I believe US DOT's cyber security program has improved the department's information security posture and we're on a path for continual improvement according to government best practices.

US DOT's executive ranks have many positions filled by professionals with the knowledge and the experience of providing service directly to the public. This begins with Secretary Pete Buttigieg, Deputy Secretary Polly Trottenberg, and the leaders of many of our Operating Administrations or modes. They have also held key elected and appointed leadership positions in cities and states solving problems, protecting citizens, and improving the quality of life of their constituents. We now have before us one of the greatest opportunities to improve the quality of life for all Americans. We look forward to partnering with Congress and our sister federal agencies to implement the landmark Bipartisan Infrastructure Law. In fact, on the same day that President Biden signed the Law, he executed an Executive Order to ensure—among other priorities—increased coordination across the public sector to implement it effectively.

Our executive leadership team's experience includes making improvements to systems while they continue to operate. Similarly, we'll continue to improve our existing systems to make them more secure, while they continue to operate, so that they resiliently support DOT's operations and the American people.

I want to transparently acknowledge that we have multiple open findings from previous OIG and GAO cybersecurity audits. I have designated cyber security improvement as the top priority for DOT's Information Technology organization, the Office of the Chief Information Officer.

We have begun a series of "cyber sprints" that will establish Plans of Action and Milestones to meet our federal cyber security requirements and implement best practices, including those from President Biden's Executive Order 14028 Improving the Nation's Cybersecurity; the Federal Information Technology Acquisition Reform Act (FITARA); the Federal Information Security Management Act (FISMA); Office of Management and Budget (OMB) memoranda; the National Institute for Standards and Technology (NIST) Cybersecurity Framework; and inspector general and GAO findings.

DOT is actively working to meet its responsibilities to securely improve the Department's information technology infrastructure while implementing our portions of the Bipartisan Infrastructure Law. We will also meet the challenge of continuously improving the cybersecurity of DOT information technology systems while keeping those systems available for use. We look forward to working with this Committee, our agency partners, and the White House to strengthen and protect our infrastructure and systems. Thank you again for the opportunity to testify. I will be happy to answer your questions.

Mr. DEFAZIO. Thank you, Mr. Schachter, for doing it exactly in 5 minutes. I appreciate that. We will now move on to Mr. Larry Grossman.

Mr. Grossman?

Mr. GROSSMAN. Good morning. From air traffic control, to the largest airliner, or the lightest drone, connectivity is the way of the future in aerospace. It is also why we have to constantly raise the bar when it comes to cybersecurity.

Chair DeFazio, Ranking Member Graves, members of the committee, cyber threats are an ongoing concern, and our increasing reliance on highly integrated and interdependent computers and networks is cause for vigilance at all levels of the aviation industry. This is especially true at FAA, where we are responsible for operating the Nation's air traffic control system, and overseeing design, manufacture, and testing of aircraft and systems, including avionics, and also for me personally, as a pilot, a flight instructor, and an aircraft owner.

But I am here today to discuss the FAA's approach to cybersecurity within our agency for those we regulate, and for the aerospace community at large.

I want to start by noting the importance of this administration's recent Executive order on improving the Nation's cybersecurity, and I want to thank Congress for the continuing guidance and direction over many years.

The FAA's efforts to address cyber challenges have benefited from your oversight and the cooperative efforts with other executive branch agencies.

We appreciate all input as we continually strive to make our airspace system safer and more efficient. You have heard Administrator Dickson say it before, and I will repeat it here again: Safety is a journey, not a destination.

The same is true of cybersecurity. What we do today will not be good enough for tomorrow or the day after. We are always striving to improve. We are constantly updating and evolving FAA cybersecurity strategy we put into action through the cross-agency Cybersecurity Steering Committee. The strategy includes protecting and defending FAA networks and systems, enhancing our risk management capabilities, building and maintaining workforce capabilities, and engaging with external partners.

We defend our air traffic control and other networks by using separate and distinct security perimeters and controls that are the responsibility of the FAA chief information security officer and FAA chief information officer.

To assess cyber threats and vulnerabilities to our networks, we have developed the cyber test facility at our William J. Hughes Technical Center, where we also conduct testing and evaluation. We ensure cyber resilience in connected aircraft through risk assessments during initial certification process, or any time there is a change to a previous design certification. When existing regulations will not provide adequate protection, we issue special conditions.

Throughout an aircraft's life, operators must track cybersecurity issues in much the same way that they do for all other issues, using data-driven methodologies. That allows operators in the FAA to make informed risk management decisions. Smart decisions require a talented and dedicated cyber workforce, and we continue to invest in our people.

Congress recognized the importance of this effort, and in 2018 asked the FAA to enter into an agreement with the National Academy of Sciences to conduct the cybersecurity workforce study. The results of that study, which we received in June, made it clear that there is more work to do, although I will say that many of the recommendations are consistent with FAA cybersecurity strategic objectives, and many others align with broader, ongoing FAA workforce development and recruitment efforts.

And finally, one of the major components of our strategy is to build and maintain relationships and trust with our external partners. This is critical for defending and reacting and recovering from a cyberattack. It is why we are a lead agency on the Aviation Cyber Initiative interagency task force with DHS and DoD. It is why we work collectively to identify and address cybersecurity risks in the aviation ecosystem. The ecosystem includes stakeholders ranging from airport authorities to manufacturers.

As technology of the aviation ecosystem evolves, we expect that cybersecurity will continue to be a growing challenge and a significant component of aviation safety and aerospace efficiency. We are prepared for this challenge and look forward to keeping Congress and this committee informed on our progress.

I will be happy to answer any questions that you may have.

[Mr. Grossman's prepared statement follows:]

Prepared Statement of Larry Grossman, Chief Information Security Officer, Federal Aviation Administration

Good morning Chair DeFazio, Ranking Member Graves, and Members of the Committee:

Thank you for the opportunity to be here with you today to discuss the Federal Aviation Administration's (FAA) approach to cybersecurity, both in terms of how the FAA addresses cybersecurity matters internally and how the FAA interacts with the aviation community on cybersecurity matters.

The core and continuing mission of the FAA is to provide the safest and most efficient aerospace system in the world. Technology has contributed greatly to the safety and efficiency of the national airspace system (NAS). It has also resulted in highly integrated and increasingly interdependent computers and networks supporting the aviation community. Cyber-based threats have made the integration of cybersecurity protections into all aspects of the FAA's mission increasingly important. This Administration has recognized the growing importance of cybersecurity. President Biden's Executive Order 14028, "Improving the Nation's Cybersecurity", is a sweeping directive that addresses cyber threat information sharing, cybersecurity modernization, software supply chain security, identifying and remediating cyber vulnerabilities, and incident response.[1] This executive order will drive many ele-

[1] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

ments of FAA's strategic cyber initiatives across both the agency's IT infrastructure as well as the infrastructure of the NAS.

FAA's Cybersecurity Structure and Strategy

To achieve its mission, the FAA is dependent on information systems, and operates these systems in three separate domains: the NAS Domain, operated by FAA's Air Traffic Organization (ATO), the Mission Support Domain, operated by FAA's Office of Finance and Management (AFN), and the Research and Development Domain, operated by FAA's Office of NextGen (ANG). Each of the three domains represents a separate security perimeter with a distinct set of security controls. While each FAA Domain operator is responsible for the cybersecurity of its infrastructure, the FAA Chief Information Security Officer (CISO) and the Chief Information Officer have overall responsibility for the FAA's cybersecurity and ensuring that Domain operators comply with applicable agency, departmental, and federal requirements.

Overall, the FAA manages all aspects of the agency's cybersecurity mission through the Cybersecurity Steering Committee (CSC). The CSC was established in 2014 after the agency recognized the need to work more holistically at cybersecurity across the FAA enterprise. The CSC is charged with developing the FAA's cybersecurity strategy, setting priorities, and operational guidelines in support of an integrated agency-wide approach to protecting the FAA from cyber-threats. The FAA Cybersecurity Strategy was first developed in 2015 and sets clear goals and objectives for the FAA's cybersecurity program. These responsibilities are all accomplished through the collaboration of AFN, ATO, ANG, the Office of Aviation Safety (AVS), the Office of Airports, the Office of Security & Hazardous Materials Safety, and the Department of Transportation (DOT) CISO as members of the FAA CSC. With the input of these groups, other FAA offices as needed, and oversight of the CSC by senior FAA officials, the FAA continues to review, update, and maintain the framework to support a more cyber-secure and resilient aviation ecosystem.

Following the establishment of the CSC, Congress continued to recognize the growing significance of cyber-threats. In 2016, Congress directed the FAA to develop a comprehensive strategic framework to reduce cybersecurity risks to the NAS, civil aviation, and agency information systems. Congress also directed the FAA to establish a cybersecurity research and development plan for the NAS, clarify cybersecurity roles and responsibilities of FAA offices and employees, identify and implement actions to reduce cybersecurity risks to air traffic control systems, and assess the cost and timeline of developing and maintaining an agency-wide cybersecurity threat model.[2] In response to the mandate, the FAA expanded its Cybersecurity Strategy and it is updated annually. The Cybersecurity Strategy discusses in detail the FAA's five goals which are: 1) refine and maintain a cybersecurity governance structure to enhance cross-domain synergy; 2) protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery; 3) enhance data-driven risk management decision capabilities; 4) build and maintain workforce capabilities for cybersecurity; and 5) build and maintain relationships with, and provide guidance to, external partners in government and industry to sustain and improve cybersecurity in the aviation ecosystem.

In 2018, Congress directed the FAA to assess the Cybersecurity Strategy for risks, review its objectives, and assess the FAA's level of engagement with stakeholders in carrying out the Strategy.[3] Although the FAA found the Cybersecurity Strategy's framework to be fundamentally sound, modifications were made to align it with other executive branch cyber initiatives, such as the National Cybersecurity Strategy and the National Strategy for Aviation Security. Enhancements were made to address the growing use of cloud and "as-a-service" technologies. The Cybersecurity Strategy was also modified to reflect efforts to improve response times in mitigation of internet-facing vulnerabilities, as well as cyber hygiene principles. It was strengthened by including a focus on external stakeholder engagement activities, including information-sharing and best practices around aviation cybersecurity.

Further, in response to a March 2019 DOT Office of Inspector General audit of FAA's Cybersecurity Strategy, the FAA finalized the application of its cyber risk model to support its air traffic mission and related systems, and established priorities for research and development activities on cybersecurity. These efforts have improved the FAA's ability to maintain up-to-date capabilities necessary for identifying and addressing rapidly evolving cyber threats.

[2] Pub. Law No. 114–190, § 2111.
[3] Pub. Law No. 115–254, § 509.

FAA's Cybersecurity Role in the Aviation Ecosystem

When discussing cybersecurity as it relates to aviation, the FAA frequently refers to the "aviation ecosystem." Aspects of the aviation ecosystem include aircraft, air carriers, airports, air traffic operations, maintenance facilities and the personnel that carry out the functions for each. Although there is some overlap of cyber responsibilities with other participants for certain parts of the ecosystem, the FAA has safety oversight responsibilities for aircraft design, manufacturing and testing of aeronautical products, production, the continuous operational safety of certified products, and the certification of airmen and maintenance personnel. This includes components installed in aircraft, such as avionics. These responsibilities require the FAA to routinely engage with other aviation cybersecurity stakeholders including the private sector and other executive branch agencies that may have cyber responsibilities in the aviation ecosystem.

With respect to FAA's safety oversight responsibility in certificating aircraft, modern airplanes are designed and equipped with safety-enhancing systems that enable improved communications and navigation information. These systems rely on connectivity between an airplane and ground or space-based infrastructure. The reliance upon such connectivity creates cyber risks and, since such risks could affect the airworthiness of the aircraft, requires that such risks be addressed during the certification process. As part of the FAA's certification practices for standard category aircraft, cybersecurity risk assessments are conducted by the applicant when they apply for design certification or a change to a previously certified product. The FAA relies upon its broad safety regulatory authority to ensure that cyber risks are managed through the application of applicant-specific "special conditions" that require critical aircraft systems to be protected from adverse intentional unauthorized electronic interference. The FAA issues special conditions, which are rules of particular applicability, when the current airworthiness regulations do not contain adequate or appropriate safety standards for a novel or unusual design feature. The FAA addresses cybersecurity safety issues in much the same way as all safety issues, by monitoring safety impacts using a data-driven methodology. In response to an October 2020 Government Accountability Office report, the FAA conducted an initial cybersecurity risk assessment of avionic systems.[4] The FAA intends to do an in-depth analysis of our oversight responsibilities with respect to current and evolving avionics. At the request of the FAA, the Aviation Rulemaking Advisory Committee made 30 recommendations on Aircraft Systems Information Security and Protection. To date, the FAA has updated policy, standards and industry guidance for certifying critical aircraft systems.

The FAA also has a direct operational role in the air traffic aspect of the aviation ecosystem and manages cyber threats to the NAS Domain through ATO. The NAS Domain consists of over a hundred systems and an ever-growing networking infrastructure. The networking infrastructure is dedicated to NAS Domain operations and segregated from non-NAS infrastructures via secure monitored gateways. The NAS Domain provides five major FAA mission-critical services that directly support air traffic control: automation, communications, navigation, surveillance, and weather. ATO is responsible for air navigation services in all U.S.-controlled airspace and performs maintenance services for all NAS Domain systems. ATO is responsible for NAS Domain operational cybersecurity and provides the identification, protection, detection, response, and recovery capabilities to ensure continued NAS Domain operations under a range of cyber conditions. Further, in support of its cyber responsibilities for the NAS, in 2015, the FAA established the Cyber Test Facility, or CyTF, to assess cyber threats and vulnerabilities and conduct cyber testing and evaluation.

FAA's Coordination with Other Stakeholders in the Aviation Ecosystem

One of the major components of the FAA's Cybersecurity Strategy is focused on the FAA's continual effort to build and maintain relationships with, and provide guidance to, external partners in government and industry to sustain and improve cybersecurity in the aviation ecosystem. Building trust between the FAA and aviation cybersecurity stakeholders is critical to the success of building an aviation cybersecurity framework that enhances defense, reaction, and recovery from a cyber-incident and improves resilience. An example of the FAA's efforts in this area is the establishment of the Aviation Cyber Initiative (ACI) interagency task force. In May 2019 the Secretaries of Transportation, Homeland Security, and Defense chartered ACI as a forum for coordination and collaboration among federal agencies on a wide

[4] https://www.gao.gov/assets/gao-21-86.pdf.

range of activities aimed at cyber risk reduction within the aviation ecosystem. Such activities include research, development, testing, evaluation initiatives relating to aviation cybersecurity, engaging with stakeholders on activities for reducing cyber risks, and seeking potential improvement opportunities and risk mitigation strategies. The task force is tri-chaired by the three Departments, with the FAA representing the DOT on the task force. Some of the key areas for ACI working groups involve efforts to increase information sharing among ecosystem stakeholders—including airports and airlines, participation in inter-agency cyber exercises, and the development of risk mitigation strategies and guidance to improve and standardize risk management across the aviation ecosystem.

FAA's outreach, collaboration, and coordination with other stakeholders in the aviation ecosystem is not limited to its participation in ACI, and the FAA will continue to support information sharing efforts within the aviation industry to develop information security standards and best practices consistent with the National Institute of Standards and Technology Cybersecurity Framework. This engagement recognizes the increasingly interconnected nature of aviation information systems from the flight deck to air traffic control and air carrier operations, which necessitate innovative and collaborative solutions to secure them. Additionally, one-on-one engagements with industry groups and standards bodies are essential to ensure comprehensive cybersecurity policy and guidance for manufacturers and operators of aircraft. Further, the FAA will continue to actively engage with stakeholders around the globe to raise awareness of cybersecurity issues relevant to the aviation ecosystem and support initiatives to address cyber threats and vulnerabilities in a coordinated and collaborative manner.

FAA'S CYBERSECURITY WORKFORCE

One of the overarching goals of the FAA's Cybersecurity Strategy is to continue building and maintaining the agency's workforce capabilities for cybersecurity. Congress also recognized the importance of this effort and in 2018 directed the FAA to enter into an agreement with the National Academy of Sciences to conduct a study on the FAA cybersecurity workforce in order to develop recommendations to increase its size, quality, and diversity.[5] In June 2021, the FAA received the results of the Cyber Workforce Study, conducted by the National Academy of Sciences. The study identified key challenges facing the FAA's cyber workforce, it noted opportunities for strengthening that workforce, and made recommendations to help the FAA capitalize on those opportunities and address the challenges. For example, the study emphasized the importance of the FAA's ability to anticipate the need to continually retool the cybersecurity skills of its workforce given the rapidly changing nature of the challenge. It noted that the FAA cannot assume that today's cyber knowledge and skills will be sufficient to meet the needs of the future. The FAA recognizes that leveraging training and reskilling for the workforce will be a powerful tool for the FAA to grow and maintain the cyber skills needed now and in the future. The FAA also embraces the value of workforce training through participation in exercises. For example, the FAA regularly exercises its incident response plan to ensure familiarity with communications and escalation procedures. These internal exercises provide valuable experience for staff and increase the level of preparedness to respond to a cyber-incident. The FAA will continue to examine where expanding internal exercises will benefit preparedness.

Finally, many of the recommendations in the National Academy of Science study are consistent with the FAA's cybersecurity strategic objectives, and many others align with broader ongoing FAA workforce development, diversity, and recruitment efforts. As technology and systems continue to evolve to meet the aviation challenges of tomorrow, so must our workforce. The FAA recognizes that a diverse pool of talent is critical to finding the right people for the right job at the right time. We also recognize that competitiveness in cybersecurity hiring and retention is important in order to attract and retain top talent. The FAA will use all of its federal recruiting, hiring and retention capabilities to continue building and to maintain the FAA cybersecurity workforce.

CONCLUSION

Chair DeFazio, Ranking Member Graves, and Members of the Committee, the FAA's cybersecurity responsibilities and our strategy to implement those responsibilities has expanded and evolved significantly over the years. Our efforts to address cybersecurity challenges have benefited from congressional oversight, our own

[5] Pub. Law No. 115–254, § 549.

initiatives, and our cooperative efforts with other executive branch agencies. As the technology of the aviation ecosystem evolves, we expect that cybersecurity will continue to be a growing challenge and a significant aspect of both aviation safety and the efficient use of airspace. We look forward to keeping Congress informed of our progress on all aspects of cybersecurity. I would be happy to answer any questions you may have.

Mr. DEFAZIO. Thank you. Thank you, Mr. Grossman.

Now, Ms. Victoria Newhouse, you are recognized for 5 minutes.

Ms. NEWHOUSE. Good morning, Chairman DeFazio, Ranking Member Graves, and distinguished members of this committee. My name is Victoria Newhouse, and I serve as the Deputy Assistant Administrator for Policy, Plans, and Engagement at the Transportation Security Administration. I greatly appreciate the opportunity to appear before you today to discuss TSA's important role in cybersecurity for our Nation's infrastructure.

As you know, TSA was established by the Aviation and Transportation Security Act, which was signed into law on November 19th, 2001. Under that law, TSA assumed the mission to oversee transportation security in all modes of transportation, be that aviation, or the Nation's surface transportation system, mass transit and passenger rail, freight rail, highway and motor carrier, pipeline, as well as supporting maritime security with our United States Coast Guard partners.

As we recently observed TSA's 20th anniversary, we rededicated ourselves to our critical mission to protect our Nation's transportation systems.

My personal commitment to TSA's important mission to ferociously protect our homeland is fueled by my own personal experience on September 11, 2001, surviving the attack on the Pentagon on that fateful day, when we all lost over 2,977 friends, family members, and colleagues.

This is not a mission we can accomplish alone. Our success is highly dependent on close collaboration and strong relationships with our transportation industry stakeholders and our Federal agency partners, including several who are on this esteemed panel today.

Cybersecurity incidents affecting transportation are a growing, evolving, and persistent threat. Across the U.S. critical infrastructure, cyber threat actors have demonstrated their willingness and ability to conduct malicious cyber activities targeting critical infrastructure by exploiting the vulnerability of operational technology and information technology systems. Malicious cyber actors continue to target U.S. critical infrastructure through transportation systems. For instance, as mentioned earlier, the ransomware incident against the Colonial Pipeline last May underscores this threat.

TSA is highly dedicated to protecting our transportation networks against these evolving threats, and we continue to work collaboratively with public and private stakeholders to drive the implementation of intelligence-driven, risk-based policies and programs, and continue our robust information-sharing efforts.

As reflected in the cybersecurity infrastructure testimony provided by our industry colleagues on November 4th of this year, we have a vital national interest in understanding, mitigating, and protecting its people and infrastructure from cybersecurity threats. Constantly evolving potential for malicious cyber activity against the transportation infrastructure points to the need for continued vigilance, information sharing, and development of dynamic policies and capabilities to strengthen our cybersecurity posture. TSA has fought to mitigate the degradation, destruction, or malfunction of systems that control this infrastructure by implementing immediate security requirements through security policies.

After the Colonial Pipeline ransomware incident in May, there was a clear understanding that we need to take more actions to prevent another pipeline incident in the future. In that vein, TSA issued two security directives to immediately address these threats. We required the pipeline operators who operate and transport over 85 percent of the Nation's energy and assets to take immediate actions to report cybersecurity incidents to my partner agency, Cybersecurity and Infrastructure Security Agency; designate an express cybersecurity coordinator that is available 24/7; and implement specific mitigation measures.

We continue our work across all of our modes, as credible cyber threat information is driving our most recent efforts to issue more directives in this vein. As Chairman DeFazio mentioned earlier, we are working with our rail, higher risk freight rail, passenger rail, and rail transit operators, and aviation in four critical actions: designate a cybersecurity coordinator; reporting incidents to CISA; developing an incident response plan; and conducting self-assessments to address potential vulnerabilities and gaps.

Chairman DeFazio, we continue our robust engagement with our partners through our Surface Transportation Security Advisory Committee and our Aviation Security Advisory Committee, along with numerous corporate executives, all the way down to the security level.

Chairman DeFazio, on behalf of all of my colleagues at TSA, we would like to congratulate you on your decades of service, and thank you for your service to all of us in our Nation.

I look forward to taking any questions you may have. Thank you.

[Ms. Newhouse's prepared statement follows:]

Prepared Statement of Victoria Newhouse, Deputy Assistant Administrator for Policy, Plans, and Engagement, Transportation Security Administration, U.S. Department of Homeland Security

Good morning, Chairman DeFazio, Ranking Member Graves, and distinguished Members of the Committee. My name is Victoria Newhouse and I serve as the Deputy Assistant Administrator for Policy, Plans, and Engagement within the Transportation Security Administration (TSA). I appreciate the opportunity to appear before you today to discuss TSA's role in cybersecurity for our Nation's infrastructure.

TSA was established by the *Aviation and Transportation Security Act* (ATSA), which was signed into law on November 19, 2001. With the enactment of ATSA, TSA assumed the mission to oversee security in all modes of transportation, be that aviation or the Nation's surface transportation systems—mass transit and passenger rail, freight rail, highway and motor carrier, pipeline, as well as supporting maritime security with our U.S. Coast Guard (USCG) partners. As we recently observed TSA's 20th anniversary, we rededicated ourselves to our critical mission to protect our Nation's transportation systems as they remain attractive targets for our adversaries to directly attack our Homeland, our commercial markets, and ultimately the freedoms we hold so dear. My personal commitment to TSA's important mission to ferociously protect our Homeland is fueled by my own experience on September 11, 2001, surviving the attack on the Pentagon on that fateful day when we lost 2,977 friends, family members and colleagues. This is not a mission we can accomplish alone. TSA's mission success is highly dependent on close collaboration and strong relationships with our transportation industry stakeholders and our Federal agency partners, including several who are present on this esteemed panel today. TSA's motto—"not on my watch"—truly reflects our collective approach to secure our Homeland against all threats, including cybersecurity threats.

TRANSPORTATION CYBERSECURITY THREATS

Cybersecurity incidents affecting transportation are a growing, evolving, and persistent threat. Across U.S. critical infrastructure, cyber threat actors have demonstrated their willingness and ability to conduct malicious cyber activity targeting critical infrastructure by exploiting the vulnerability of Internet-accessible Operational Technology (OT) assets and Information Technology (IT) systems. Malicious cyber actors continue to target U.S. critical infrastructure, to include transportation systems, through malicious cyber activity and cyber espionage campaigns. For instance, the ransomware incident against Colonial Pipeline last May underscores this threat. The United States' adversaries and strategic competitors will continue to use cyber espionage and malicious cyber activity to seek economic, political and military advantage over the United States and its allies and partners. TSA is dedicated to protecting our Nation's transportation networks against evolving threats and continues to work collaboratively with public and private stakeholders to expand the implementation of intelligence-driven, risk-based policies and programs and continue robust information sharing to reinforce the security posture of these networks.

ADDRESSING CYBERSECURITY THREATS

As reflected in cybersecurity and infrastructure testimony provided by industry colleagues to this committee on November 4, 2021, the United States has a vital national interest in understanding, mitigating, and protecting its people and infrastructure from cybersecurity threats in the transportation domain. The constantly evolving potential for malicious cyber activity against the transportation infrastructure point to the need for continued vigilance, information sharing, and development of dynamic policies and capabilities to strengthen our cybersecurity posture. Consistent with the President's *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 28, 2021), Department of Homeland Security priorities, and our broader statutory authorities, TSA has sought to mitigate the "degradation, destruction, or malfunction of systems that control this infrastructure" by implementing immediate security requirements through security policies.

After the Colonial Pipeline ransomware incident in May, there was a clear understanding across the Administration, Congress, industry, and the public for the need to take action to prevent another pipeline incident in the future. The TSA Administrator leveraged authority under 49 U.S.C. § 114 to respond to emerging threats by directing select owners and operators of pipeline and natural gas facilities to implement necessary cyber protections. TSA issued two Security Directives (SDs), effective May 28, 2021, and July 26, 2021, to immediately address these threats. Among several requirements, the SDs required pipeline companies to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA), designate a cybersecurity coordinator to be available 24/7, and implement specific mitigation measures to protect against ransomware incidents.

Credible cyber threat information also supported our recent efforts to implement similar security measures across the domestic surface and aviation transportation networks. In the surface domain, new cybersecurity protocols require higher risk freight railroads, passenger rail and rail transit operators to take four critical actions:

1. Designate a cybersecurity coordinator;
2. Report cybersecurity incidents to CISA;
3. Develop a cybersecurity incident response plan to reduce the risk of an operational disruption; and
4. Conduct a cybersecurity self-assessment to identify potential gaps or vulnerabilities in their systems.

In addition to these requirements, TSA also issued an Information Circular to lower risk surface transportation operators, including over-the-road buses and lower risk rail operators, strongly recommending they immediately implement these same measures.

Within the aviation subsector, TSA recently updated established security programs with these same measures, starting with designating a cybersecurity coordinator and reporting specific cybersecurity incidents to CISA. In a second set of security program updates to be issued in the near future, TSA will also implement the requirements to conduct cybersecurity self-assessments and develop cybersecurity incident response plans.

DHS and TSA engaged with stakeholders throughout the development process for these measures to ensure awareness of the threat picture, review draft proposals, and obtain industry feedback. This included stakeholder CEO-level discussions with DHS and TSA leaders, threat briefings for aviation, pipeline, and other surface transportation stakeholders, multiple policy reviews by industry and government stakeholders, and consistent engagement sessions with transportation associations and regulated entities for awareness on the proposed strategies. For example, we engaged TSA's Surface Transportation Security Advisory Committee (STSAC) on several occasions to share and discuss these new security requirements and held numerous stakeholder calls and engagements with the specific covered operators prior to issuing these most recent security requirements. In addition, airport and airline stakeholders also provided extensive input to our aviation cyber requirements to ensure they can operationalize them effectively and efficiently. Our interagency partners also participated extensively to ensure unity of effort across DHS and the interagency. We incorporated stakeholder inputs resulting in revisions to these cybersecurity policy requirements, including adjustments to incident reporting and response plan timeframes, defining reportable cybersecurity incidents, and using established methods to conduct self-assessments. We continue working closely with stakeholders to assist with implementation and respond to any questions regarding these requirements with an eye on continually improving our collective efforts to secure the Nation's transportation systems from cyber threats.

INFORMATION SHARING AND ENGAGEMENT

Our work does not simply end after issuing these cybersecurity requirements. On the contrary, the TSA enterprise continues our robust stakeholder engagement to mitigate cyber threats. We work closely with these covered operators to successfully implement these requirements, educate our vast network of transportation operators, and continue to seek input from both the STSAC and the Aviation Security Advisory Committee (ASAC) on how to best integrate cybersecurity into the fabric of our transportation security mission. For example, we have sought, incorporated, and continue to seek stakeholder input, including from those advisory committees, on TSA's Cybersecurity Roadmap. TSA conducts robust outreach with thousands of individual transportation operators to implement these requirements and ensure consistent application across the transportation sector. We continually seek opportunities to expand information exchanges and to provide evaluation tools and training programs to evaluate systems, identify vulnerabilities, and incorporate security measures and best practices that mitigate cyber threats. This includes efforts such as the Baseline Assessment for Security Enhancement (BASE) program and the Intermodal Security Training and Exercise Program (I–STEP). TSA actively supports broader DHS efforts, such as the 60-day Transportation Cybersecurity Sprint in September and October that focused on enhancing cyber risk management and cybersecurity in the context of the transportation sector with particular emphasis on TSA, CISA, and USCG engagements.

On behalf of DHS, TSA and USCG are the Co-Sector Risk Management Agency for the Transportation Security Sector (TSS) along with the Department of Transportation (DOT). In that role, TSA serves as the executive agent with the USCG for developing, deploying, and promoting TSS-focused cybersecurity initiatives, programs, assessment tools, strategies, and threat and intelligence information-sharing products. TSA is in close alignment with CISA and coordinates on both a tactical and strategic level to raise the cybersecurity baseline across the transportation sector.

TSA also supports DHS's cybersecurity efforts in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Framework). The Framework is designed to provide a foundation for industry to better manage and mitigate their cyber risk. TSA shares information and resources and develops products for stakeholders to support their adoption of the Framework. For example, TSA in conjunction with the USCG and the DOT, has been working with NIST to develop transportation-specific profiles for the Framework through a series of sector surveys to allow for further targeted sector adoption of the Framework.

Robust information and intelligence sharing is a key enabler of TSA's mission to protect the nation's transportation systems to ensure the freedom of movement for people and commerce. TSA coordinates with the DHS Office of Intelligence and Analysis and Intelligence Community (IC) partners across the federal government to share cyber threat information with industry as soon as it becomes available. To enhance mission performance, TSA also facilitates both classified and unclassified briefings for industry representatives to ensure that the evolving threat picture is communicated to trade associations, industry executive leadership, and key industry security personnel. TSA's commitment to information sharing is strongly supported by two full-time threat intelligence sharing cells—the Aviation Domain Intelligence Integration & Analysis Cell (ADIAC) and the Surface Information Sharing Cell (SISC). Through these information sharing entities, TSA shares thousands of threat items, including cyber threat information. Additionally, we issue various cyber assessments and analytic products, including Cybersecurity Awareness Messages to operators and other products in conjunction with our sister component CISA and Federal law enforcement, to ensure widest distribution across the transportation sector. These two information sharing cells are excellent examples of government and industry partnership, and their establishment resulted directly from stakeholder collaboration. For instance, the SISC's establishment fulfills an important STSAC recommendation, and we continue working to enhance the SISC's capabilities.

CLOSING

Chairman DeFazio, Ranking Member Graves, and distinguished Members of the Committee, thank you for this opportunity to share the steps and measures TSA has taken in concert with our stakeholders to strengthen transportation critical infrastructure to address the serious and persistent cybersecurity threat. TSA is committed to ensuring appropriate security measures are in place to increase the cyber and physical security posture of our Nation's transportation systems. Thank you for the chance to appear before you today. I look forward to answering any questions you may have.

Mr. DEFAZIO. Thanks, Ms. Newhouse. I have quite a history with TSA. John Mica chaired the Aviation Subcommittee, and I was ranking, and it was under our jurisdiction then. We had no Homeland Security Committee, and we stood it up in pretty short order. And I can say it is still a work in progress. But, it is so far ahead of where we were pre-9/11. And I would love to go into that at some point and talk about it. But anyway, it is not the subject of this hearing.

Rear Admiral John W. Mauger?

Admiral MAUGER. Good morning, Chairman DeFazio, Ranking Member Graves, and distinguished members of the committee. I am honored to be here this morning to discuss cybersecurity in the maritime transportation system, a top priority for the Coast Guard.

Our national security and economic prosperity are inextricably linked to a safe and efficient Marine Transportation System, or MTS. The MTS is an integrated network of 361 ports and 25,000 miles of waterways. Marine transportation supports one-quarter of U.S. GDP, and provides employment for one in seven working-age Americans. The MTS enables our Armed Forces to project power around the globe, and any substantial disruption to marine transportation can cause cascading effects to our economy and to our national security. Cyberattacks are a significant threat to the maritime critical infrastructure. And while we must continue to work to prevent attacks, we must also be clear-eyed that attacks will occur, and we must ensure that the MTS is resilient.

Protecting maritime critical infrastructure and ensuring resiliency is a shared responsibility. Thank you for holding both sessions to allow industry and Government to describe their efforts.

The Coast Guard is the Nation's lead Federal agency for protecting the MTS. In August, the Commandant released a cyber strategic outlook to guide our work ahead. At the core of the Coast Guard strategy is the recognition that cybersecurity is an operational imperative, both for our Service and for the maritime industry. With support from Congress, we established Coast Guard Cyber Command, and built an operational force to execute missions and protect Coast Guard and DoD networks. Coast Guard cyber forces are manned, trained, and equipped, in accordance with joint DoD standards, but have a broad range of authorities to address complex issues spanning national defense and homeland security, including protecting the MTS.

The Coast Guard's approach to protecting the MTS leverages our proven prevention and response framework. To prevent incidents, we leverage our authorities in the Nation's ports to set standards and conduct compliance. We refer to this as "cyber risk management" and require accountability assessments, mitigation exercises, and incident reporting. To prepare for and respond to cyber incidents, Coast Guard sectors are leading field-level exercises with Area Maritime Security Committees and have established unified commands with FBI and CISA to lead the Federal response to cyberattacks in the ports.

Cyberattacks will increasingly have physical impacts beyond computer networks. By incorporating cybersecurity into our prevention and response framework, we provide a comprehensive, all-hazards approach to this threat. But we cannot do this alone. As the co-Sector Risk Management Agency for transportation, we look to both CISA and TSA as key partners.

The MTS is dependent on other critical infrastructure. CISA coordinates across sectors, shares threat and vulnerability information, and provides cyber technical assistance. These efforts build coherence within the interagency, foster collaboration with the private sector, and enhance our ability to protect the MTS. Our relationships with CISA and TSA are strong, and will continue to mature.

Cybersecurity is a shared responsibility with the private sector, as well. Collaboration with the industry is paramount and focused on information sharing and good governance. At the national level, we stood up a Maritime Cyber Readiness Branch within Coast Guard Cyber Command as a focal point for maritime threat monitoring, information sharing, and response coordination. At the local level, we continue to strengthen communications through engagement at our Area Maritime Security Committees.

Risk-based regulations, which leverage international and industry-recognized standards, are the foundation for good governance. With congressional support, we established the National Maritime Security Advisory Committee to facilitate consultation with industry on standards development. We worked with the International Maritime Organization, or IMO, to address the risks posed by foreign vessels. We are committed to a transparent approach, as we balance the urgency of cyber threats with informed rulemaking.

The cyber threat is dynamic. As we continually evolve to address emergent needs, we will need Congress' continued support. We are grateful for the fiscal year 2021 appropriations. The investments in

Coast Guard Cyber Command provide additional capability for our Service, and serve a key role in protecting the MTS. The establishment of 22 MTS cyber advisors in the field are key nodes for coordination and collaboration at our field units.

We look forward to the continued dialogue with Congress on this important issue, and I appreciate the opportunity to testify, and look forward to your questions.

[Admiral Mauger's prepared statement follows:]

Prepared Statement of Rear Admiral John W. Mauger, Assistant Commandant for Prevention Policy, U.S. Coast Guard

Introduction

Good morning Chairman DeFazio, Ranking Member Graves, and distinguished Members of the Committee. I am honored to be here to discuss a top priority for the U.S. Coast Guard: cybersecurity in the marine transportation system (MTS). Since the early days of the Revenue Cutter Service, we have protected our Nation's waters, harbors, and ports. While much has changed over the centuries—with our missions expanding from sea, air, and land into cyberspace—our ethos and operational doctrine remain steadfast. We employ a risk-based approach to protect the Nation from threats in the maritime environment. Regardless of the threat, we leverage the full set of our authorities; the ingenuity and leadership of our people; and the breadth of our civil, military, and law enforcement partnerships to protect the Nation, its waterways, and those who operate on them.

I recognize that protecting the MTS from cyber threats is also a top priority for Congress. The Coast Guard thanks Congress for Fiscal Year 2021 appropriations that will deliver more cyber risk management capability for the nation and build a more resilient MTS. The Coast Guard is committed to maximizing the return on this important investment and we look forward to the continued dialog with Congress on such a critical issue for our country.

The Criticality of the Marine Transportation System

Our national security and economic prosperity are inextricably linked to a safe and efficient MTS. One of the challenges with protecting the MTS is that it can be difficult to quantify. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. But it is more than ports and waterways. It is cargo and cruise ships, passenger ferries, waterfront terminals, offshore facilities, buoys and beacons, bridges, and more. The MTS supports $5.4 trillion of economic activity each year and accounts for the employment of more than 30 million Americans. It also enables critical national security sealift capabilities, enabling U.S. Armed Forces to project and maintain power around the globe.

The maritime transportation of cargo is considered the most economical, environmentally friendly, and efficient mode of freight transport. As the economic lifeblood of the global economy and critical to U.S. national interests, the MTS connects America's consumers, producers, manufacturers, and farmers to domestic and global markets. Any significant disruption to the MTS, whether man-made or natural, has the potential to cause cascading and devastating impact to our domestic and global supply chain and, consequently, America's economy and national security.

The Growing Cyber Risks

Cyber attacks are a significant threat to the economic prosperity and security of the MTS, and will require a whole of nation effort to address the threat. The MTS's complex, interconnected network of information, sensors, and infrastructure continually evolves to promote the efficient transport of goods and services around the world. The information technology and operational technology networks vital to increasing the efficiency and transparency of the MTS also create complicated interdependencies, vulnerabilities, and risks.

The size, complexity, and importance of the MTS make it an attractive target. Terrorists, criminals, activists, adversary nation states and state-sponsored actors may view a significant MTS disruption as favorable to their interests. The diversity of potential malicious actors and their increasing levels of sophistication present substantial challenges to government agencies and stakeholders focused on protecting the MTS from constantly evolving cyber threats.

Recent destructive cyber activities highlight the risk posed to the vast networks and system of the MTS. Cyber attacks, such as ransomware attacks, can have a devastating impact on the operations of maritime critical infrastructure. A successful cyber attack could impose unrecoverable losses to port operations, electronically-stored information, national economic activity, and disruption to global supply chains. The increased use of automated systems in shipping, offshore platforms, and port and cargo facilities creates enormous efficiencies, but also introduces additional attack vectors for malicious cyber actors. This growing reliance on cyber-physical systems and technologies requires a comprehensive approach by all MTS stakeholders to manage cyber risks and ensure the safety and security of the MTS.

Shared Responsibility

The U.S. Coast Guard is the Nation's lead federal agency for safeguarding the MTS. We apply a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces. Our authorities and capabilities cut across threat vectors, allowing operational commanders at the port level to quickly evaluate risks, apply resources, and lead a coordinated and effective response.

Just like the other risks we manage, the maritime industry has a vital role in cyber risk management—Cyber risk management is a shared responsibility. In a number of forums and industry engagements, I hear the consistent message that cybersecurity does not have a one-size-fits-all solution. I agree with that assessment. However, the building blocks of sound cyber risk management practices have common threads across the maritime industry and other critical infrastructure sectors.

It starts with accountability and focus. First, companies need to identify and empower a responsible person with the authority and resources to address the cyber challenge. Then, companies need to have a plan. This includes conducting vulnerability assessments, identifying gaps, and working to close them. Third, companies need to exercise their plan, so cybersecurity is ingrained in all of the work they do. Lastly, companies need to report cyber incidents—reporting of cybersecurity incidents is absolutely critical because it enables a coordinated response, and more importantly, can help to inform other companies and critical infrastructure to take action and mitigate risk.

Information sharing is clearly an essential component of our shared responsibility, and we have heard from industry that it must happen at the "speed of cyber" to spur meaningful prevention and response activities. While we have existing information sharing networks—within the Coast Guard and across government—we must deliver specific, timely information with appropriate levels of privacy protection in order to build trust and confidence in the system. Without that trust, we will lose the massive benefit of the industry's perspectives, experiences, and trends.

The U.S. Coast Guard's Approach

For the U.S. Coast Guard, protecting the MTS from threats is not new, and we will continue to leverage our foundational operational concepts and strong relationships to strengthen the cyber resiliency of the MTS. In August of 2021, we released a new Coast Guard Cyber Strategic Outlook that outlines our strategic direction for facing cyber threat. One of the three primary Lines of Effort is to "Protect the Marine Transportation System," and a fundamental element for this effort is applying our proven prevention and response framework.

Prevention

The Prevention Concept of Operations—Standards, Compliance, and Assessment—guides all of our prevention missions including our cyber risk management activities. It begins with establishing expectations in the MTS. Regulations and standards provide a set of minimum requirements, and are critical to establishing effective and consistent governance regimes. With effective standards in place, compliance activities systematically verify that the governance regime is working. This part of the system is vital in identifying and correcting potential risks before they advance further and negatively impact the MTS. Effective assessment is paramount to continuous improvement. It provides process feedback and facilitates the identification of system failures so that corrective actions can be taken to improve standards and compliance activities.

Importantly, we are operationalizing this framework at the port-level. U.S. Coast Guard Captains of the Port are overseeing Maritime Transportation Security Act (MTSA)-regulated facilities as they incorporate cybersecurity into their mandated

Facility Security Assessments and Facility Security Plans. We have provided the industry with detailed guidance on ways to meet the regulatory requirements related to computer systems and networks, including personnel training, drills and exercises, communication, vessel interfaces, security systems, access control, cargo handling, delivery of stores, and restricted area monitoring. On October 1, 2021, Coast Guard field units began reviewing these Facility Security Assessments and Facility Security Plans to validate that cybersecurity is satisfactorily addressed, and all MTSA-regulated facilities will be inspected for compliance by September 30, 2022.

The U.S. Coast Guard worked closely with the International Maritime Organization on guidelines for commercial vessels operating internationally to integrate cyber risk management into mandated safety management systems. During regular inspections, the U.S. Coast Guard is verifying that foreign vessels operating in U.S. waters are complying with these requirements.

The U.S. Coast Guard is hiring Cybersecurity Advisors at each Area, District, and Captain of the Port Zone. These new positions create a dedicated staff to build and maintain port level cyber-related relationships, facilitate information sharing across industry and government, advise Coast Guard and Unified Command decision-makers, and plan cyber-related security exercises.

Finally, Coast Guard Cyber Command's (CGCYBER) Maritime Cyber Readiness Branch is assessing technology employed in the MTS, evaluating known or potential threats, and sharing information across industry and government. Their Cyber Protection Teams (CPTs) are conducting detailed vulnerability assessments of maritime critical infrastructure when requested to help the industry identify and close gaps in their cybersecurity systems.

Response

Similar to our Prevention Concept of Operations, the U.S. Coast Guard has a proven, scalable response framework that can be tailored for all-hazards. This is especially important as cyber incidents can quickly transition to physical impact requiring operational commanders to immediately deploy assets to mitigate risks. Depending on the incident's size and severity, commanders will set clear response priorities, request specialized resources to help mitigate risk, and notify interagency partners to help coordinate the response. We are not approaching this alone.

By regulation, MTSA-regulated vessels and facilities are required to report Transportation Security Incidents, breaches of security, and suspicious activity without delay. We have provided additional guidance on reporting requirements specifically related to cyber incidents. These reports enable our operational commanders to rapidly notify other government agencies, evaluate associated risks, deploy resources, and unify the response.

CGCYBER is also bringing specialized operational capability to MTS cyber response. These teams will support maritime critical infrastructure owners and operators after a cyber attack and provide extensive technical expertise for post-incident investigation, response, and recovery. Their cyber skills are unprecedented for our Service.

While we are converting our strategy into action, we know our work is not done. Through all of these prevention and response activities in the field and engagements with industry, the U.S. Coast Guard will capture lessons learned, recommendations, and best practices that strengthen the maritime industry's cybersecurity posture and inform future policy, law, and regulations.

Partnerships

MTS cyber risk management requires a whole-of-government effort to protect America's critical infrastructure. As the Federal Maritime Security Coordinator, the U.S. Coast Guard Captain of the Port directs Area Maritime Security Committee (AMSC) activities. AMSCs are required by federal regulations and serve an essential coordinating function during normal operations and emergency response. They are comprised of government agency and maritime industry leaders, and have adapted to the cyber threat, serving as the primary local means to jointly evaluate cyber risks, share threat information, and participate in cyber preparedness exercises.

In addition to being the federal government's lead regulator for the MTS, we are also the co-Sector Risk Management Agency (SRMA), along with the Department of Transportation for the Maritime Transportation Subsector, as outlined in Presidential Policy Directive 21. As an SRMA, we are responsible for coordinating risk management efforts, including cyber, with DHS, the Cybersecurity and Infrastructure Security Agency (CISA), other Federal departments and agencies, and MTS stakeholders. We also provide, support, and facilitate technical assistance for the

MTS to address vulnerabilities and develop processes and procedures to mitigate risk.

CISA is a key partner in all of our cyber risk management activities. CISA's technical expertise directly supports our ability to leverage our authorities and experience as the regulator and SRMA of the MTS. CISA provides technical expertise, integrates a whole-of-government response, analyzes broader immediate and long-term impacts, and facilitates information sharing across transportation sectors. Our relationship with CISA is strong and will continue to mature.

Our enduring relationship with the Department of Defense (DoD) is also crucial to safeguarding the MTS. In many cases, DoD's ability to surge forces from domestic to allied seaports depends on the same commercial maritime infrastructure as the MTS. We must ensure our surge capability and sea lines of communication will be secure and available during times of crisis. By sharing intelligence on cyber threats, developing interoperable capabilities like Cyber Protection Teams, and using DoD's expertise to protect our own cyber networks, we enable national security sealift capabilities and jointly support our nation's ability to project power around the globe.

FUTURE FOCUS

Recent cyber incidents, including attacks on multiple segments of maritime critical infrastructure only reinforce that cyberspace is a contested domain. Working in close collaboration with the Department of Homeland Security, CISA, and our other government partners, foreign allies, and the maritime industry, we will continue to leverage strong and established relationships across the maritime industry—at the international, national, and port levels—to build confidence and establish trust through cyber prevention and response activities.

We have secured and safeguarded the maritime environment for over 230 years. During that time we have faced many complex challenges. These trials have honed our operating concepts, bolstered our capabilities, and strengthened our resolve. We will employ these same concepts and capabilities to secure and protect our Nation and maritime critical infrastructure from malicious cyber activity and cyber attacks. In addressing cyber risks to ports and other aspects of the maritime industry, our commitment is to address those risks with the same level of professionalism, efficiency, and effectiveness that the public has come to expect. The Coast Guard will continue to adapt, as it has done over the last two centuries, to the challenges and opportunities that accompany technological advancements in our operating environment.

Thank you for the opportunity to testify today, and thank you for your continued support of the United States Coast Guard. I am pleased to answer your questions.

Mr. DEFAZIO. Thank you, Admiral.

Mr. Kevin Dorsey?

Mr. DORSEY. Good morning. Chairman DeFazio, Ranking Member Graves, and distinguished members of the committee, thank you for inviting me to testify on securing our Nation's infrastructure in an evolving cybersecurity landscape.

The Department of Transportation relies on over 400 IT systems to ensure the safety and efficiency of our Nation's transportation system.

As you know, malicious cyberattacks and other compromises to these systems and DOT networks may put public safety, sensitive information, or taxpayer dollars at risk. Our office has long identified cybersecurity as one of the Department's top management challenges.

Today I will focus on three key areas: one, developing a comprehensive, DOT-wide cybersecurity strategy to address recurring weaknesses; two, protecting IT infrastructure and sensitive information within DOT's operating administrations; and three, coordinating with other agencies and industry partners.

First, on the whole, DOT has established formal policies and procedures for a cybersecurity program that align with Federal guidelines. However, it still faces challenges implementing this program in a consistent or comprehensive manner. As a result, DOT faces the risk that its mission-critical systems could be compromised. Our office has reported on longstanding deficiencies due to DOT's inconsistent enforcement of an enterprisewide information security program, ineffective communication with its operating administrations, and inadequate efforts to remediate recurring weaknesses.

Many of these weaknesses can be attributed to DOT's lack of progress in addressing 66 of our prior audit recommendations, including those to resolve more than 10,000 identified vulnerabilities.

Leadership challenges also limit DOT's oversight. For example, the individual serving as the acting chief information security officer over the last year was not tasked with information security as an official primary duty. That has made it difficult for DOT to implement long-term changes.

Second, DOT must better protect the IT infrastructure managed by its operating administrations. For example, to increase cybersecurity, FAA must finish selecting and implementing more stringent security controls for 45 high-impact systems that are critical for safely managing air traffic.

In addition, unresolved security control deficiencies with FTA's financial management systems could impede its ability to disburse billions of grant dollars.

Furthermore, during vulnerability assessments and penetration testing of the IT infrastructure at multiple operating administrations, we were able to gain unauthorized access to millions of sensitive records, including personal identifiable information.

Finally, DOT is one of the lead agencies designated to protect the Nation's transportation infrastructure. As such, it must effectively partner with other Federal agencies and the private sector on efforts such as securing cloud-based services and meeting the President's recently issued Executive order on improving cybersecurity. To that end, FAA is working with DHS and DoD on the Aviation Cyber Initiative. Still, as the U.S. upgrades its transportation infrastructure, DOT must continue to strengthen and secure its IT systems and networks, while working to improve its efforts to respond to increasingly sophisticated malicious cyber campaigns.

We remain committed to supporting DOT's efforts as it works to remediate existing vulnerabilities and bolster its overall cybersecurity posture. We will continue to update you on our work on these and related matters.

This concludes my prepared statement. I would be happy to address any questions from you or members of the committee at this time.

[Mr. Dorsey's prepared statement follows:]

Prepared Statement of Kevin Dorsey, Assistant Inspector General for Information Technology Audits, Office of Inspector General, U.S. Department of Transportation

Chairman DeFazio, Ranking Member Graves, and Distinguished Members of the Committee:

Thank you for inviting me to testify today on securing our Nation's infrastructure in an evolving cybersecurity landscape. As you know, the Department of Transportation (DOT) aims to ensure the United States has the safest, most efficient, and modern transportation system in the world. DOT relies on over 400 information technology (IT) systems to carry out this mission, including systems that manage air traffic, administer hundreds of billions of dollars, and maintain sensitive information about the transportation industry. DOT's cybersecurity program must protect these systems from malicious attacks and other compromises that may put public safety or taxpayer dollars at risk.

DOT has expressed a commitment to improving its cybersecurity. Nevertheless, recent cyberattacks remind us why the Department must be prepared at all times to manage cyber threats, which may originate in unfriendly nation-states, international criminal syndicates, and even within the United States. Due to the increasing threat of sophisticated cyberattacks, DOT must frequently update its digital infrastructure, as well as its methodology for monitoring networks, detecting potential risks, identifying malicious activity, and mitigating threats to sensitive information and information systems.

Our office has long identified cybersecurity as one of the Department's top management challenges—a challenge that will be compounded as DOT embarks on implementing new requirements under the President's recent Executive Order to improve the Nation's cybersecurity.[1] My testimony today is based on our recent and ongoing audit work and will focus on DOT's challenges in three areas: (1) developing a comprehensive Departmentwide cybersecurity strategy to address recurring weaknesses, (2) protecting IT infrastructure and sensitive information at DOT Operating Administrations (OA), and (3) coordinating with other agencies and industry partners on cybersecurity in the transportation sector.

Summary

While DOT has formalized and documented most of the policies and procedures for its cybersecurity program, the Department continues to face significant challenges in its implementation. These challenges are due to persistent deficiencies caused by the inconsistent enforcement of an enterprise-wide information security program, ineffective communication with the OAs, leadership gaps, and inadequate efforts to remediate the issues associated with 66 of our prior-year audit recommendations. As a result, DOT faces the risk that its mission-critical systems could be compromised. While working to strengthen its cybersecurity posture across the Department, DOT must also address ongoing challenges in protecting the IT infrastructure that its OAs manage and monitor. These challenges include selecting and implementing more stringent security controls[2] for the Federal Aviation Administration's (FAA) high-impact systems that are critical for safely managing air traffic. We also recently reported that the Federal Transit Administration's (FTA) financial management systems have several security control deficiencies that could affect its ability to approve, process, and disburse billions of dollars of grant funds. Furthermore, our ongoing series of audits of the cybersecurity postures at multiple OAs has identified security weaknesses that could compromise millions of sensitive data records, including personally identifiable information (PII). These weaknesses are of particular concern given that OA networks are connected to DOT's overall IT infrastructure, exposing it to further risk. Finally, as one of the lead agencies[3] in protecting the critical infrastructure of the Nation's transportation sector, DOT must effectively partner with other Federal agencies and the private sector to improve cybersecurity, such as when securing cloud-based services. Such efforts are critically important because the incapacitation or destruction of transportation assets, systems, and networks would have a debilitating effect on the Nation.

[1] Executive Order 14028: Improving the Nation's Cybersecurity (May 12, 2021).

[2] Security controls are safeguards or countermeasures designed to protect the confidentiality, integrity, and availability of information that is processed, stored, or transmitted by systems or organizations and to manage information security risk.

[3] The other lead agency is the Department of Homeland Security.

Background

New guidance from the President has changed the manner in which executive agencies must identify and manage risk associated with information systems. Issued on May 12, 2021, Executive Order 14028: Improving the Nation's Cybersecurity, directs the Federal Government to improve its efforts to identify, deter, protect against, detect, and respond to persistent and increasingly sophisticated malicious cyber campaigns that threaten the public and private sectors and ultimately the security and privacy of the American people. To protect our Nation from malicious cyber actors and foster a more secure cyberspace, the Order also requires the Federal Government to partner with the private sector, which must adapt to the continuously changing threat environment and ensure its products are built and operate securely.

DOT's Office of the Chief Information Officer (OCIO), under authority granted by the Secretary of Transportation, has issued the *Departmental Cybersecurity Policy*,[4] which establishes the policies, processes, procedures, and standards of the DOT cybersecurity program. The policy also implements the mandatory requirements specified for all Federal agencies in the Federal Information Security Modernization Act of 2014 (FISMA), as amended,[5] and other laws, regulations, and standards related to information security, information assurance, and network security. FISMA requires Federal agencies to develop, document, and implement agencywide cybersecurity programs to protect the information and information systems that support their operations and assets. Under FISMA, DOT must provide information security protection commensurate with the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of:

- information collected or maintained by or on behalf of DOT; and
- information systems used or operated by DOT employees or contractors or by another organization on DOT's behalf.

DOT is also required to implement mandatory cybersecurity requirements issued by other entities, including, but not limited to, the White House, Congress, Department of Homeland Security (DHS), Office of Management and Budget(OMB), and National Institute of Standards and Technology (NIST). The Department has adopted NIST's Risk Management Framework as the standard methodology for security authorization for its information systems and continuous monitoring of security controls.

Developing a Comprehensive Departmentwide Cybersecurity Strategy To Address Recurring Weaknesses

For the most part, DOT has formalized and documented its cybersecurity policies and procedures for protecting its information systems and data. Specifically the *Departmental Cybersecurity Policy*, and its supplement, the *Departmental Cybersecurity Compendium*, authorize DOT's Chief Information Officer (CIO) to secure all IT, information systems, networks, and data that support DOT operations. Moreover, in the wake of increased telework during the Coronavirus Disease 2019 (COVID–19) pandemic, the OCIO upgraded security and tripled departmental network bandwidth. These actions ensured that employees working from home could access systems and data to fulfill their responsibilities.

The Department's formal policies align with Federal guidelines—specifically, those for security controls for identifying and managing risks, protecting information systems, detecting potential cybersecurity incidents, and responding to and recovering from incidents. However, DOT does not implement them in a consistent or comprehensive manner. As a result, the Department faces the risk that its mission-critical systems could be compromised.

Since 2003, we have conducted annual reviews of DOT's information security programs and practices, in accordance with FISMA requirements. As we reported in our most recent FISMA audit,[6] the Department has yet to address longstanding cybersecurity deficiencies related to its practices for protecting its mission-critical systems from unauthorized access, alteration, or destruction. For example, we continue to note inconsistencies in DOT's implementation of its cybersecurity program (see table).

[4] DOT Order 1351.37, *Departmental Cybersecurity Policy*, July 14, 2017.

[5] Pub. L. No. 113–283 (December 18, 2014).

[6] *Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security System Program and Practices* (OIG Report No. QC2022006), October 25, 2021. OIG reports are available on our website: https://www.oig.dot.gov/.

Table. Weaknesses in DOT's Implementation of Its Cybersecurity Program

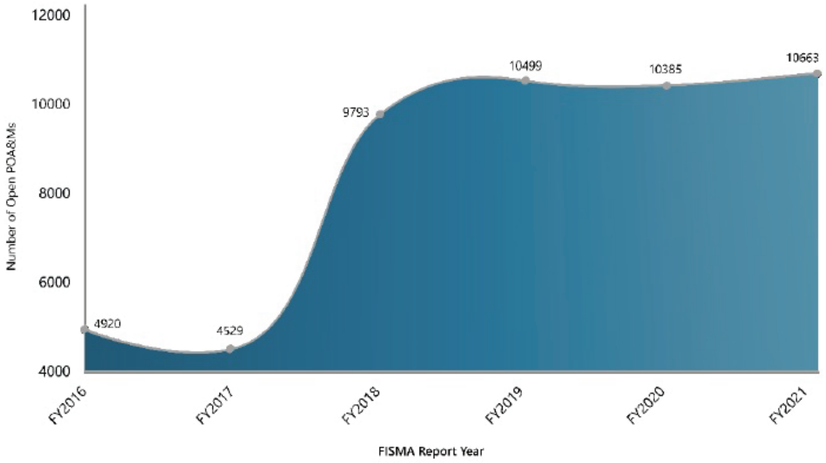
Category	Issues OIG Identified in 2021
Risk management	*Inventories*: DOT did not maintain accurate and complete inventories of all OA information systems and was unable to demonstrate that it had a formal process in place for ensuring the accuracy and completeness of the hardware asset inventories it reports to OMB—key prerequisites to an effective risk-management program.
	Security controls: DOT did not always test the security controls for its information systems or properly approve security assessment and authorization documentation.
	Tracking vulnerabilities: DOT did not always report, manage, and close security weaknesses identified in plans of action and milestones (POA&M).
	Supply chain risk management: DOT has not developed a supply chain risk management strategy and implementation plan to ensure that external providers comply with departmental cybersecurity requirements.
Protecting DOT's information systems from risk of compromise.	*Configuration management*: DOT has not consistently remediated vulnerabilities related to unsupported operating systems, unpatched applications, and configuration weaknesses, which may allow unauthorized access into mission-critical systems and data.
	Identity and access management: Employees and contractors do not always access the DOT network with personal identity verification (PIV) cards because many Department systems are not enabled to use PIV cards or do not require them.
	Data protection and privacy: DOT does not always review privacy documentation designed for the protection of PII each year; in some cases, the documentation is not current or has not been developed. This puts the PII stored in DOT's information systems at risk for compromise.
Detecting potential cybersecurity threats.	*Information security continuous monitoring*: DOT does not conduct annual security control assessments on some systems. As a result, it lacks an ongoing awareness of information security, vulnerabilities, and threats to systems and information.
Responding to cybersecurity incidents.	*Incident response*: DOT did not provide evidence that it evaluates the effectiveness of its incident response technologies or adjusts configurations and toolsets as appropriate, raising questions about the effectiveness of its automated detection capabilities. DOT's Security Operations Center also does not have file-integrity checking software for detecting signs of cyber incidents.
Recovering from cybersecurity incidents.	*Contingency plans*: DOT does not test all of its contingency plans on an annual basis; other plans have not been developed, reviewed, or updated in a timely manner. Comprehensive testing is crucial to ensure organizational systems and data are available and that IT systems and applications can function during outages.

Source: Independent auditor analysis

Many of these and other weaknesses can be attributed to the Department's lack of progress in addressing our 66 prior-year audit recommendations. DOT has struggled to remediate its security weaknesses in a timely manner and has yet to close 10,663 vulnerabilities associated with its information systems, as compared with the

10,385 weaknesses we found in 2020.[7] Figure 1 identifies the number of DOT plans of action and milestones (POA&M) that have remained open for the past 6 years.

Figure 1. Total Number of Open Departmentwide POA&Ms Since FY 2016



Source: OIG analysis of DOT data

Furthermore, as early as 2012, we identified high-risk security vulnerabilities—including inconsistent software updates—that an attacker could exploit to control systems or access files and data. Since 2013, DOT has not had a comprehensive and accurate inventory of its information systems and, as a result, may be unable to identify and address all system vulnerabilities. The Department has also not resolved our 2018 recommendation to develop and maintain accurate inventories of cloud systems, contractor systems, and websites that allow public access. The lack of accurate inventories of its hardware assets may be even more critical in light of the increased use of telework in response to COVID–19.

These vulnerabilities are compounded by the inconsistent enforcement of a Departmentwide information security program. For one, DOT has not had a permanent Chief Information Security Officer with the leadership authority to perform effective oversight and ensure accountability for departmental information security improvements for close to a year. Thus, it is challenging for DOT to move forward with a continuity of strategy that can affect long-term changes. To address these longstanding and recurring cybersecurity weaknesses, we made one overarching key recommendation to the Department this year: require the OCIO to develop a multiyear strategy and approach—complete with objective milestones and resource commitments—to implement the necessary corrective actions to ensure an effective information security program. To DOT's credit, it agreed with our recommendation and directed the CIO to develop and implement such an approach by December 2022.

Protecting IT Infrastructure and Sensitive Information at DOT Operating Administrations

Our recent audit work shows that DOT faces ongoing challenges protecting the IT infrastructure that its OAs manage and monitor. This infrastructure includes systems that are integral to the safe and efficient operation of our Nation's transportation system; help manage the disbursement of billions of dollars to grantees; and contain sensitive information, including PII.

Strengthening Security Controls for High-Impact Systems at FAA

The Department faces some of its most significant cybersecurity challenges at FAA, which owns 325—or about 75 percent—of DOT's 431 information technology systems. Specifically, FAA operates a vast network of systems and facilities for man-

[7] *Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security Program and Practices* (OIG Report No. QC2021003), October 26, 2020.

aging air traffic in the National Airspace System (NAS). This complex network has evolved over the years into an amalgam of diverse legacy radars and newer satellite-based systems for tracking aircraft, as well as a new initiative for controllers and pilots to share information through data link communications.

Recognizing the importance of protecting its infrastructure from rapidly evolving cyber-based threats, FAA recently re-categorized 45 low- and moderate-impact systems as high impact. According to the Federal Information Processing Standards,[8] a high-impact system is one in which a security breach or loss is expected to have a severe or catastrophically adverse effect on organizational operations, assets, or individuals. For example, one of the recently re-categorized systems is the En Route Automation Modernization system, which air traffic controllers rely on to manage high-altitude air traffic nationwide.

Re-categorizing a system as high impact creates more stringent security control requirements to safeguard the confidentiality, integrity, and availability of information processed or stored on the system. However, we recently reported that FAA lacks formalized policies and procedures for selecting and implementing high security controls for its high-impact systems.[9] As FAA's reliance on interconnectivity increases, so does the risk of cybersecurity breaches, which can have a significant impact on the NAS. To increase cybersecurity, FAA must complete its selection and implementation of all required high-security controls for these mission-critical systems.

Protecting FTA's Financial Management Systems

We recently reported [10] that FTA's financial management systems have several security control deficiencies that could affect the Agency's ability to approve, process, and disburse grant funds, including nearly $70 billion in COVID–19 relief appropriations. Security controls for FTA financial management systems are especially critical given that the transit industry is vulnerable to cyberattacks. For example, we reported that in 2020 and 2021, at least five FTA grant recipients were victims of cyberattacks that exposed PII, personnel data, and financial data. Grant recipients' security incidents may result in the compromise of usernames and credentials and expose FTA to cyberattacks that may delay the distribution of COVID–19 related funds to recipients.

Despite these risks, we found that FTA did not always effectively select, document, implement, and monitor the security controls for its financial management systems. For example, FTA security officials reported that 139 of 269 security controls were satisfied, but we found they were not tested or implemented as required. As a result of these and other issues, FTA officials may not have accurate pictures of security risks. Additionally, FTA has not remediated longstanding security control weaknesses that it has identified since 2016—including issues with multifactor authentication—which increases the risk that malicious actors could gain unauthorized access. Other weaknesses include unsecure databases, a lack of integrity monitoring tools, and insufficient contingency and incident response planning. If compromised, these weaknesses could lead to a cybersecurity attack.

Safeguarding PII by Preventing Cyberattacks at Multiple OAs

Several of our recent reviews have raised concerns regarding whether the OAs have the appropriate security controls in place to protect DOT's networks and information systems from unauthorized access, including insider threats. In our recent audits of the cybersecurity postures at the Volpe National Transportation Systems Center (Volpe), Maritime Administration (MARAD), and Federal Motor Carrier Safety Administration (FMCSA),[11] we identified and could have exploited security weaknesses and accessed millions of data records. As part of our vulnerability assessments and penetration testing, we were able to access to millions of sensitive records, including PII (see figure 2).

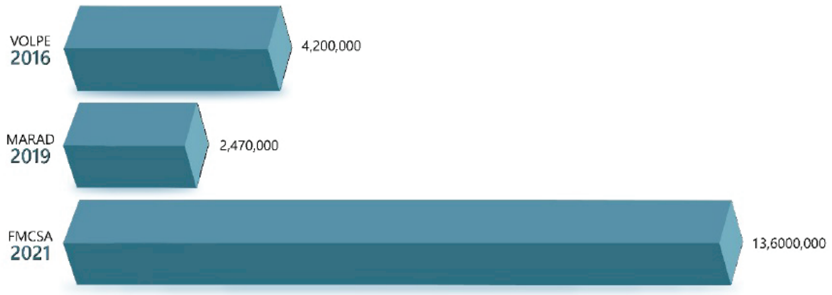
[8] Federal Information Processing Standards Publication 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

[9] *FAA Is Taking Steps to Properly Categorize High-Impact Information Systems but Security Risks Remain Until High Security Controls Are Implemented* (OIG Report No. IT2021033), August 2, 2021.

[10] *FTA Does Not Effectively Assess Security Controls or Remediate Cybersecurity Weaknesses To Ensure the Proper Safeguards Are in Place To Protect Its Financial Management Systems* (OIG Report No. IT2022005), October 20, 2021.

[11] *The Volpe Center's Information Technology Infrastructure Is at Risk for Compromise* (OIG Report No. FI2016056), March 22, 2016; *The Maritime Administration's Information Technology Infrastructure Is at Risk for Compromise* (OIG Report No. FI2019057), July 24, 2019; *FMCSA's IT Infrastructure Is at Risk of Compromise* (OIG Report No. IT2022003), October 20, 2021.

Figure 2. Number of Unauthorized PII Records That OIG Was Able To Access at Volpe, MARAD, and FMCSA



Source: Results of OIG audits of Volpe, MARAD, and FMCSA security postures conducted in 2016, 2019, and 2021, respectively.

For example, we successfully penetrated FMCSA's infrastructure and gained unauthorized access to 13 million PII records. If breached, these systems could have cost the Department millions of dollars in credit monitoring fees to protect affected individuals from identity theft. We also identified recurring weaknesses that we could exploit, including poor security practices, such as weak administrative-level login credentials, unpatched servers and workstations, and a lack of encryption of sensitive data.

Many of the weaknesses we found at FMCSA also tie into the same persistent enterprise-level security risks we found during our audits of MARAD and Volpe's IT networks and systems. These weaknesses are of particular concern given that these OAs' networks process, store, and transmit a substantial amount of sensitive information and are connected to DOT's overall network. Until the Department implements appropriate safeguards and countermeasures to protect its networks, DOT and its OAs will continue to be at risk for an enterprise-wide cybersecurity attack that could have a major impact on mission-critical systems. We plan to continue to review the IT infrastructure at individual OAs; our fourth audit in this series will focus on the Federal Highway Administration.

Coordinating With Other Agencies and Industry Partners To Ensure Cybersecurity in the Transportation Sector

As a lead agency in protecting the critical infrastructure of the Nation's transportation sector, DOT must partner effectively with other Federal agencies and industry to mitigate vulnerabilities and ensure cybersecurity. Both DHS and DOT have the authority and responsibility to protect the U.S. transportation sector from physical and cyber threats.[12] DOT also coordinates with other Federal agencies and industry partners. For example, the FAA Extension, Safety, and Security Act of 2016 directs FAA to develop a comprehensive, strategic framework to reduce cybersecurity risks to civil aviation. FAA's efforts to implement this framework involve coordinating and collaborating on aviation cybersecurity with DHS and the Department of Defense through the Aviation Cyber Initiative. Protecting flight-critical systems—and the safety of the flying public—from rapidly evolving cyber-based threats also requires the cooperation of aviation stakeholders from industry, airlines, airports, and manufacturers.

DOT's collaboration and coordination across the transportation sector is of critical importance because the incapacitation or destruction of transportation assets, systems, or networks would have a debilitating effect on the Nation's security, economy, and public health and safety. On May 8, 2021, for example, the Colonial Pipeline Company announced that it had halted its pipeline operations due to a ransomware attack, disrupting critical supplies of gasoline and other refined products throughout the East Coast. This incident and other cyberattacks have elevated concerns about the security of the Nation's critical infrastructure, including energy pipelines and the transportation sector.

Accordingly, we will monitor DOT's ongoing efforts to ensure cybersecurity in the transportation sector, particularly as it increasingly relies on private-sector partners

[12] See Executive Order 14028: Improving the Nation's Cybersecurity (May 12, 2021) and Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (February 12, 2013).

for internet-based computing services (commonly referred to as cloud services) to address IT needs. To that end, we have initiated a review of the Department's strategy to secure cloud services and transition toward zero trust architecture, key provisions of Executive Order 14028. As defined by NIST,[13] zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), rather than network location, which is no longer seen as the prime component of an entity's security posture. We will keep the committee updated on our progress in monitoring and assessing the Department's cybersecurity program, including its partnerships with the private sector and other agencies.

CONCLUSION

DOT's cybersecurity program is critical to protect its vast network of IT systems from malicious attacks and other breaches that pose a threat to the U.S. transportation system. In today's rapidly evolving cybersecurity landscape, and as the Nation embarks on a new journey to upgrade and improve its transportation infrastructure, DOT faces significant challenges in strengthening its systems while adapting to new and rising challenges and threats. We remain committed to supporting the Department's efforts as it works to remediate existing vulnerabilities and bolster DOT's overall cybersecurity posture. We will continue to update you on our work on these and related matters.

This concludes my prepared statement. I would be happy to address any questions from you or Members of the Committee at this time.

Mr. DeFAZIO. Thank you. Thank you, Mr. Dorsey.

And now, finally—this is ridiculous [referring to his laryngitis]—Mr. Nick Marinos.

Mr. MARINOS. Thank you, Chairman DeFazio, Ranking Member Graves, and members of the committee for inviting GAO to contribute to this important discussion about critical infrastructure cybersecurity.

As you know, our Nation's infrastructure increasingly relies on IT systems to carry out operations, and the protection of these systems is vital to public confidence and safety, and to national security.

GAO has long emphasized the urgent need for the Federal Government to improve its ability to protect against cyber threats to our Nation's infrastructure. In fact, we have designated cybersecurity as a Governmentwide, high-risk area since 1997. Our most recent high-risk updates to Congress emphasize the need for the Federal Government to address major cybersecurity challenges through 10 critical actions. Today I will focus on two of them.

The first is the need to develop and execute a comprehensive, national cyber strategy, and the second is the need to strengthen the Federal role in protecting critical infrastructure from cyber threats.

Over the last several decades, the Federal Government has struggled in establishing a national strategy to guide how we plan to engage both domestically and internationally on cyber-related issues. Last year, we reported that the prior administration's national cyber strategy needed improvements, and that it was unclear which official was ultimately responsible for coordinating the execution of the national strategy. We recommended that the National Security Council update the document, and that Congress consider passing legislation to designate a position in the White House to lead such an effort.

[13] NIST Special Publication 800–207, *Zero Trust Architecture*, August 2020. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or on asset ownership (enterprise or personally owned).

In January, we saw Congress pass a law that established the Office of the National Cyber Director within the Executive Office of the President. And in June, the Senate confirmed a Director to lead this new office. While this is an important step forward, until we see the executive branch establish a comprehensive strategy, our Government will continue to operate without a clear roadmap for how it intends to overcome the cyber threats facing the Nation.

We have also long reported that the Federal Government has been challenged in working with the private sector to protect our Nation's critical infrastructure from cyberattacks. Since 2010, we have made over 80 recommendations aimed at strengthening the role in critical infrastructure. This includes by enhancing the capabilities and services of DHS's Cybersecurity and Infrastructure Security Agency, known as CISA, and ensuring that Federal agencies with sector-specific responsibilities are providing their sector partners with the effective guidance and support they need. These include important corrective actions within the transportation sector, too, such as improving FAA's oversight of commercial airplane cybersecurity, and TSA's oversight of the cybersecurity of both critical pipeline and passenger rail systems.

Finally, I would like to highlight the urgency for Federal agencies to implement all of the cyber-related recommendations that have come out of the work performed by GAO and the inspectors general. Since 2010, GAO has made over 3,700 recommendations on cyber-related topics. Many of these recommendations extend far beyond topics related to critical infrastructure, but they represent work that is needed to elevate the entire Federal Government in its ability to tackle today's cyber problems, and to anticipate those we will face in the future.

For example, they deal with important workforce issues, such as our recommendation to the Department of Transportation that it assess its skill gaps in order to better oversee automated technologies like those that control planes, trains, or vehicles without human intervention.

They also call for improvements to Federal agencies' own protections, such as through our recommendations to DHS that it work with agencies, including FAA, to better implement cybersecurity tools that check for vulnerabilities and insecure configurations on agency networks.

Although agencies deserve credit for implementing many of our recommendations, over 900 still have yet to be implemented, including over 50 related to improving critical infrastructure cybersecurity. So clearly, there is a lot more work to do, and we think that agencies need to move with a greater sense of urgency to improve their cybersecurity protections.

In summary, in order for our Nation to overcome its ever-mounting and increasing array of cyber-related challenges, our Federal Government needs to do a better job of implementing strategy, oversight, and coordination among Federal agencies, and with the owners and operators that are on the front lines of this digital battle.

This concludes my remarks, and I look forward to answering any questions you may have. Thank you.

[Mr. Marinos's prepared statement follows:]

Prepared Statement of Nick Marinos, Director, Information Technology and Cybersecurity, U.S. Government Accountability Office

CYBERSECURITY: FEDERAL ACTIONS URGENTLY NEEDED TO BETTER PROTECT THE NATION'S CRITICAL INFRASTRUCTURE

Chairman DeFazio, Ranking Member Graves, and Members of the Committee:

Thank you for the opportunity to contribute to today's discussion on federal perspectives to secure the nation's infrastructure. As you know, our nation's critical infrastructure sectors are dependent on information technology (IT) systems and digital data to carry out operations and to process, maintain, and report essential information.[1] The security of these systems and data is vital to public confidence and national security, prosperity, and well-being.

We have long stressed the urgent need for effective cybersecurity, as underscored by increasingly sophisticated threats and frequent cyber incidents.[2] Recent events, including the ransomware attack that led to a shutdown of a major U.S. fuel pipeline, have illustrated that the nation's critical infrastructure and the federal government's IT systems continue to face growing cyber threats.[3] The cybersecurity of critical infrastructure sectors has been a long-standing challenge for the federal government, underscored by the need for federal agencies to improve their own cybersecurity posture and enhance the cybersecurity support provided to the nation's critical infrastructure.

At your request, my remarks today will focus on the federal government's efforts to address the cybersecurity of the nation's critical infrastructure and will highlight critical areas where we have identified an urgent need for improvement. This statement is based on the results of our prior work, which includes the reports and testimonies that we cite throughout this statement. To develop the statement, we reviewed prior reports and testimonies that described cyber-related challenges faced by the nation and the extent to which federal entities have taken actions to address them. More detailed information about our scope and methodology can be found in the products cited throughout this statement.

We conducted the work on which this statement is based in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions.

BACKGROUND

Information systems supporting federal agencies and our nation's critical infrastructure—such as transportation systems, communications, education, energy, and financial services—are inherently at risk. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems and networks used by federal agencies and our nation's critical infrastructure are also often interconnected with other internal and external systems and networks, including the internet.

[1] The term "critical infrastructure," as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, refers to systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e). Federal policies identify 16 critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2] See, for example, GAO, *Cybersecurity and Information Technology: Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas*, GAO–21–105325 (Washington, D.C.: July 28, 2021) and *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO–21–288 (Washington, D.C.: Mar. 24, 2021).

[3] For more information regarding such recent events, see GAO, *Cybersecurity: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks*, GAO–21–594T (Washington, D.C.: May 25, 2021). Ransomware is a type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.

With this greater connectivity, threat actors are increasingly willing and capable of conducting a cyberattack on our nation's critical infrastructure that could be disruptive and destructive. The *2021 Annual Threat Assessment of the U.S. Intelligence Community* and the *2020 Homeland Threat Assessment* noted that criminal groups and nations pose the greatest cyberattack threats to our nation.[4] According to the 2020 assessment, both criminal groups and nation cyber actors—motivated by profit, espionage, or disruption—will exploit the Coronavirus Disease 2019 (COVID–19) pandemic by targeting the U.S. health care and public health sector, government response entities, and the broader emergency services sector.

Recent events highlight the significant cyber threats facing the nation. For example,

- In May 7, 2021, the Colonial Pipeline Company learned that it was the victim of a cyberattack. A joint alert from the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) indicated that malicious actors used ransomware against Colonial Pipeline's information technology network.[5] The alert also explained that, to ensure the safety of the pipeline, the company disconnected certain industrial control systems that monitor and control physical pipeline functions so that they would not be compromised by the criminals. According to CISA and the FBI, as of May 11, 2021, there was no indication that the threat actors had compromised the industrial control systems. However, disconnecting these systems resulted in a temporary halt to all pipeline operations. This, in turn, led to gasoline shortages throughout the southeast United States.
- In February 2021, CISA issued an alert explaining that cyber threat actors obtained unauthorized access to a U.S. water treatment facility's industrial controls systems and attempted to increase the amount of a caustic chemical that is used as part of the water treatment process. According to CISA, threat actors likely accessed systems by exploiting cybersecurity weakness, including poor password security and an outdated operating system.
- In December 2020, CISA issued an emergency directive and alert explaining that an advanced persistent threat actor had compromised the supply chain of a network management software suite and inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a genuine version of that software product. The malicious actor then used this backdoor, among other techniques, to initiate a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations.

GAO Has Previously Identified Four Major Cybersecurity Challenges Facing the Nation

To underscore the importance of this issue, we have designated information security as a government-wide high-risk area since 1997.[6] In 2003, we added the protection of critical infrastructure to the information security high-risk area, and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.[7]

In our high-risk updates from September 2018 and March 2021, we emphasized the critical need for the federal government to take 10 specific actions to address four major cybersecurity challenges that the federal government faces.[8] These challenges are: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. Figure 1 provides an overview of the critical actions needed to address these major cybersecurity challenges.

[4] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (April 9, 2021). Department of Homeland Security, *Homeland Threat Assessment* (October 6, 2020).

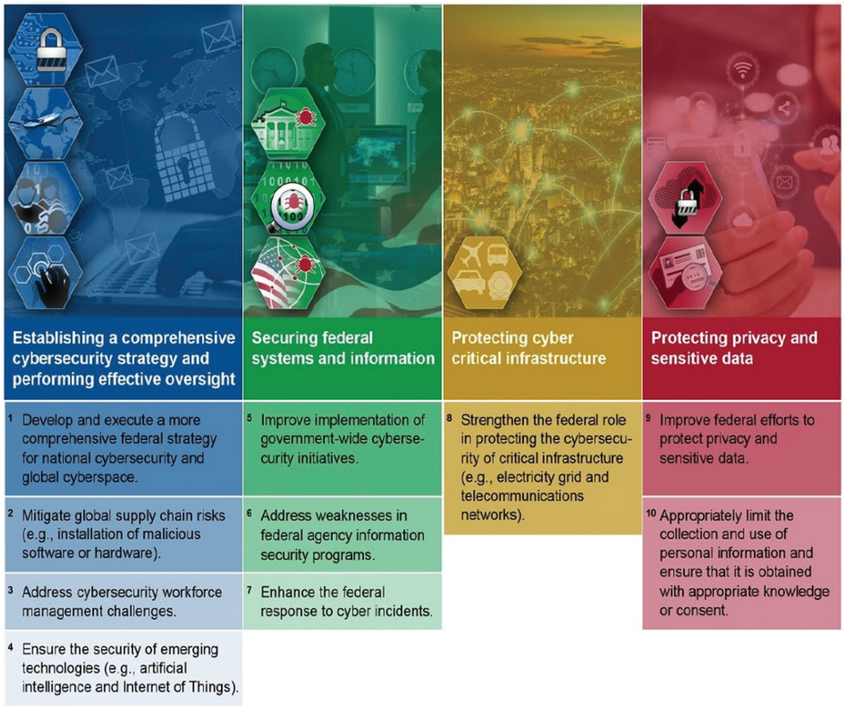
[5] CISA and the FBI, *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, Alert (AA21–131A), May 11, 2021.

[6] GAO, *High-Risk Series: Information Management and Technology*, HR–97–9 (Washington, D.C.: Feb. 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high-risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[7] GAO, *High-Risk Series: An Update*, GAO–15–290 (Washington, D.C.: Feb. 11, 2015) and *High-Risk Series: An Update*, GAO–03–119 (Washington, D.C.: Jan. 2003).

[8] GAO–21–288 and GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO–18–622 (Washington, D.C.: Sept. 6, 2018).

Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Establishing a comprehensive cybersecurity strategy and performing effective oversight

1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).

3 Address cybersecurity workforce management challenges.

4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

5 Improve implementation of government-wide cybersecurity initiatives.

6 Address weaknesses in federal agency information security programs.

7 Enhance the federal response to cyber incidents.

Protecting cyber critical infrastructure

8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

Protecting privacy and sensitive data

9 Improve federal efforts to protect privacy and sensitive data.

10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. GAO–22–105530

Since 2010, we have made about 3,700 recommendations related to our high-risk area focused on enhancing our nation's cybersecurity efforts. As of November 2021, about 900 of those recommendations had yet to be implemented.

As indicated by the figure above, these recommendations include but also extend far beyond topics related to critical infrastructure cybersecurity, representing work across all of the high-risk challenge areas and calling for urgent actions to help address them. The following examples reflect the wide range of challenge areas:

- *Cybersecurity workforce management*. In December 2020, we reported that the U.S. Department of Transportation's (DOT) workforce faced challenges related to overseeing the safety of automated technologies, such as those that control a function or task of a plane, train, or vehicle without human intervention.[9] These technologies require regulatory expertise as well as engineering, data analysis, and cybersecurity skills. Although DOT had identified most skills it needed to oversee automated technologies, it had not fully assessed whether its workforce had these skills. Accordingly, we recommended that DOT (1) assess skill gaps in key occupations involved in overseeing automated technologies and (2) regularly measure the progress of strategies implemented to close skill gaps. As of November 2021, these recommendations had not yet been fully implemented, although DOT reported it intended to so by June 2022.
- *Government-wide cybersecurity initiatives*. Federal agencies face cyber threats against that continue to grow in number and sophistication. The Continuous Diagnostics and Mitigation (CDM) program was established to provide federal agencies with tools and services that have the intended capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. In August 2020, we reported that selected agencies—the Federal Aviation Adminis-

[9] GAO, *Automated Technologies: DOT Should Take Steps to Ensure Its Workforce Has Skills Needed to Oversee Safety*, GAO–21–197 (Washington, D.C.: Dec. 18, 2020).

tration (FAA), Indian Health Services, and Small Business Administration—had generally deployed these tools intended to provide cybersecurity data to support the Department of Homeland Security's (DHS) CDM program.[10] However, while agencies reported that the program improved their network awareness, none of the three agencies had effectively implemented all key CDM program requirements. As part of our review, we made six recommendations to DHS and nine recommendations to the three selected agencies. DHS and the selected agencies concurred with the recommendations. As of November 2021, only one of the recommendations made to DHS had been implemented.

- *Federal agency cybersecurity risk management*. In July 2019, we reported on key practices for establishing an agency-wide cybersecurity risk management program that include designating a cybersecurity risk executive, developing a risk management strategy and policies to facilitate risk-based decisions, assessing cyber risks to the agency, and establishing coordination with the agency's enterprise risk management program.[11] Although the 23 agencies we reviewed almost always designated a risk executive, they often did not fully incorporate other key practices in their programs, such as (1) establishing a cybersecurity risk management strategy to delineate boundaries for risk-based decisions; (2) establishing a process for assessing agency-wide cybersecurity risks; and (3) establishing a process for coordinating between cybersecurity and enterprise risk management programs for managing all major risks.[12] We made 57 recommendations to the 23 agencies to address the challenges identified in our report. As of November 2021, 25 of these recommendations had yet to be implemented.

Federal Law and Policy Establish Requirements for Critical Infrastructure Cybersecurity

Federal law and policy establish roles and responsibilities for the protection of critical infrastructure, discussed in chronological order.

- *Executive Order 13636*. In February 2013, the White House issued *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, which called for a partnership with the owners and operators of critical infrastructure to improve cybersecurity-related information sharing.[13] To do so, the order established mechanisms for promoting engagement between federal and private organizations. Among other things, the order designated nine federal sector-specific agencies with lead roles in protecting critical infrastructure sectors. The lead agencies coordinate federally sponsored activities within their respective sectors. Further, the order directed DHS, with help from the lead agencies, to identify, annually review, and update a list of critical infrastructure sectors for which a cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or national security.
- *Presidential Policy Directive 21*. Also, in February 2013, the White House issued Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, to further specify critical infrastructure responsibilities.[14] Among other things, the policy directed DHS to coordinate with lead agencies to develop a description of functional relationships across the federal government related to critical infrastructure security and resilience. The policy further prescribed DHS, in coordination with lead agencies, to conduct an analysis and recommend options for improving public-private partnership effectiveness.
- *National Institute of Standards and Technology (NIST) Cybersecurity Framework*. Executive Order 13636 directed NIST to lead the development of a flexible performance-based cybersecurity framework that was to include a set of

[10] GAO, *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO–20–598 (Washington, D.C.: Aug. 18, 2020).

[11] GAO, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO–19–384 (Washington, D.C.: July 25, 2019).

[12] The 23 civilian CFO Act agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development. There are 24 CFO Act agencies. We did not include the Department of Defense because our scope was the civilian agencies.

[13] The White House, *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636 (Washington, D.C.: Feb. 12, 2013), 78 Fed. Reg. 11739 (Feb. 19, 2013).

[14] The White House, *Presidential Policy Directive/PPD–21: Critical Infrastructure Security and Resilience*, (Washington, D.C.: Feb. 12, 2013).

standards, procedures, and processes.[15] Further, the order directed the lead agencies, in consultation with DHS and other interested agencies, to coordinate with critical infrastructure partners to review the cybersecurity framework. The agencies, if necessary, should develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

In response to the order, in February 2014, NIST first published its framework—a voluntary, flexible, performance-based framework of cybersecurity standards and procedures. The framework, which was updated in April 2018, outlines a risk-based approach to managing cybersecurity that is composed of three major parts: a framework core, profiles, and implementation tiers.[16] The framework core provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes.

- *Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018*. The November 2018 act established CISA,[17] within DHS, to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructure in the face of both physical and cyber threats. To implement this legislation, CISA undertook a three-phase organizational transformation initiative aimed at unifying the agency, improving mission effectiveness, and enhancing the workplace experience for CISA employees.
- *National Defense Authorization Act (NDAA) for Fiscal Year 2021*. The act established roles and responsibilities for lead agencies, known as sector risk management agencies, in protecting the 16 critical infrastructure agencies.[18] According to the act, the lead agencies are required to (1) coordinate with DHS and collaborate with critical infrastructure owners and operators, regulatory agencies, and others; (2) support sector risk management, in coordination with CISA; (3) assess sector risk, in coordination with CISA; (4) coordinate the sector, including by serving as a day-to-day federal interface for the prioritization and coordination of sector-specific activities; and (5) support incident management, including supporting CISA, upon request, in asset response activities.

Federal Actions Urgently Needed to Protect Critical Infrastructure from Cyber Threats

Over the last several decades, we have emphasized the urgent need for the federal government to improve its ability to protect against cyber threats to our nation's infrastructure. In recent high-risk updates, we emphasized the critical need for the federal government to address major cybersecurity challenges through critical actions. This includes the need for the federal government to (1) develop and execute a comprehensive national cyber strategy and (2) strengthen the federal role in protecting the cybersecurity of critical infrastructure.

Executive Branch Urgently Needs to Establish and Implement a Comprehensive National Cyber Strategy

We and others have reported on the challenges in establishing a comprehensive national strategy to guide how the United States government will engage both domestically and internationally on cybersecurity related matters. In September 2020, we reported that the prior administration's 2018 *National Cyber Strategy*[19] and associated 2019 *Implementation Plan* had collectively detailed the executive branch's approach to managing the nation's cybersecurity. However, these documents only addressed some, but not all, of the desirable characteristics of national strategies,

[15] The Cybersecurity Enhancement Act of 2014 authorized NIST to facilitate and support the development of a voluntary set of standards to reduce cyber risks to critical infrastructure. 15 U.S.C. § 272(c)(15). *The Framework for Improving Critical Infrastructure Cybersecurity* represents that voluntary set of standards.

[16] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Washington, D.C.: April 2018).

[17] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, 132 Stat. 4168, 4169, (Nov. 16, 2018) (codified at 6 U.S.C. §652). The act renamed the DHS National Protection and Programs Directorate as CISA.

[18] The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 states that the term "sector risk management agency" replaces the term "sector-specific agency" in the Homeland Security Act of 2002. The NDAA amends the Homeland Security Act of 2002 and sets out sector risk management agency responsibilities within this critical infrastructure framework. Pub. L. No. 116–283, § 9002, 134 Stat. 3388, 4768 (Jan. 1, 2021).

[19] The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018).

such as goals and resources needed.[20] Accordingly, we recommended that the National Security Council work with relevant federal entities to update cybersecurity strategy documents to include goals and resource information, among other things.[21] The National Security Council staff neither agreed nor disagreed with our recommendation and has yet to address it.

We have also stressed the urgency and necessity of clearly defining a central leadership role in order to coordinate the government's efforts to overcome the nation's cyber-related threats and challenges. In September 2020, we also reported that, in light of the elimination of the White House Cybersecurity Coordinator position in May 2018, it was unclear which official within the executive branch ultimately maintained responsibility for coordinating the execution of the National Cyber Strategy and related implementation plan. Accordingly, we suggested that Congress consider legislation to designate a position in the White House to lead such an effort. In January 2021, the NDAA for Fiscal Year 2021 established the Office of the National Cyber Director within the Executive Office of the President.[22] Among other responsibilities, the Director is to serve as the principal advisor to the White House on cybersecurity policy and strategy, including coordination of implementation of national cyber policy and strategy.

In June 2021, the Senate confirmed a Director to lead this new office. In October 2021, the National Cyber Director issued a strategic intent statement, outlining a vision for the Director's office and the high-level lines of efforts it intends to focus on, including national and federal cybersecurity; budget review and assessment; and planning and incident response, among others.[23]

The establishment of a National Cyber Director is an important step toward positioning the federal government to better direct activities to overcome the nation's cyber threats and challenges and to perform effective oversight. Nevertheless, the implementation of our recommendation to fully develop and execute a comprehensive national cyber strategy remains more urgent than ever to ensure that there is a clear roadmap for overcoming the cyber challenges facing our nation, including its critical infrastructure.

Federal Government Needs to Strengthen Its Role in Protecting the Cybersecurity of Critical Infrastructure

The federal government has been challenged in working with the private sector to protect cyber critical infrastructure. We have made recommendations aimed at strengthening the federal role in critical infrastructure cybersecurity, including by (1) enhancing the capabilities and services of DHS' Cybersecurity and Infrastructure Security Agency and (2) ensuring that federal agencies with sector-specific responsibilities are providing their sector partners with effective guidance and support.

DHS Needs to Complete CISA Transformation Activities to Better Support Critical Infrastructure Owners and Operators

The importance of clear cybersecurity leadership extends beyond the White House to other key executive branch agencies, including DHS. Federal legislation enacted in November 2018 established CISA within the department to advance the mission of protecting federal civilian agencies' networks from cyber threats and to enhance the security of the nation's critical infrastructure in the face of both physical and cyber threats. The act elevated CISA to agency status; prescribed changes to its structure, including mandating that it have separate divisions on cybersecurity, infrastructure security, and emergency communications; and assigned specific responsibilities to the agency.[24]

To implement the statutory requirements, CISA leadership launched an organizational transformation initiative. In March 2021, we reported that while CISA had completed the first two of the three phases of its organizational transformation ini-

[20] GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO–20–629 (Washington, D.C.: Sept. 22, 2020).

[21] The *National Cyber Strategy* assigns National Security Council staff to coordinate with departments, agencies, and the Office of Management and Budget on a plan to implement the strategy.

[22] Pub. L. No. 116–283, Div. A, Title XVII, § 1752, 134 Stat. 4144 (Jan. 1, 2021) (codified at 6 U.S.C. § 1500).

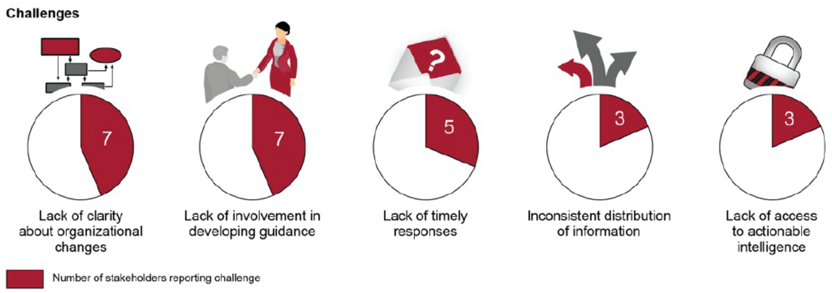
[23] The White House, *A Strategic Intent Statement for the Office of the National Cyber Director* (Washington, D.C.: Oct. 28, 2021).

[24] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278, § 2,132 Stat. 4168, 4169, (Nov. 16, 2018)(codified at 6 U.S.C. §652). The act renamed the DHS National Protection and Programs Directorate as CISA.

tiative.[25] Specifically, we noted DHS had not fully implemented its phase three transformation, which included finalizing the agency's mission-essential functions and completing workforce-planning activities, that was intended to be completed by December 2020.

We also reported that of 10 selected key practices for effective agency reforms we previously identified, CISA's organizational transformation generally addressed four, partially addressed five, and did not address one. Further, we reported on a number of challenges that selected government and private-sector stakeholders had noted when coordinating with CISA, including a lack of clarity surrounding its organizational changes and the lack of stakeholder involvement in developing guidance. Although CISA had activities under way to mitigate some of these challenges, it had not developed strategies to, among other things, clarify changes to its organizational structure. Figure 2 below describes the coordination challenges identified by private-sector stakeholders.

Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Coordination Challenges Reported by Stakeholders Representing the 16 Critical Infrastructure Sectors



Source: GAO analysis of stakeholder interviews. GAO–22–105530

To address these weaknesses, we made 11 recommendations to DHS. The department concurred with our recommendations and, as of September 2021, reported that it intends to fully implement them by the end of calendar year 2022. Implementing these recommendations will better position CISA to ensure the success of its reorganization efforts and carry out its mission to lead national efforts to identify and respond to cyber and other risks to our nation's infrastructure.

Sector Risk Management Agencies Need to Ensure Effective Guidance and Support of Critical Infrastructure Owners and Operators

Since 2010, we have made about 80 recommendations for various federal agencies to enhance infrastructure cybersecurity. For example, in February 2020, we recommended that agencies better measure the adoption of the NIST framework of voluntary cyber standards and correct sector-specific weaknesses. Specifically, we reported that most sector lead agencies—known as sector risk management agencies[26]—were not collecting and reporting on improvements in the protection of critical infrastructure as a result of using the framework across the sectors.[27] We concluded that collecting and reporting on these improvements would help the sectors understand the extent to which sectors are better protecting their critical infrastructure from cyber threats.

To address these issues, we made 10 recommendations—one to NIST on establishing time frames for completing selected programs—and nine to the lead agencies, to collect and report on improvements gained from using the framework. Eight agencies agreed with the recommendations, while one neither agreed nor disagreed

[25] GAO, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, GAO–21–236 (Washington, D.C.: Mar. 10, 2021).

[26] Sector-specific agencies was a term formally used to describe the nine agencies that have a lead role in protecting the 16 critical infrastructure sectors. Pursuant to the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116–283, § 9002, any reference to sector-specific agencies in any law, regulation, document, or other paper of the United States shall be deemed a reference to the sector risk management agency of the relevant critical infrastructure sector.

[27] GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO–20–299 (Washington, D.C.: Apr. 9, 2020).

and one partially agreed. However, as of November 2021, none of the recommendations had been implemented. Until the lead agencies collect and report on improvements gained from adopting the framework, the extent to which the 16 critical infrastructure sectors are better protecting their critical infrastructure from threats will be largely unknown.

We have also frequently reported on the need for lead agencies to enhance the cybersecurity of their related critical infrastructure sectors and subsectors—such as transportation systems, communications, energy, education, and financial services.[28]

- *Aviation*.[29] The Federal Aviation Administration (FAA) is responsible for overseeing the safety of commercial aviation, including avionics systems. The growing connectivity between airplanes and these systems may present increasing opportunities for cyberattacks on commercial planes. In October 2020, we reported that FAA had established a process for certification and oversight of U.S. commercial airplanes, including their operations.[30] However, FAA had not prioritized risk-based cybersecurity oversight or included periodic testing as part of its monitoring process, among other things. To address these and other related issues, we made six recommendations to FAA; however, as of November 2021, the agency had not implemented the recommendations.
- *Mass Transit and Passenger Rail*.[31] Recent physical and cyberattacks on rail systems in U.S. and foreign cities highlight the importance of strengthening and securing passenger rail systems around the world. TSA is the primary federal agency responsible for securing transportation in the United States. To assess risk elements for physical and cyber security in passenger rail, TSA utilizes various risk assessments, including, among other things, the Baseline Assessment for Security Enhancement (BASE).[32] TSA uses these risk assessments to evaluate threat, vulnerability, and consequence for attack scenarios across various transportation modes. In April 2020, we reported[33] that while TSA had taken initial steps to share cybersecurity key practices and other information with passenger rail stakeholders, the BASE assessment did not fully reflect the updated cybersecurity key practices presented in NIST's Cybersecurity Framework,[34] nor did it include the framework in a list of available cyber resources.[35] Our review of the BASE cybersecurity questions in the template found that they covered selected activities associated with three of the five functions outlined in the framework—Identify, Protect, and Respond. However, the remaining two functions—Detect and Recover—were not represented in the BASE. We made two recommendations to TSA, including that the agency update the BASE cybersecurity questions to ensure they reflect key practices. DHS agreed with our recommendations. As of November 2021, one recommendation had not been implemented.
- *Pipeline Systems*.[36] The nation depends on the interstate pipeline system to deliver critical resources such as oil and natural gas. This increasingly computerized system is an attractive target for hackers and terrorists. In December 2018, we found weaknesses in the Transportation Security Administration's (TSA)

[28] GAO–21–288.

[29] The transportation systems sector consists of seven key subsectors, including aviation.

[30] GAO, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, GAO–21–86 (Washington, D.C.: Oct. 9, 2020).

[31] The transportation systems sector consists of seven key subsectors, including mass transit and passenger rail.

[32] The BASE is a voluntary security assessment of national mass transit, passenger rail, and highway systems conducted by TSA surface transportation inspectors that addresses potential vulnerabilities, among other things. The BASE is a nonregulatory security assessment, which requires surface transportation entities' voluntary participation. It consists of an assessment template with 17 security action items developed by TSA and the Federal Transit Administration that address, among other best practices, security training programs, risk information sharing, and cybersecurity. TSA developed this assessment in 2006 to increase domain awareness, enhance prevention and protection capabilities, and further response preparedness of passenger transit systems nationwide.

[33] GAO, *Passenger Rail Security: TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices*, GAO–20–404 (Washington, D.C.: Apr. 3, 2020).

[34] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*.

[35] For example, TSA has shared cybersecurity information through American Public Transportation Association working groups, through training exercises such as the Intermodal Security Training and Exercise Program, and through regional cybersecurity workshops promoting the NIST Cybersecurity Framework. TSA further shares cybersecurity key practices through questions in the BASE.

[36] The transportation systems sector consists of seven key subsectors, including pipeline systems.

management of its pipeline security efforts.[37] We reported that TSA, a component agency of DHS, had issued revised pipeline security guidelines; however, the revisions did not include all elements from the NIST Cybersecurity Framework and did not include clear definitions to ensure the identification of critical facilities by pipeline operators.[38] We also reported that the agency had conducted pipeline security reviews to assess pipeline systems vulnerabilities; however, the quantity of TSA's reviews of corporate and critical facilities security had varied considerably. To address these and other issues we made 10 recommendations to TSA. The agency agreed with all of our recommendations. In July 2021, we testified that the TSA had not fully addressed pipeline cybersecurity-related weaknesses that GAO had previously identified, such as aged protocols for responding to pipeline security incidents.[39] As of November 2021, TSA had implemented 10 of the 13 recommendations from 2018 and 2019 and had not implemented three.

- *Communications*. The Communications sector is an integral component of the U.S. economy and faces serious cyber-related threats that could affect the operations of local, regional, and national level networks. In November 2021, we reported that CISA has a leadership role in coordinating federal efforts intended to aid in the resilience of the Communications Sector.[40] The agency fulfills its responsibilities to private sector owners and operators through a variety of programs and services, including incident management and information sharing. We found CISA had not assessed the effectiveness of these activities, nor updated a strategic sector guidance document, despite being recommended by DHS to do so every 4 years. Specifically, the current plan, from 2015, lacks information on new and emerging threats to the Communications Sector, such as security threats to the communications technology supply chain. Developing and issuing updated guidance would enable CISA to set goals, objectives, and priorities that address threats and risks to the sector, and help meet its sector risk management agency responsibilities. As such, we made three recommendations to CISA, including that the agency assess the effectiveness of support provided to sector, and revise the sector plan to include, among other things, new and emerging threats and risks. DHS concurred with the recommendations and described initial actions under way or planned to address them in a 2021 letter in response to our report.
- *Energy*. The U.S. grid's distributing systems—which carry electricity from transmission systems to consumers and are regulated primarily by states—are increasingly at risk from cyberattacks. In August 2019, we reported that the electric grid faced various cybersecurity risks.[41] We noted that the Department of Energy (DOE) had developed plans and an assessment to address the risks. However, these documents did not fully address all of the key characteristics of a national strategy. Subsequently, in March 2021, we reported that the electric grid's distribution systems continued to face various cybersecurity risks.[42] DOE had developed plans and an assessment to address the risks to the electric grid; however, these documents did not fully address risks to the grid's distribution systems. To mitigate this issue, we recommended that the department more fully address cyber risks to the grid's distribution systems in its plans to implement the national cybersecurity strategy for the grid. DOE agreed with our recommendation; however, as of November 2021, the department had not implemented our recommendation.
- *Education*. When the COVID–19 pandemic forced the closure of schools across the nation, many kindergarten through grade 12 (K–12) schools moved from in-person to remote education, increasing their dependence on IT and making them potentially more vulnerable to cyberattacks. In October 2021, we reported that the Department of Education's sector-specific plan for the Education Facilities subsector had not been updated since 2010 and did not reflect substantially

[37] GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO–19–48 (Washington, D.C.: Dec. 18, 2018).

[38] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Gaithersburg, MD: Feb. 12, 2014).

[39] GAO, *Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses*, GAO–21–105263 (Washington, D.C.: July 27, 2021).

[40] GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector*, GAO–20–104462 (Washington, D.C.: Nov. 23, 2021).

[41] GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO–19–332 (Washington, D.C.: Aug. 26, 2019).

[42] GAO, *Electric Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO–21–81 (Washington, D.C.: Mar. 18, 2021).

changed cybersecurity risks affecting K–12 schools.[43] Further, Education had not determined whether sector-specific guidance was needed for K–12 schools to help protect against cyber threats, including against the increasing threat of ransomware attacks. To address these issues, we recommended that Education initiate a meeting with CISA to determine how to update its sector-specific plan and determine whether sector-specific guidance is needed. Education concurred with GAO's recommendations and described actions that it would take to address them.

- *Financial Services*. The federal government has long identified the financial services sector as a critical component of the nation's infrastructure. In September 2020, we reported that the Department of the Treasury and other federal agencies were taking steps to reduce risks and bolster the financial sector's efforts to improve its cybersecurity.[44] However, Treasury had not worked with other federal agencies and sector partners to better measure progress and to prioritize efforts in line with sector cybersecurity goals laid out in the implementation plan of the 2018 National Cyber Strategy. To address these issues, we made two recommendations to Treasury. The department agreed with our recommendations; however, as of November 2021, Treasury had not implemented the recommendations.

Overall, federal agencies have not addressed most of our recommendations related to protecting critical infrastructure.[45] About 50 of the about 80 recommendations made in our public reports since 2010 have not been implemented, as of November 2021. We also designated 14 of these as priority recommendations; as of November 2021, 11 had not been implemented. Until our recommendations are fully addressed, federal agencies will not be effectively positioned to ensure critical infrastructure sectors are adequately protected from potentially harmful cybersecurity threats.

In summary, the federal government needs to move with a greater sense of urgency in response to the serious cybersecurity threats faced by the nation and its critical infrastructure. This would include developing and executing a comprehensive national strategy and strengthening the federal role in protecting the cybersecurity of critical infrastructure. Without implementing our recommendations, the federal government will continue to be hindered in its ability to provide effective support to the cybersecurity of the nation's critical infrastructure. As a result, the risk of unprotected infrastructure being harmed is heightened.

Chairman DeFazio, Ranking Member Graves, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

Mr. DEFAZIO. Thank you for your testimony. I will try and squeak out a couple of questions here.

Mr. Grossman, what are—briefly—let's say, the top three cybersecurity challenges at the FAA?

And what are you doing to quickly implement measures to mitigate this?

Mr. GROSSMAN. Thank you for your question, Chairman DeFazio.

The FAA operates a large, complex infrastructure of interconnected networks and services. We have many service providers. Connectivity includes satellite-based communications, automated communications between aircraft, et cetera. The system has become very, very complex.

Most of our challenges really are around the purpose-built, legacy nav systems that are in operation today. These systems are operated 24/7/365, they require extensive testing, and operate custom-built software. Really, they don't allow remote patching capabilities. So, keeping up with the cyber hygiene component is a fairly large challenge from an FAA air traffic control perspective.

[43] GAO, *Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K–12 Schools from Cyber Threats*, GAO–22–105024 (Washington, D.C.: Oct. 13, 2021).

[44] GAO, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO–20–631 (Washington, D.C.: Sept. 17, 2020).

[45] GAO–21–288.

We protect that system, though, through compensating controls, meaning that network, while it is very difficult to patch and update, is very difficult to attach to, as well. It doesn't have internet access. There is a very mature access control list. In other words, system A can only speak to system B over very specific ports, with very specific protocols, and everything else is not addressed.

Additionally, we——

Mr. DEFAZIO. One more——

Mr. GROSSMAN. OK, sir.

Mr. DEFAZIO. Mr. Dorsey, you were pretty critical, I thought. Do you agree with Mr. Grossman's assessment on the top challenges, and why do you think they aren't yet rectified?

Mr. DORSEY. Thank you for your question, Chairman DeFazio.

I think the three key top challenges for the Department are: to solidify leadership at the chief information security officer level to provide the needed leadership, oversight, and accountability necessary for agencywide improvements to address ongoing information security weaknesses; two, I think the Department needs to develop a comprehensive, DOT-wide cybersecurity strategy to address recurring weaknesses; and three, they need to better protect and secure its IT infrastructure and sensitive information from potential compromises.

Those are the three key areas I believe that the Department needs to focus on to address the weaknesses that we have identified over the last 10 years.

Mr. DEFAZIO. So, Mr. Grossman, are those things in progress?

Mr. GROSSMAN. Well, I am the chief information security officer for the FAA, so there is leadership within FAA, and we are working with the OIG to close these audit recommendations.

We believe that we have protections in place. While many of the compliance-type audits have a lot of findings, the actual vulnerabilities are, in our opinion, most of them are mitigated through compensating controls.

Mr. DEFAZIO. OK, all right.

Mr. DORSEY. Sir——

Mr. DEFAZIO. I have exhausted my time——

Mr. DORSEY. Sir?

Mr. DEFAZIO. OK, briefly.

Mr. DORSEY. Sir, when I was speaking——

Mr. DEFAZIO. Sure.

Mr. DORSEY. Sir, when I was speaking of the chief information officer, chief information security officer, I was speaking about at the Department level. They are responsible for providing oversight of all of the OAs, including FAA. Thank you.

Mr. DEFAZIO. So, you are saying at DOT, [inaudible] FAA and other agencies?

Mr. DORSEY. Yes, sir. Thank you.

Mr. DEFAZIO. And there is no one in that position right now?

Mr. DORSEY. There is no permanent chief information security officer at the Department level at this time.

Mr. DEFAZIO. OK.

Mr. DORSEY. When we were conducting our reviews last year, there was a—he was serving as the acting chief information security officer.

Mr. DEFAZIO. OK, all right. Well, thank you. I am going to yield now to Ranking Member Graves, because he can ask questions better with a voice than I can. Thank you.

Mr. CRAWFORD. All right, thank you, Mr. Chairman.

As a committee, we continue to hear conflicting reports from TSA and pipeline industry stakeholders regarding the process and engagements throughout the issuance of two TSA security directives.

Furthermore, myself and Ranking Member Graves, as well as Senate Committee on Homeland Security and Governmental Affairs Ranking Member Portman, sent letters to DHS OIG to review the process in which TSA and CISA drafted the directives, which I ask unanimous consent to be entered into the record, Mr. Chairman.

Mr. DEFAZIO. Without objection.

[The information follows:]

Letter of November 12, 2021, to Hon. Joseph V. Cuffari, Inspector General, Department of Homeland Security, from Hon. Sam Graves, Ranking Member, Committee on Transportation and Infrastructure and Hon. Eric A. "Rick" Crawford, Ranking Member, Subcommittee on Railroads, Pipelines, and Hazardous Materials, Submitted for the Record by Hon. Eric A. "Rick" Crawford

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
U.S. HOUSE OF REPRESENTATIVES,
WASHINGTON, DC 20515,
November 12, 2021.

The Honorable JOSEPH V. CUFFARI,
Inspector General,
Department of Homeland Security, Office of the Inspector General, Washington, DC 20528–0305.

DEAR INSPECTOR GENERAL CUFFARI:

We write to request a review of the Transportation Security Agency's (TSA's) use of emergency security directives in coordination with the Cybersecurity and Infrastructure Security Agency (CISA) for the transportation and infrastructure sectors.

On May 27, 2021, TSA Administrator David Pekoske exercised emergency authority following the Colonial Pipeline ransomware attack and issued a security directive mandating certain pipeline operators to take actions to strengthen their cybersecurity measures.[1] On July 20, 2021, TSA issued a second pipeline-focused security directive outlining further mandatory steps required of pipeline operators.[2] Unfortunately, we have learned that these security directives were likely established with little communication or input from relevant stakeholders, would require burdensome reporting, and their prescriptive requirements could potentially interfere with safe pipeline operations and existing cybersecurity measures.[3] On August 24, 2021, several associations representing pipeline operators affected by the new security directives wrote to TSA outlining these concerns with the directives and urged TSA to share threat information so operators can better defend against potential cyber threats.[4]

In addition to the security directives for pipeline operators, on October 6, 2021, Department of Homeland Security (DHS) Administrator Alejandro Mayorkas an-

[1] Press Release, DHS, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021), *available at* https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[2] Press Release, DHS, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (Jul. 20, 2021), *available at* https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[3] Aaron Schaffer and Ellen Nakashima, *New emergency cyber regulations lay out 'urgently needed' rules for pipelines but draw mixed reviews*, WASH. POST, (Oct. 3, 2021), available at https://www.washingtonpost.com/national-security/cybersecurity-energy-pipelines-ransomware/2021/10/03/6df9cab2-2157-11ec-8200-5e3fd4c49f5e_story.html.

[4] Letter from Pipeline Trade Associations to TSA Administrator David P. Pekoske (Aug. 24, 2021) (on file with Committee).

nounced TSA would issue additional security directives on cybersecurity for railroads and rail transit, as well as further mandatory requirements for aviation.[5] Stakeholders have also expressed serious concerns with the development and potential implementation of any forthcoming directives, citing the stringent timeframes for reporting, high costs for compliance, and the extensive amount of information to be reported, which may obscure true cyber threats.[6]

We must protect our Nation's critical transportation and infrastructure assets against cyber-attacks and intrusions from malicious actors. The consequences of failing to do so could lead to negative impacts on the operability and reliability of our most essential transportation and infrastructure assets and subsequently affect safety, business operations, and the economies that rely upon them.[7] However, in doing so, we must ensure that efforts to secure our transportation and infrastructure are done in a collaborative manner with private industry and relevant stakeholders and do not impose regulatory burdens that interfere with ongoing cybersecurity efforts.

Given this, we are concerned that the recently issued and forthcoming security directives from TSA on cybersecurity in the transportation and infrastructure sectors do not follow these critical principles. To address these concerns, we request a review of TSA's development and issuance of security directives or emergency amendments this year. In particular, we request that you examine the following in regards each security directive or emergency amendment related to cybersecurity issued or in development this year:

1. The basis for the directive or amendment and, in each case, the basis for employing the emergency authority under section 114(l)(2) of title 49, United States Code, to issue those directives without full notice and comment, including:
   a. Any consultation with the Office of the Secretary of Homeland Security or the Executive Office of the President;
   b. TSA's identification of imminent, elevated, or additional specific threats to infrastructure and operations of pipelines, railroads, rail transit systems, and the aviation sector; and
   c. The timing and public announcements of the directives including those announced by the Secretary for railroads, rail transit agencies, and the aviation sector on October 6, 2021;
2. The consultation process with stakeholders in each case, including industry, other federal agencies, and Congress, which should examine:
   a. The timelines accorded for affected industries to provide feedback;
   b. The extent to which TSA modified the content of the draft security directives to address industry comments or concerns raised by stakeholders in the pipeline, railroad, rail transit, and aviation industries ; and
   c. The Federal agencies that contributed to the development of these security directives and their involvement, including the Department of Transportation, and any modifications to the content of the draft security directives to address any comments or concerns;
3. The basis for designating of all or parts of the draft and final security directives and related documents as Sensitive Security Information (SSI) and the non-designation of the final SD–01 as SSI including:
   a. Whether the SSI designation was used to restrict access for any reason other than those authorized by law;
   b. The basis for designating information as SSI in a draft but not a final security directive; and
   c. The specific information designated as SSI in each draft or final security directive and why such a designation was made;

[5] Press Release, DHS, Secretary Mayorkas Delivers Remarks at the 12th Annual Billington CyberSecurity Summit (Oct. 6, 2021), *available at* https://www.dhs.gov/news/2021/10/06/secretary-mayorkas-delivers-remarks-12th-annual-billington-cybersecurity-summit.

[6] Letter from the American Public Transportation Association to the Hon. Peter A. DeFazio and the Hon. Sam Graves, H. Comm. on Transportation & Infrastructure (Nov. 4, 2021) (on file with Committee); *see also: The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure: Hearing before the H. Comm. on Transportation & Infrastructure*, 117th Cong. (Nov. 4, 2021) (Statement of Tom Farmer, Asst. Vice President, Security, Association of American Railroads), *available at* https://transportation.house.gov/imo/media/doc/2021-11-04%20Testimony%20-%20Thomas%20Farmer.pdf.

[7] *The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure: Hearing before the H. Comm. on Transportation & Infrastructure*, 117th Cong. (Nov. 4, 2021), *available at* https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114196.

4. Whether CISA has statutory authority to order private sector entities to report cybersecurity incidences, including those contained in the Security Directives, to the agency; should examine:
   a. The history of TSA using its statutory authority to require reporting by private sector entities to other agencies of the government.
5. The workforce capacity at TSA or CISA to develop and implement security directives for the transportation and infrastructure sectors, including:
   a. The number of full-time employees dedicated to development and implementation of the security directives;
   b. The number of staff with expertise in the industrial, safety, or cybersecurity operations of the pipeline, railroads, rail transit, and aviation industries; and
   c. Any use of other federal agencies or federal government contractors to develop or implement the security directives.

We request that you review this matter and submit a report to us within 120 days. In the interim, we request that you provide us with regular updates. Thank you for your attention to this matter. If you have questions, please contact Melissa Beaumont, with the Minority Staff of the Subcommittee on Railroads, Pipelines, and Hazardous Materials [phone number redacted].

Sincerely,

SAM GRAVES,
Ranking Member.

RICK CRAWFORD,
Ranking Member, Subcommittee on
Railroads, Pipelines, and Hazardous Materials.

cc: The Honorable Peter A. DeFazio, Chair, Committee on Transportation and Infrastructure
The Honorable Donald Payne, Subcommittee on Railroads, Pipelines, and Hazardous Materials of the Committee on Transportation and Infrastructure

Letter of October 28, 2021, to Hon. Joseph V. Cuffari, Inspector General, Department of Homeland Security, from Senator Rob Portman, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs et al., Submitted for the Record by Hon. Eric A. "Rick" Crawford

UNITED STATES SENATE,
WASHINGTON, DC,
October 28, 2021.

The Honorable JOSEPH V. CUFFARI,
Inspector General,
Department of Homeland Security, Office of the Inspector General, Washington, DC 20528–0305.

DEAR MR. CUFFARI:

We write to request you review the process by which the Transportation Security Administration (TSA) has developed and issued several emergency security directives this year, including recently issued and announced cybersecurity directives developed in consultation with the Cybersecurity and Infrastructure Security Agency (CISA).

Our critical infrastructure must be secured and protected against cyberattacks. However, securing critical infrastructure requires a collaborative approach with the experts in these industries—the people who operate this critical infrastructure and who are charged with implementing these directives. We believe that care must be taken to avoid unnecessarily burdensome requirements that shift resources away from responding to cyberattacks to regulatory compliance. Unfortunately, we have received reports that TSA and CISA failed to give adequate consideration to feedback from stakeholders and subject matter experts who work in these fields and that the requirements are too inflexible. We are also troubled that TSA and the DHS Office of Legislative Affairs (DHS OLA) refused to provide copies of the draft directives to Congress, including the Chairs and Ranking Members of its congressional oversight committees, despite having shared copies with the pipeline industry.

The TSA Administrator has the statutory authority to issue security regulations in the transportation sector. Under a related authority, which had never before been exercised with the pipeline sector, the Administrator may issue emergency security regulations or directives without notice and comment if the Administrator determines that it "must be issued immediately in order to protect transportation security." [1] At least until earlier this year, TSA had worked in close coordination with industry stakeholders to develop practical security guidelines and policies.[2]

We are concerned that the recently issued security directives appear to depart from TSA's historically collaborative relationship with industry experts. On May 27, 2021, in response to the Colonial Pipeline ransomware attack, TSA Administrator David Pekoske exercised the emergency security directive authority and issued TSA's first ever pipeline-focused security directive (SD–01).[3] On July 20th, TSA issued a second security directive to the pipeline industry entitled, "Security Directive Pipeline—2021–02: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing" (SD–02).[4] In response, on August 24, 2021, associations representing more than 2,700 companies in the oil and natural gas subsector sent a letter to TSA Administrator Pekoske warning of inadequate consultation and that the resulting security directives could have "operational safety and reliability" impacts.[5]

On October 6th, Secretary Mayorkas announced TSA would issue additional security directives requiring railroad and airport operators to improve their cybersecurity practices.[6] Public reports again indicate that TSA provided very little time for industry feedback.[7]

Another area of concern is that TSA and the DHS OLA also refused to provide copies of the draft directives to Congress, including the Chairs and Ranking Members of its congressional oversight committees, despite having shared copies of the drafts with the pipeline industry. In a briefing with Senate staff on July 15, 2021, TSA officials explained they would not be providing a draft of SD–02 to Senate staff because it was pre-decisional and therefore deliberative.[8] This argument appears to misapprehend the function and limits of the deliberative process privilege, which is not a bar to disclosure, especially not to Congress, and in any event is generally considered waived once an agency has "officially acknowledged" the record by prior disclosure outside the Government, as here.[9]

We agree that critical infrastructure must be protected against cyber-attacks, particularly in the wake of the Colonial Pipeline ransomware attack, but the process by which TSA has issued these directives raises concerns. To address these concerns, we request that you review TSA's development and issuance of emergency security directives this year. Specifically, we request that you examine the following with regard to each emergency security directive or emergency amendment related to cybersecurity issued this year:

1. The basis for the directive or amendment and, in each case, the basis for employing the emergency authority under section 114(l)(2) of title 49, United States Code, to issue those directives without full notice and comment, including:
   a. Any consultation with the Office of the Secretary of Homeland Security or the Executive Office of the President;
   b. TSA's identification of additional threats to pipeline critical infrastructure, rail transit systems, and the aviation sector; and
   c. The timing of the directives and announcements of the directives including those announced on October 6;
2. The consultation process with stakeholders in each case, including industry, other agencies, and Congress, which should examine:

[1] 49 U.S.C. § 114 (l)(2)(A).

[2] Transp. Sec. Admin, U.S. Dep't Of Homeland Sec., Pipeline Security Guidelines (2018), *available at* https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

[3] Ratification of Security Directive, 86 Fed. Reg. 38209 (Jul. 20, 2021); Press Release, U.S. Dep't of Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021), https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[4] Press Release, U.S. Dep't of Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (Jul. 20, 2021), https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[5] Letter from Pipeline Trade Associations to TSA Administrator David P. Pekoske (Aug. 24, 2021) (enclosed).

[6] Press Release, U.S. Dep't of Homeland Sec., Secretary Mayorkas Delivers Remarks at the 12th Annual Billington CyberSecurity Summit (Oct. 6, 2021), https://www.dhs.gov/news/2021/10/06/secretary-mayorkas-delivers-remarks-12th-annual-billington-cybersecurity-summit.

[7] *E.g.*, Oriana Pawlyk, *Freight rail blasts TSA cybersecurity proposal as redundant*, Politico (Oct. 6, 2021), https://subscriber.politicopro.com/article/2021/10/freight-rail-blasts-tsa-cybersecurity-proposal-as-redundant-3991607.

[8] Briefing with HSGAC Staff (Jul. 15, 2021) (notes on file with Committee).

[9] *See, e.g.*, Fitzgibbon v. CIA, 911 F.2d 755, 765 (1990).

a. The timeline for affected industries to provide feedback;

b. The extent to which TSA modified draft security directives to address industry comments or concerns; and

c. The Federal agencies who contributed to the development of these security directives and their involvement;

3. The basis for designating of all or parts of the draft and final security directives and related documents as Sensitive Security Information (SSI) and the non-designation of the final SD–01 as SSI including:

a. Whether the SSI designation was used to restrict access for any reason other than those reasons authorized by law;

b. The basis for designating information as SSI in a draft but not a final security directive; and

c. The specific information designated as SSI in each draft or final security directive and why such a designation was made; and

4. The basis for withholding the draft directives from Congress.

We request that you review this matter and submit a report to us within 120 days. In the interim, we request that you provide us with monthly updates. Thank you for your prompt attention to this important request.

Sincerely,

ROB PORTMAN,
Ranking Member, Committee on Homeland Security and Governmental Affairs.

JAMES LANKFORD,
Ranking Member, Subcommittee on Government Operations and Border Management, Committee on Homeland Security and Governmental Affairs.

M. MICHAEL ROUNDS,
United States Senator.

Enclosure

ATTACHMENT 1: LETTER TO ADMINISTRATOR PEKOSKE

AMERICAN FUEL AND PETROCHEMICAL MANUFACTURERS,
AMERICAN GAS ASSOCIATION,
ASSOCIATION OF OIL PIPE LINES,
AMERICAN PETROLEUM INSTITUTE,
AMERICAN PUBLIC GAS ASSOCIATION,
INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA,
GPA MIDSTREAM ASSOCIATION,
August 24, 2021.

The Honorable DAVID P. PEKOSKE,
Administrator,
Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598–6020.

ADMINISTRATOR PEKOSKE,

The included pipeline trade associations, AFPM, AGA, AOPL, API, APGA, INGAA, and GPA Midstream appreciate the opportunity to provide feedback on the recent Security Directive 2021–02, issued on July 19, 2021 (Directive). These trade associations represent almost all aspects of U.S. energy pipeline operations that serve customers reliably across North America. The associations' members represent refineries and petrochemical operators—through which pipelines receive and distribute products, regional and local natural gas distribution pipelines, liquids pipelines, integrated and midstream natural gas and oil companies, operators of municipal natural gas systems, natural gas transmission pipelines, and natural gas product pipelines and processors. Across the industry, our members all share the same concerns with the implementation of Security Directive 2021–02 and the process with which it was developed. For nearly two decades, we have worked along-side TSA in a structured oversight model applying risk-based methodology that properly balanced pipeline security with operational reliability and safety. We understand the ongoing situation presented by ransomware and other cyber threats to critical infrastructure and are committed to working with TSA to continue sound pipeline security practices and policies.

Open communication, process transparency, and timely engagement with the industry have been hallmarks of the TSA pipeline security program. Concerningly, these fundamental elements of a strong security partnership were not fully realized during the process used to develop the Directive. We wish to reemphasize the need for TSA to work efficiently with affected companies on successful Directive implementation, especially now that compliance deadlines are approaching. We encourage

TSA and its technical experts to work closely with industry experts to ensure mutual understanding of how requirements in the Directive could impact operational reliability.

While we appreciate that TSA published an initial list of frequently asked questions (FAQs) focused on administrative matters, there remain several unanswered technical questions submitted by the associations and our members to which TSA guidance is critical for compliance. These unanswered questions have left operators with significant uncertainty about what is required for compliance. We urge TSA to release the technical FAQs in a timelier manner—TSA's timeline to responding to questions should be consistent with the rapid deadlines established under the Directive. We also ask TSA to apply learnings from the recent Directive development process to improve the agency's procedures for obtaining stakeholder input on future pipeline security initiatives and avoid recreating the implementation challenges and uncertainty our members are now experiencing.

Operational reliability and safety are extremely important to the pipeline industry. The Directive's potential to cause operational disruptions or threaten safe operations remains a concern of affected pipeline operators. Our pipeline operators have expert knowledge regarding their assets, how they are managed to meet customer needs, and how to comply with the various state and federal regulations under which they are required to operate. As the Directive was developed, industry conveyed highly probable operational safety and reliability concerns that could arise by imposing prescriptive cyber requirements and untenable timelines without specific understanding of a company's existing cybersecurity protections and operations. We appreciate that TSA addressed some of our recommendations and responded to our feedback. Regretfully, significant concerns remain. The broad scope and prescriptive nature of the Directive create potential conflicts with TSA pipeline Security Guidelines and with existing cybersecurity and safety regulations from other federal government entities. The prescribed implementation schedule creates safety and reliability concerns. We urge TSA to work closely and quickly with operators on Directive implementation to ensure affected pipelines do not have to choose between complying with the Directive and ensuring continued safety and reliable operations.

The Directive allows operators flexibility to submit alternative compliance options to TSA for consideration, and TSA has stated it will respond promptly to these submissions. We recognize TSA believes operator concerns may be addressed through this alternative submittal option. However, the usability of this option is limited without further clarity on TSA's anticipated criteria and timelines for review of alternative proposals relative to the Directive's deadlines, what recourse operators have if TSA disagrees with proposed alternative compliance options, and how TSA will address scenarios where an operator determines that extensive equipment retrofits will take longer time periods than envisioned by TSA. Furthermore, TSA should ensure operators are not penalized for awaiting TSA's clarification of these issues and approval of alternative proposals as the Directive's deadlines approach. Pipeline operators also face challenges applying the Directive in the context of broader corporate structures, given that cybersecurity for some pipeline operations is managed across individual companies and countries as part of enterprise-level cybersecurity and information technology systems that also cover non-pipeline operations. As the Directive is currently written, and without clarity from TSA, some operators are in the position of guessing what nonoperational networks (e.g., finance, HR, etc.) are impacted by the Directive and may be applying prescriptive measures that divert resources while not addressing the actual risks to pipeline operations. We urge TSA to provide more clarity on the scope, so that operators can make more sound determinations of what is necessary to avoid disrupting operations or threatening pipeline safety.

We also urge TSA to reconsider its process for implementing pipeline security initiatives in the future to ensure better input on the compatibility of proposed security requirements with pipeline operational technology. It is important TSA make timely updates to its pipeline security policies to keep up with evolving threats. At the same time, it is equally important TSA's process does not sacrifice input from the regulated industry for the sake of speed. TSA's authorizing statute[1] and the Administrative Procedures Act require that the agency use formal notice-and-comment rulemaking as the primary vehicle for issuing new requirements. In this case, we believe the robust stakeholder input and advisory committee review provided by a notice-and-comment rulemaking would have resolved many of the substantive challenges created by the current Directive text and promoted stronger public-private partnership for pipeline security. We acknowledge that TSA may wish to protect certain aspects of its proposed requirements as Sensitive Security Information and note

[1] 49 U.S.C. § 114(l)(2)(A).

that procedures other than formal notice-and-comment can also be successful in soliciting and incorporating necessary input on a timely basis.

Our associations are also concerned that, as you testified to the Senate Commerce Committee on July 27, 2021, there is additional threat information driving the urgency of the Directive and the timelines that have been set. This threat intelligence has not been shared with potentially affected companies. Pipeline operators are best positioned to design mitigations to defend their systems against new threats based on their risk-based security programs. They are unable to effectively prepare for threats about which they have not been briefed. While we do appreciate the recent offer of a Secret level briefing to a limited group of associations within the Beltway, we again highlight the need for TSA, and the broader intelligence community, to ensure they are sharing the most timely and relevant information directly with the potentially impacted operators. We urge TSA, and other agencies that have threat information relevant to pipelines, to brief all potentially affected companies as soon as possible to ensure they can appropriately defend against current threats. We also encourage TSA to work with the broader intelligence community (IC) to provide regularly scheduled briefings to pipeline industry experts to ensure operators are appropriately informed about the evolving threats to their systems. TSA should also work with the IC to provide as much timely, unclassified information as possible to operators to ensure it is actionable and can be disseminated to operators who do not possess security clearances.

Listed below is a summary of our requests.

- TSA and its technical experts should work closely and quickly with industry experts to ensure mutual understanding of how requirements in the Directive could impact operational safety and reliability.
- TSA should release the technical FAQs immediately.
- TSA should provide clarity on anticipated criteria and timelines for review of alternative proposals, including addressing operator recourse if TSA disagrees with the alternative proposal and how TSA will address supply chain limitations.
- TSA should ensure operators are not penalized for awaiting TSA's review of alternative proposals.
- TSA should provide more clarity on the Directive's scope so that operators can make more sound determinations of what is necessary to avoid disrupting operations or threatening pipeline safety.
- TSA should reconsider its process for implementing pipeline security initiatives in the future to ensure better input on the compatibility of proposed security requirements with pipeline operational technology.
- TSA and pertinent government intelligence community should brief all potentially affected pipelines on relevant cybersecurity threat intelligence as soon as possible.

The associations and our members are committed to supporting efforts to build pipeline cyber security capability, and we look forward to further discussing our concerns and potential solutions to ensure the Directive implementation can be successful.

Mr. CRAWFORD. Thank you, Mr. Chairman.

I would just like to—to Ms. Newhouse, how would TSA evaluate implementation of the pipeline security directives?

Ms. NEWHOUSE. Thank you for your question, Congressman Crawford.

We continue extensive, extensive engagement. That is the hallmark of what we are doing in order to ensure continuous improvement. We have actually developed and implemented an entire field surface operational structure to do this. So, we have boots on the ground.

And what we have been finding, thus far, we—as you mentioned, sir, we have issued two security directives this summer, post-Colonial Pipeline. We are proud to announce, on behalf of us and our stakeholders, that all stakeholders that are subject to that directive have met all of the requirements in the very first security directive. It was very tight guidelines, communicated beautifully with us, very vocal, and, frankly, very direct with us when they met challenges.

We are now in the process——

Mr. CRAWFORD. Let me ask you about those challenges, if I could. What challenges have you identified during implementation?

Ms. NEWHOUSE. Well, I think the biggest one—and we have actually taken this to heart—is the definition of a reportable cybersecurity incident. And we have taken steps and a great deal of feedback to modify that definition to not include all potential incidents.

Mr. CRAWFORD. OK.

Ms. NEWHOUSE. We have narrowed that, and focused that, based on industry feedback.

Mr. CRAWFORD. Excellent. Recently, the oil and natural gas pipeline trade associations jointly requested TSA conduct an advance notice of proposed rulemaking to gather information vital to drafting a proposed regulation to replace the expiring security directives.

I ask unanimous consent for this letter to be entered into the record, Mr. Chairman.

Mr. DEFAZIO. Without objection.

[The information follows:]

Letter of November 22, 2021, to Hon. David P. Pekoske, Administrator, Transportation Security Administration, from American Fuel and Petrochemical Manufacturers et al., Submitted for the Record by Hon. Eric A. "Rick" Crawford

AMERICAN FUEL AND PETROCHEMICAL MANUFACTURERS,
AMERICAN GAS ASSOCIATION,
ASSOCIATION OF OIL PIPE LINES,
AMERICAN PETROLEUM INSTITUTE,
AMERICAN PUBLIC GAS ASSOCIATION,
INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA,
GPA MIDSTREAM ASSOCIATION,
November 22, 2021.

The Honorable DAVID P. PEKOSKE,
Administrator,
Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 22150.

ADMINISTRATOR PEKOSKE,

The included pipeline trade associations, AFPM, AGA, AOPL, API, APGA, INGAA, and GPA Midstream appreciate the opportunity to engage with TSA in the next phase of pipeline cybersecurity regulations. These trade associations represent almost all aspects of U.S. energy pipeline operations that serve customers reliably across North America. The associations' members represent refineries and petrochemical operators—through which pipelines receive and distribute products, regional and local natural gas distribution pipelines, liquids pipelines, integrated and midstream natural gas and oil companies, operators of municipal natural gas systems, natural gas transmission pipelines, and natural gas product pipelines and processors.

Across the industry, our members all share the same concerns regarding TSA's development of pipeline cybersecurity regulations. Both pipeline Security Directives[1] are slated to sunset in May and July 2022, respectively. Based on conversations with you and the TSA Surface Operations and Policy sections, we understand TSA intends to pursue formal rulemaking for pipeline cybersecurity to replace the Security Directives. Your remarks to our associations and members this Fall regarding collaboration and process transparency around future rulemaking were well-re-

[1] *Security Directive Pipeline 2021–01* issued on May 28, 2021 and *Security Directive Pipeline 2021–02* issued on July 19, 2021

ceived. Notably, you welcomed the opportunity for pre-rulemaking meetings with stakeholders and underscored TSA's intention to have a robust, thoughtful comment period for each phase of the rulemaking process.

In light of this, we strongly urge TSA to issue an Advanced Notice of Proposed Rulemaking (ANPRM) well in advance of the sunset dates for the Security Directives. Further, given the rule will likely affect a broader range of companies than presently impacted by the Security Directives, an ANPRM is appropriate for obtaining input from the additional potentially impacted entities.

TSA can leverage the ANPRM formal process to receive feedback from industry and public stakeholders on risk-based pipeline cybersecurity regulations and responses to questions that promote a greater understanding of what are reasonable, applicable, auditable, and sustainable regulations. For example, central questions TSA should address as part of pipeline cybersecurity development include:

1. What types of cybersecurity risks are most threatening to operating a pipeline safely and without interruption?
2. How can TSA design a cybersecurity regulatory program to best address the risks faced by pipeline operators?
3. What factors should TSA consider to ensure cybersecurity regulatory requirements do not disrupt or impair pipeline operations or safety systems?
4. How should TSA design a cybersecurity regulatory program so that it is able to evolve with the risks and tactics of cybercriminals?

By following the approach of other federal government agencies and asking a series of questions on the subject matter, TSA can develop, issue, and receive ANPRM comments on a short timeline. To the extent TSA questions whether an ANPRM would add additional time to the rulemaking process, our trade associations pledge to respond to an ANPRM in a timely manner.

Operational reliability and safety are important to the pipeline industry. We are committed to supporting efforts to advance pipeline cybersecurity capability. Our associations and members have the technical expertise to inform such regulations so that prescribed actions do not compromise reliability and safety, nor conflict with existing cybersecurity regulations. We look forward to working with TSA on regulation development.

Mr. CRAWFORD. Thank you, sir. I hate to keep bothering you with that, I know your throat is killing you.

As they stated, TSA can leverage the ANPRM informal process to promote a greater understanding of what are reasonable, applicable, auditable, and sustainable regulations.

Will TSA issue an ANPRM to gather this important information?

Ms. NEWHOUSE. Thank you for your question, Congressman.

We are considering all of our options, including the most transparent options. An ANPRM, or advanced notice of proposed rulemaking, is one tool that we have exercised in the past successfully. And as we have continued robust engagement both at the classified and unclassified level with all of our surface transportation stakeholders, in particular our pipeline, rail, freight rail, passenger rail, and aviation stakeholders, we are considering all of those options. So yes, sir, that is on the table.

Mr. CRAWFORD. As you know, we are anticipating the release of a new security directive for rail. It should be as early as this afternoon, if I understand correctly.

Unfortunately, we have heard concerns about the development of these directives from stakeholders, including from the freight rail industry, at our previous hearing on cybersecurity, and in a November 4th letter from the American Public Transportation Association, which I also ask unanimous consent to be entered into the record.

I apologize for that inconvenience one more time, Mr. Chairman.

Mr. DEFAZIO. Without objection.

[The information follows:]

Letter of November 4, 2021, to Hon. Peter A. DeFazio and Hon. Sam Graves of the Committee on Transportation and Infrastructure, from Paul P. Skoutelas, President and CEO, American Public Transportation Association, Submitted for the Record by Hon. Eric A. "Rick" Crawford

American Public Transportation Association,
1300 I Street NW, Suite 1200 East,
Washington, DC 20005,
November 4, 2021.

The Honorable Peter A. DeFazio,
Chairman,
House Committee on Transportation and Infrastructure, 2165 Rayburn House Office Building, Washington, DC 20515.

The Honorable Sam Graves,
Ranking Member,
House Committee on Transportation and Infrastructure, 2164 Rayburn House Office Building, Washington, DC 20515.

Dear Chairman DeFazio and Ranking Member Graves:

On behalf of the 1,500 member organizations of the American Public Transportation Association (APTA), and in advance of the House Committee on Transportation and Infrastructure's hearing on *The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure*, I write to share our concerns on the forthcoming Transportation Security Administration (TSA) Security Directive for rail transit and passenger rail operations. On October 6, 2021, U.S. Department of Homeland Security Secretary Alejandro Mayorkas announced that TSA is expected to impose cybersecurity mandates on certain rail transit systems and railroads, including a stringent incident reporting deadline and a short timeframe to develop and implement response and contingency plans.

Specifically, APTA is concerned that TSA is imposing these new and potentially costly requirements through an emergency security directive without the benefit of public notice and comment, including an analysis of the economic impact of the new requirements on rail transit and passenger rail operators. For example, mandating a prescriptive 24-hour reporting requirement in a security directive could negatively affect cyber response and mitigation by diverting personnel and resources to reporting when incident response is most critical. Further, the additional personnel and resources needed to comply with the requirements will add significant compliance costs just as transit agencies are working to recover from the COVID–19 pandemic. TSA has previously employed the federal rulemaking process for other security requirements on surface transportation systems, including a rulemaking on Security Training for Surface Transportation Employees (86 Fed. Reg. 23629).

Accordingly, APTA strongly recommends that the Committee on Transportation and Infrastructure urge TSA to utilize the federal rulemaking process for this security directive and allow for public comment before imposing any new requirements. Publication in the *Federal Register*, with an opportunity for notice and comment, will allow all affected parties, including APTA members, to identify concerns and potential impacts of the proposed requirements on rail transit and passenger rail operations, and would provide TSA sufficient time to address any issues raised during the process.

In addition, APTA recommends that TSA provide technical assistance, workshops, response plan templates, and funding for public transit agencies to implement the requirements of any final security directive.

We welcome any opportunity to work with the Committee on Transportation and Infrastructure to address these important issues and ensure that rail transit and passenger rail operators continue to meet any cyber or other security challenges that may arise.

Sincerely,

Paul P. Skoutelas,
President and CEO.

Mr. Crawford. Ms. Newhouse, how much stakeholder engagement has TSA conducted while working on these directives?

And how is TSA specifically incorporating feedback into these directives?

Ms. Newhouse. Thank you, Congressman.

We have continued robust engagement and, frankly, we have been working extremely closely with the United States intelligence community, our partners at CISA, and particularly the Departments of Homeland Security, DOT, Department of Energy, and across the interagency to provide that background information, that threat information that is driving all of these requirements.

As recently as this week, I, along with several of my top leadership here at TSA, have met with freight rail and passenger rail executives with a classified briefing in our facilities to show them what we are seeing, elicit input, and ask them for more input for either future requirements or other guidelines that we could issue together, versus us just telling them this is what they need to do.

So, we have—we have been having some successful engagements. As a matter of fact, today, a number of pipeline individuals, CISOs, and other security personnel are receiving briefings, as we speak, and we do have an apparatus around the United States to support those briefings, thanks to our law enforcement and intelligence community partners.

Mr. DEFAZIO. I thank the——

Mr. CRAWFORD. Will you consider utilizing the Federal rulemaking process for any future cyber requirements?

Mr. DEFAZIO. I think his time has expired.

Ms. NEWHOUSE. Absolutely, Congressman. All of those options are on the table.

Mr. CRAWFORD. Thank you. I yield back.

Mr. DEFAZIO. I thank the gentleman. Representative Norton is now recognized.

Ms. NORTON. Thank you very much, Mr. Chairman. I hope everyone can hear me. My first question is for Mr. Schachter of DOT, Mr. Grossman of FAA, and Ms. Newhouse of TSA. I am interested in information sharing among Federal partners.

You each oversee critical infrastructure entities, with some overlap, especially regarding aviation and surface transportation, which I am particularly interested in because I sit on the Subcommittee on Aviation, and serve as chair of the Subcommittee on Highways and Transit.

Can you explain to us in some detail how you collaborate to oversee the same sectors and critical infrastructure entities?

[Pause.]

Ms. NORTON. Mr. Schachter, Mr. Grossman, Ms. Newhouse?

Mr. SCHACHTER. Am I on mute?

Thank you very much for that question, Congresswoman. Information sharing is vital to securing the Nation's critical infrastructure, and the infrastructure that DOT is responsible for.

We collaborate extensively within DOT. We collaborate with the FAA, and also with our Federal partners—in particular, TSA, CISA, and even with OMB, which houses the Federal chief information security officer. Chris DeRusha, the Federal Chief Information Security Officer, was one of the first Federal officials that I met—virtually, of course—after joining the DOT in late August.

I have had subsequent sessions with Jen Easterly, as well as Chris Inglis, the Assistant Director and National Cyber Director. And we intend to keep up an open channel of communication, as well as following up on various directives and formal information sharing that DHS has required.

Ms. NORTON. Thank you.

Mr. Marinos, Mr. Dorsey, can you highlight cybersecurity issues that give you the most concern, and also explain why you believe the Government has repeatedly failed to fully address them?

Mr. MARINOS. Yes, Congresswoman. I could jump in first, and perhaps Kevin can go after.

I think the bottom line is that we are constantly operating behind the eight ball. The reality is that it just takes one successful cyberattack to take down an organization, and each Federal agency, as well as owners and operators in critical infrastructure, have to protect themselves against countless numbers of attacks. And so, in order to do that, we need our Federal Government to be operating in the most strategic way possible.

So, as I mentioned in my oral statement, the importance of having a national strategy isn't just to have something on paper, but to actually execute that strategy. And that also carries forward to those agencies like the Department of Transportation, TSA, and others who have sector-specific responsibilities to do the same.

We have seen consistently in our work that agencies have had challenges in maintaining very up-to-date sector plans that actually would talk about the cyber threats that agencies are facing and the infrastructure is facing today. So, we think it is very important for sector-specific agencies to work with their industry partners to make sure that they are operating off the same song sheet, if you will.

Ms. NORTON. Thank you very much.

Thank you, Mr. Chairman, I yield back.

Mr. DEFAZIO. I thank the gentlelady for yielding back. I am now going to yield the chair to André Carson, who, as we all know, has a loud and booming voice, and you will be able to understand him. So, thank you.

Mr. CARSON [presiding]. Thank you, Chair, I hope you feel better. We appreciate you.

Mr. Gibbs?

Mr. GIBBS. Thank you, Chair. This hearing is titled, "The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure." I was really kind of surprised we didn't bring in a witness from the Cybersecurity and Infrastructure Security Agency, CISA. It might be a good idea for the future.

Admiral Mauger, we had testimony in the past, and we know that the Coast Guard is trying to update your own IT systems and the significant challenges you face in doing that. Can you provide us an update on how the Coast Guard is working to improve in this area, and improve your IT systems that you have been mandated by Congress to do?

Admiral MAUGER. Congressman Gibbs, our approach to protecting the maritime transportation system relies on us having our own ability to defend and operate our networks.

And so, as part of the Commandant's strategy for our work ahead, he has put defend and operate the networks, protect maritime critical infrastructure, and enable Coast Guard operations as those three pillars for how we move forward to accomplish all of our missions.

With regard to defending and operating our networks through investments in the CARES Act, with over $65 million in funding, we have been able to make significant investments to modernize our infrastructure and push more information out to our mobile users out in the field, and our cutters underway.

But all of this is premised—our security is premised on it being an operational imperative. And so, the key thing that has really driven us forward is the establishment of Coast Guard Cyber Command as an operational command under the purview of a two-star commander that oversees our daily mission execution in the IT space, and then the coordination with our CIO, who is driving those investments and modernization projects forward.

Mr. GIBBS. OK, thank you. Also, Admiral, can you expand a little bit on the activities and resources you are making available to the ports to work with our port facilities at the port level on their IT infrastructure, cybersecurity?

Admiral MAUGER. Congressman, at the port level we are really focused on working across the prevention and response framework to ensure that we have the ability to defend, and then also respond resiliently from attacks. This is a shared responsibility between the private sector and the Federal agencies involved, and so we are doing a number of different things.

First of all, we put standards in place that require them to conduct assessments, have an accountable person, develop a plan, mitigate that plan, exercise it, and report incidents. All those pieces are really important.

Through those assessments, we then have the opportunity to drive investments through the Port Security Grant Program to update security posture in the ports. And so last year, $17 million was allocated from the Port Security Grant Program for cybersecurity.

These are some of the things that are being done to increase the capability of the commercial infrastructure, while also maintaining our operational ability.

Mr. GIBBS. Also, Admiral, as your role as assistant commandant for prevention policy, you are responsible for the Coast Guard's maritime safety and security regulatory programs. Which side is winning: the increased cyber threats or increased digital-based safety operational enhancements?

How are we doing? I guess the question is, how are we doing in this fight? Who is winning it?

Admiral MAUGER. Congressman, it is not an either/or proposition for this. It is really an all-of-the-above.

And so, as the assistant commandant for prevention policy, we make sure that we bring together the best of our ability to secure private industry, but then be able to respond, as well. And so, leveraging our prevention and response framework, we have made sure that we have taken a multilayered approach to engaging with the industry, sharing information with them at the local level through the Area Maritime Security Committees, and conducting compliance activities, and then, at the national level, engaging across the interagency with our National Maritime Security Advisory Committee, with the MTS–ISAC, and then with other interagency partners to make sure that we are tied together, and providing a comprehensive network and comprehensive approach to this problem.

Mr. GIBBS. All right, thank you. I am just about out of time. I just wanted to mention that I know you are not a cybersecurity expert yourself, and so, hopefully, you are aware of that fact, and you are coordinating with your cybersecurity people, both at the Coast Guard, and also in the private sector.

And I have to yield back, I am out of time. Thank you for your service.

Mr. CARSON. Mr. Larsen?

Mr. LARSEN. Thank you, Mr. Chair.

Mr. Dorsey, has the GAO investigated the progress of the Federal agencies or the private sector in implementing the guidance and requirements laid out in the May Executive order from the President to modernize and strengthen the defense of Federal technology systems?

Mr. DORSEY. Thank you for that question, Congressman. However, you asked whether or not the GAO has investigated. I think that question should be directed towards the GAO representative. That is, if I am not mistaken.

Mr. LARSEN. I am sorry, yes. Well, the GAO representative Mr. Marinos, can answer that.

Mr. MARINOS. Yes, Congressman, happy to. We have looked at aspects of the Executive order. We, actually, just have work underway right now, specifically looking at the progress that has been made by the administration in actually overseeing whether the many requirements that it has placed on agencies have actually been adhered to.

So, there are aspects within it that our work has touched on, including cloud computing and supply chain, more recently, but we have work underway right now that is going to be looking squarely at the Executive order.

Mr. LARSEN. And do you have the timeline laid out for the report already?

Mr. MARINOS. We are expecting to be able to periodically report on the status of implementing the Executive order throughout the upcoming calendar year. So, we are looking to provide information out sort of in a real-time basis, looking to provide something closer to the early spring.

Mr. LARSEN. Early spring? Thank you.

And Mr. Dorsey, then, I will go back to you. At what point would the DOT IG get involved?

Mr. DORSEY. Thank you for your question, Congressman. Actually, we have actually already initiated a review of the DOT's efforts to implement cloud-based services with respect to the request, or issues that were identified in the Presidential Executive order directing Federal agencies to ensure that they secure their cloud-based services as they migrate forward.

We are also planning to look at the Department's efforts to implement or migrate towards a zero trust architecture, as outlined in the President's Executive order, too.

I have also been in contact with the Department's chief information officer, and he has informed me that the Department is working towards addressing the current initiatives, and I plan to work with him over the next year or two to ensure that the Department is doing what they say they are planning to do, as well as report back to the administration, as necessary. Thank you.

Mr. LARSEN. Thank you.

Mr. Grossman, the U.S. aviation sector is very complex. I am sure that you are considering that complexity as you consider how to make the system less vulnerable to cyberattacks.

But the testimony from GAO in the first part of the hearing a few weeks ago stated that less than half of the respondents to a global study investigating cybersecurity trends within the air transport industry identified cybersecurity as a top organizational risk.

Have you all considered how Congress can incentivize the private sector to address cybersecurity issues?

Mr. GROSSMAN. How Congress can——

Mr. LARSEN. Incentivize the private sector to address these cybersecurity issues that continue to persist in the air transport industry.

Mr. GROSSMAN. Well, we have reached out to industry through the Aviation Cyber Initiative extensively. We have built a community of interest of over 1,000 members that is across all of the components of the aviation ecosystem. And we are using the bully pulpit, and it seems to be, from an aviation perspective, we seem to be gaining a lot of traction.

Mr. LARSEN. Can I follow up on that with a particular issue? And I don't know if you are handling this at FAA, but Chair DeFazio and I recently have expressed safety concerns to the Federal Communications Commission on the telecom industry's plan to utilize the C-band for 5G broadband service, and the potential interference with aircraft radio altimeters.

I know that Administrator Dickson is weighing in on this with the FCC. Can you update us on what the status of that is, and, as well, are there other technologies that are coming online that we need to be concerned about?

Mr. GROSSMAN. Well, Congressman, thank you for that question.

I am not personally involved with the 5G effort, but I am aware that the telecommunications companies have voluntarily agreed to a 1-month deployment delay to their 5G C-band to allow further safety analysis.

We believe that aviation and 5G C-band wireless services can safely coexist, and the FCC and FAA are using this time to gather and exchange information to come up with a path forward.

Mr. LARSEN. Yes, and I guess implied in our letter is that whatever solution you all think you come up with, that we would be very interested in that solution to make some determinations about our own thoughts on it.

Mr. GROSSMAN. Absolutely.

Mr. LARSEN. Thank you very much.

Thank you, Mr. Chairman.

Mr. CARSON. Thank you.

Mr. Perry?

Mr. PERRY. Thank you very much, Mr. Chairman.

Mr. Schachter and Mr. Marinos, during last month's hearing on cybersecurity threats, I had an interesting back-and-forth with Mr. Scott Belcher from the Mineta Transportation Institute regarding the increased cybersecurity threats associated with the transition to electric buses, and the fact that it brings with it a whole new level of cyber exposure and other security risks not previously anticipated.

Mr. Belcher agreed that these increased risks include the ability to degrade batteries remotely, cause fires, manually take over controls of the vehicle, et cetera, and went on as far as to say we would be safer if we were still running diesel buses.

Now, I am a fan of both diesel and—well, all of them. We have just got to be ready to implement the processes to make sure that we are safe.

While we were discussing these issues in the context of electric buses purchased by transit agencies with FTA funding, these concerns are much more widespread than just buses. In fact, the same concerns apply to our electric vehicles, owned either by the Government or by private citizens, and the associated charging infrastructure.

I wonder if either of you can expand on the significant increase in cybersecurity risks and threats we should expect as the result of the reckless pursuit of an electrified vehicle fleet by the majority, this administration, and, unfortunately, some Socialist-voting Members of my own party. Can you expand upon what we can expect?

Mr. SCHACHTER. Well, thank you. Thank you for that question.

I think we are conflating two separate and very important issues. One is the fuel that any vehicle uses, whether it is electric power, diesel power. Inherently, they are not more or less at risk, from a cyber perspective.

What we are really talking about here, and the cyber issue, is the electronic control system that is on board with not only electric buses, but if you were to buy a new diesel bus, or gasoline bus, or gasoline car, those vehicles all have some sort of electronic control system there, communications system, which is potentially vulnerable. And the correct steps, just like in protecting Government IT systems, the correct steps need to be taken to protect the IT system in that vehicle.

And when we are talking about fossil-fuel powered vehicles or electric vehicles—obviously, the administration has identified addressing climate change as a top priority. And if we take the conversation to the subject of this hearing, which is cybersecurity, there are means and mechanisms of protecting those vehicles' intelligence systems on board. And we need to do that. And there are several organizations within DOT at work on that right now.

Mr. PERRY. Mr. Marinos?

Mr. MARINOS. Yes, Congressman. We have looked at issues with respect to modern vehicle cybersecurity over the last several years. And indeed, whether the fuel is gas or electric, the reality is that we are seeing an increase in the number of interfaces, the number of chips that are being placed, and the systems that those chips are powering.

In fact, that is what we are seeing right now, as one of the challenges in terms of supply chain, is having those chips to be able to manufacture new cars, regardless of the fuel.

The reality is that, if those interfaces are not properly secured, they can be exploited through direct physical access, and even remotely, as well. I think the reality, and maybe the very important element to this, is the need for our workforce to be able to be in the best position to oversee these types of automated technologies. And, as we reported back earlier this year, we think that the Department of Transportation needs to take a close look at its workforce to make sure that, as vehicles become more and more autonomous, that they have the appropriate folks in place to oversee that type of technology.

Mr. PERRY. Given DOT's lackluster cybersecurity posture at this moment, do you think they are prepared to deal with a massive increase in risk?

And I would characterize—while I know that all of them have electronic interfaces, chips, and so on and so forth, not all of them have the ability to set the battery on fire if they are not battery-powered, if the battery is just in there to start the vehicle.

But would you say that they are prepared to deal with the increase in risk?

Mr. MARINOS. I think that the Department—and I don't want to speak on its behalf, but in response to our recent work—I think would also recognize that it has more to do, in terms of being able to fill the skill gaps that they are going to need to fill to be in the best position to oversee this emerging technology.

Mr. PERRY. Mr. Schachter?

Mr. SCHACHTER. I would say DOT's security posture is on par or even better than other organizations that I have observed.

All of us—the Government, as a whole, as well as individual agencies—will have a continual challenge to meet cybersecurity requirements. And, as we have said earlier in the hearing, we receive thousands of cybersecurity attacks every day, and only one has to slip through. So, normal batting averages here don't apply. We have to be perfect to protect our systems, our agencies, the Government, and the American people. It is an immense challenge with limited resources. We all know that.

So that—I think DOT's posture is forward. Its attempts to include some of the very latest technologies—we were already on the road to many of the items that are contained in President Biden's Executive order on cybersecurity before that Executive order was issued.

The audit that was referred to a little while ago by Mr. Dorsey regarding cloud services, they are seen as a best practice, as opposed to desktop applications, because they can be better protected from a common perimeter. And DOT had previously organized itself into a—using a common operating environment, unifying all of the operating modes, with the exception of FAA, into a single system, thereby providing one surface to protect from attacks. That is a best practice.

We were there prior—toward the——

Mr. CARSON. The gentleman's time has expired.

Mr. PERRY. Thank you, Mr. Chairman, I yield.

Mr. CARSON. Mrs. Napolitano?

Mrs. NAPOLITANO. Yes, sir. Thank you, Mr. Chairman.

Mr. Marinos, you highlight in the testimony that, in February of this year, the Cybersecurity and Infrastructure Security Agency issued an alert explaining that the cyber threat actors obtained an unauthorized access to a U.S. water treatment facility's industrial control system and attempted to increase the amount of caustic chemical that is used as part of the treatment process.

My biggest concern is on security of our water systems, including our treatment plants, our dams, and our waterways. Are we doing enough to address the water systems' security? And what are your concerns in this area?

Mr. MARINOS. Simply put, we aren't, Congresswoman. The threats to the water infrastructure are real, and it comes from many of the same challenges that other sectors like it suffer, which include a reliance on legacy systems, systems that are not only outdated, but beyond even being supported by the vendors that actually created them.

These include also workforce issues, having appropriate staff within often very small organizations that manage these types of facilities to be able to respond. In fact, in the case of the February attack, or the attempted attack, it was fortunate that there was, according to reports, an official that was actually monitoring, and was able to see the efforts as it happened, so they were able to thwart it.

And so, I think the reality is that there needs to be more that is done. We are encouraged by the fact that Congress passed a law last year to establish in law the expectations of sector-specific agencies, known as Sector Risk Management Agencies, and the Environmental Protection Agency is that for the water sector.

We think that EPA can do more to reach out to the sector to better understand whether the guidance that it provides is adequate to be able to address many of the challenges that I mentioned.

Mrs. NAPOLITANO. Would you suggest that they do training, virtual training of all water agencies, small and large?

Mr. MARINOS. Yes, I think that it is important for them to do that, in concert with their sector partners. And so, there is a good establishment of both Government and sector-specific representation that, as I am aware, based on even the prior hearing that your committee held, are working towards better training.

But the reality is that we need to continue to see that happen more rapidly, because those cyber threats continue to evolve, as well.

Mrs. NAPOLITANO. Well, that is everyday security. We are having 1,000 or more security threats a day. Certainly, we can train people what to look for, initially, without having to wait months for training.

Mr. MARINOS. That is a very important point, Congresswoman. It is about elevating the entire cybersecurity awareness of the Nation. The reality is that, until we do that, the bad guys are going to continue to exploit those that have the least knowledge and expertise in this area.

Mrs. NAPOLITANO. So, what are your biggest concerns in the area?

Mr. MARINOS. Well, I think first and foremost is making sure that the support that Federal Government agencies is providing is the right one, and that means doing more to assess what the actual risks are to the specific sectors, and then reflecting that in actual plans that they can execute.

Mrs. NAPOLITANO. Would that be EPA's responsibility?

Mr. MARINOS. That would be EPA's. It would also be the Department of Homeland Security within CISA.

We are still waiting to see a National Infrastructure Protection Plan get updated, hoping to see that in the next couple of years. But unfortunately, sectors can't wait to do that themselves.

Mrs. NAPOLITANO. Well, we should promote some kind of movement to immediately start assisting the agencies that have no way of knowing what to look for.

Mr. MARINOS. Well, actually, Congresswoman, you have done that in law. So, Congress did pass a law that tasked GAO with evaluating how effective Sector Risk Management Agencies are in fulfilling their statutory responsibilities. So, we will be reporting back to you in the near future.

Mrs. NAPOLITANO. Yes, but many agencies are too small. They don't have personnel that are either equipped or trained, and they may not know that the new law exists, and it would help in being able to help them identify. So, we need to go down to the grassroots, to the smallest of the small.

Mr. MARINOS. I would agree. I think a better—not only better information about what the expectations and responsibilities are, but also what offerings the Federal Government can provide through CISA, through EPA, and others to those operators that need the help is very important.

Mrs. NAPOLITANO. Well, with the Army Corps' oversight over the dams, I think they should be part of it, too.

Mr. MARINOS. They are part of the sectors that have been identified. So, responsibilities do carry forward to the agencies that have responsibilities for dams, as well.

Mrs. NAPOLITANO. Thank you very much for your concern, and I look forward to talking to you later.

Mr. Chairman, I yield back.

Mr. CARSON. The gentlelady yields back.

Mr. Davis?

Mr. RODNEY DAVIS. Thank you, Mr. Chair.

First, Ms. Newhouse, we understand that TSA will soon release security directives for passenger rail, freight rail, and rail transit operators.

But unfortunately, though, we have heard concerns about the development of these directives from stakeholders, not the TSA, including from the freight rail industry. And that was at our previous hearing on cybersecurity and in a November 4th letter from the American Public Transportation Association, which, Mr. Chair, I ask unanimous consent to insert into the record.

Mr. CARSON. Without objection.

[This letter was submitted for the record by Hon. Eric A. "Rick" Crawford on page 179.]

Mr. RODNEY DAVIS. Thank you.

Ms. Newhouse, it is good to see you again. I can't wait to see you all in person.

Unfortunately, the TSA failed to provide this committee with advance notice of this, despite that you were coming here the same week to discuss these same cybersecurity issues. Committee staff even asked and were essentially told to wait for official congressional notification, despite what we knew of other committees receiving advance notice.

After back-and-forth by staff, I am told we received an embargoed copy at 9:25 a.m. this morning, which really doesn't give our team or us any time to meaningfully review, and actually figure out what important questions we might have for you today to ask you about it.

Further, the letters attached indicate that the directives were actually issued yesterday, December 1st, which was—I just want you to take a message back, Ms. Newhouse, that this committee—because we, obviously, have some jurisdiction over the issues we are talking about today, otherwise you wouldn't be here—we expect to be notified of actions that your agency is going to take, just like other committees get that notification.

If anything you are doing is going to affect the modes of transportation, and the safety of those modes of transportation, and the areas that we have jurisdiction over, we expect to be notified here. I mean, we are one of the largest committees in Congress. Can you please make sure you send that message back to your colleagues, and take that message back to TSA, too? Because we are pretty frustrated. And frankly, these are issues that I think we all ought to work together on, and—instead of have a minimal amount of time to be able to address them.

But thank you, it is great to see you. I hope to talk to you again in the future, and I look forward to our next meeting.

Mr. Marinos, it is my understanding that the GAO is in the process of completing its annual report on cybersecurity and surveillance threats to Congress. In undertaking this assessment, how has GAO pursued access to House and Senate cybersecurity data, and how does the GAO plan to ensure that information about Congress' cyber posture remains secure?

Mr. MARINOS. Well, first, Congressman, I just want to say that we appreciate Congress tasking us with this important review, and we take the responsibility of performing it very seriously.

In terms of how we are protecting the information, we recognize that the information that we have been asked to review is very sensitive, but we also have a very long, successful track record of handling and protecting sensitive information that we receive from Government agencies, and also from industry. And we will, obviously, apply the most rigorous protections that we can to the information that we that we receive.

Mr. RODNEY DAVIS. Well, as you can imagine, access to House data is something that we all—Republicans, Democrats—guard very closely. However, we also recognize GAO's expertise in this area, and hope congressional entities are cooperating so that we achieve the desired aim of the annual report. So, thank you, again.

Another question, Mr. Marinos. We have seen attacks on our critical infrastructure, including the one earlier this year on the

Colonial Pipeline, as mentioned in earlier testimony. Monitoring is critical to thwart future attacks. However, monitoring is not the end of what our efforts should be, and we should have a layered approach to cybersecurity, especially when protecting our Nation's most vital infrastructure assets.

Can you tell us—and this may be a question for DOT also, Mr. Schachter—what is the Department of Transportation doing to fortify our critical assets in the field, such as air traffic control towers, pipelines, and railroads, that are carrying hazardous materials or passengers, so that they can operate effectively when malicious actors have already compromised the integrity of the network?

Let's just go to you, Mr. Schachter. Can you answer that with the time I have left?

Mr. SCHACHTER. Sure. Thank you very much for the question.

So, DOT, in each of the areas that you mentioned, is working with our private-sector partners to improve their cybersecurity practices. And, as stated before, our cooperation through TSA to those private-sector partners, we act as co-sector risk management officials in those areas. So, we need the participation from all of those parties to become more cyber secure.

Mr. RODNEY DAVIS. Well, we continue to offer to work with you on these endeavors. And I apologize for mispronouncing your name earlier, Mr. Schachter.

Thank you all for being here today, and I yield back the balance of my time.

Mr. CARSON. The gentleman yields back.

Mr. Johnson?

Mr. JOHNSON OF GEORGIA. Thank you, Mr. Chairman, and thank you to the witnesses for your time and your testimony today.

During part 1 of this hearing, we learned how our critical infrastructure remains vulnerable to cyberattacks. And in October of 2021, the DOT's OIG released a report on the Federal Transit Administration's cybersecurity weaknesses, which found that weaknesses in FTA's financial management systems could affect its ability to disburse COVID–19 funds.

In Atlanta, the Metropolitan Atlanta Rapid Transit Authority has been anticipating $284 million in emergency funding, which is critical to the mobility of our residents, especially communities of color and essential workers who disproportionately depend on transit to get to work and school. My constituents can't afford a delay in funding because of a cybersecurity incident.

The OIG report notes that the FTA has failed to fix weaknesses that have been known since 2016, a total of 5 years. While the delay is not unique to FTA, it puts us all at risk. Mr. Dorsey, why has FTA moved so slowly to implement security control fixes?

Mr. DORSEY. Thank you for your question, Congressman.

We have worked with the Department for a number of years regarding the various cybersecurity weaknesses that we have identified through our reviews of the various—what we call system-level reviews. And with respect to FTA, what the Department had informed us was the fact that they had accepted the risk for a number of reasons regarding why they had these longstanding weaknesses.

One of the reasons was primarily because they said they had to get the proper guidance at the Department level, with respect to addressing some of the weaknesses.

Another reason was the fact that they had stated that they were concerned about decommissioning their systems or upgrading their systems for the fear that the systems needed to be operational 24/7.

With those issues in mind, we decided to report out on those particular weaknesses. And what the FTA decided to do, after we had reported out, they indicated to us that they would take the immediate actions to address our concerns.

Mr. JOHNSON OF GEORGIA. Well——

Mr. DORSEY. However, regarding the vulnerabilities associated with the 6 years or so associated with outdated databases, the Department had indicated——

Mr. JOHNSON OF GEORGIA. Well——

Mr. DORSEY [continuing]. They would provide us with a response by 2023.

Mr. JOHNSON OF GEORGIA. Well, let me ask you, is there anything that Congress needs to do to ensure that FTA maintains better control over their cybersecurity?

Mr. DORSEY. I believe what Congress can do is work with the Department, and maybe provide a sprint initiative, if you will, and require them to make sure they prioritize the implementation of what we consider to be some of the most significant cybersecurity weaknesses that we have identified over the years, and make sure that they follow up with Congress and report on their attempts and efforts to address those weaknesses.

Mr. JOHNSON OF GEORGIA. Thank you.

Mr. Schachter, as the chief information officer at DOT, you lead on IT and cybersecurity issues. How can you ensure that DOT's component agencies, such as FTA and FAA, have the resources, capabilities, and leadership to correct current cybersecurity deficiencies, so that cities like Atlanta are not detrimentally impacted?

Mr. SCHACHTER. Well, thank you very much for that question.

And as I specified in my testimony, cybersecurity is our number-one priority. And I highlighted three areas that we are prioritizing within that to take immediate action: the first is access control; the second is website security; and the third is governance and coordination across DOT. All of those issues are impacted, involved in the situations that you mentioned and Mr. Dorsey has mentioned.

We have created cyber sprints, that I also referenced in my testimony, as a way to expedite improved performance in all of these areas. And I believe we will be able to report back to you later this year that we have made significant improvements.

Mr. JOHNSON OF GEORGIA. Thank you. My time is up, and I yield back.

Mr. CARSON. The gentleman yields back.

Mr. Babin?

Dr. BABIN. Sir, thank you, Mr. Chairman. As I said the other week, when we had witnesses from the private sector here, I am so glad that we are having this hearing, and prioritizing this very important topic, for this committee to weigh in on the issue of cybersecurity in the transportation and critical infrastructure space.

It is a great responsibility, and one we should all take very, very seriously.

It is also a very timely topic. Right before we went home for Thanksgiving, the Director of CISA told the House Homeland Security Committee that “ransomware has become the scourge on nearly every facet of our lives, and it’s a prime example of the vulnerabilities that are emerging as our digital and our physical infrastructure increasingly converge.” She went on to say that, “The American way of life faces serious risks.”

She is right. internet attacks are a full-fledged standard feature of our modern-day life. Hardly a day passes anymore without a media story breaking about a cyberattack, or at least a threat. These threats are disruptive, costly, and potentially life threatening. All of us saw what happened with the Colonial Pipeline breach last May, and how the attack led to gas shortages and interrupted supply chains.

There is certainly a legitimate and appropriate role for us in the Federal Government to play in protecting the American people and our companies and businesses against theft, espionage, and cyberattacks. No question that each of you testifying here today are fighting for our national security. However, as you all know, cyber intrusions are very hard to track.

We have got to be extraordinarily careful, as lawmakers, and as rulemakers, that we don’t meddle in something that we don’t properly understand, and unintentionally create more bloated regulation, or stifle innovation with overly burdensome requirements that don’t truly secure our infrastructure. Any policy that we push forward has got to be aggressive, but consistent with our Nation’s founding principles. Meanwhile, we provide for the common defense, while at the same time protecting civil liberties and free economic markets.

Former Director of National Intelligence, and my former Texas colleague and classmate, John Ratcliffe, said that we need to attribute these attacks and either overtly or covertly retaliate against those responsible, thereby creating a deterrent for the future. If our long-term strategy to cyber criminals is just to simply pay the ransoms, and hope for the best with cyber insurance, we will certainly lose to our foes in this new battlefront.

So, my question for you all is this, and I will open this to anyone who would like to answer, time permitting: What are some commonsense steps we, as lawmakers, can take to help you, our partners in the executive branch, better protect our infrastructure, and to encourage better reporting of cyber threats without infringing on people’s civil liberties and the free market? I will open that up.

Mr. SCHACHTER. Thank you for that——

Admiral MAUGER. Congressman—go ahead. I will yield to my colleague at DOT.

Dr. BABIN. OK. Then, Admiral, you can come on second. Thank you.

Mr. SCHACHTER. Thank you, Congressman. Thank you, Admiral, I will try to be brief.

I think your—one, a summary of your statement, Congressman, is that cybersecurity is everyone’s responsibility, public sector and private sector, and we are all going to either succeed or fail at this together.

And I think, from a congressional standpoint, it is understanding that new systems, or improvements to existing systems, need to be secure by design, and created with cybersecurity in mind. That is step 1. That would help us achieve our objectives. Thank you.

Dr. BABIN. Thank you.

Admiral?

Admiral MAUGER. Congressman, thank you. I support the comments made by Mr. Schachter there, at DOT. What I would offer, as well, though, is that we have to treat cybersecurity as an operational imperative, and it has to be part of an overall risk management approach within—about the private sector and the Federal Government.

And so, I think that in order to achieve that, you have to have an accountable person, they have to be able to do an assessment, and understand the risks. They have to be empowered to manage those risks. And then it also comes back to exercising and reporting.

When it comes to reporting, right now we have to change the paradigm from "what is the minimum I need to disclose?" to "how can I help protect others?" Because, as we've heard through testimony already, these incidents cut across so many different infrastructures, and reporting really helps us to make us all stronger, Congressman.

Dr. BABIN. Absolutely. Thank you so very much. And I hope that we will remember retaliation can curtail some of this.

I will yield back, Mr. Chairman.

Mr. CARSON. The gentleman yields back. At this time, I will yield to myself.

Mr. Grossman, the aviation sector is composed of aircraft, airlines, airports, and aviation operators, such as air traffic control personnel and ground crew. As you know, it's a mix of private-sector companies and public agencies, including the FAA. However, a cyberattack on one portion of this sector can have cascading effects on the entire system, with devastating impacts to the public.

Can you describe, from a cybersecurity perspective, how the FAA assists and supports the aviation sector?

Mr. GROSSMAN. Absolutely, thank you for that question, Congressman. The FAA engages with industry on several fronts. We are a regulator and a collaborator.

So, from a collaboration perspective, we engage with much of the aviation community through efforts like the Aviation ISAC, which we are close partners with; the Aviation Sector Coordinating Council; manufacturer associations; and, of course, through our primary engagement, the ACI, the Aviation Cyber Initiative. In these engagements, we share best practices and standards, guidance, and we promote information sharing.

As a regulator, we work directly with manufacturers and [inaudible] standards to assure that these two are kind of married up, and so folks are using industry standards, and are building products that are appropriate.

Mr. CARSON. So, in defending the aviation sector from various cyber crimes, do you believe it is important to coordinate and even cooperate with the private sector to assist them?

Mr. GROSSMAN. Well, I think, as Mr. Schachter mentioned earlier, cybersecurity is a team sport, and we are all in this together. The public and private sector work together, which is really why we formed the cyber initiative for aviation itself, across the entire ecosystem, so we can work more collaboratively with operators, manufacturers, and other agencies. Private and public sectors work together to share information and to try to improve the resiliency of the ecosystem.

Mr. CARSON. So, this is for the entire panel: Where do you see the biggest cyber threats coming from, from specific actors like the recent attacks on local government entities with ransomware, from foreign entities, from nonstate actors?

Are there significant threats from even some of our own weaknesses, like our failure to update and strengthen our cyber infrastructure, or poor cyber hygiene, and failure to apply strict cybersecurity protocols?

What are your insights?

Mr. GROSSMAN. Well, Congressman, I think you just listed them all. I don't know that any of us—I don't want to speak for the rest of the panel—would highlight one over the other.

We are all aware of the recent compromise of SolarWinds that occurred last year, but there are other threats out there. And I think that compromise is certainly still fresh in our minds. But, I wouldn't choose that actor over other actors or other vulnerabilities, if you were asking me which is worse.

Mr. MARINOS. But I would like to just mention that—I think it has come up several times, both from the witnesses and from the congressmen, as well—it is the interdependencies between the critical infrastructure that make this so challenging.

So, we are talking about transportation, and transportation not only relies on other sectors to operate effectively, but other sectors rely on it, as well. We issued a report just last month on the communication sector, and the transportation sector was one of those sectors that had been identified by CISA as one it depended on. In other words, it could not operate without it.

And so, I think the challenge there is, while there is resiliency built in, in many ways, to physical attacks, the cyberattacks continue to show us that we need to do more to not only shore up specific sectors, but the entire Nation's approach to cybersecurity, as well, which is why we emphasized in our recent work the importance of having a national cyber strategy, so that it can be an all-in-Government effort to elevate our cyber capabilities within the Nation.

Mr. CARSON. Thank you. Thank you all.

Mr. Graves of Louisiana?

Mr. GRAVES OF LOUISIANA. Thank you, Mr. Chairman. I appreciate the witnesses testifying today, and I appreciate the importance of this topic. We have offered a number of amendments trying to increase funds for different cybersecurity programs related to infrastructure, and I think this is critically important.

Ms. Newhouse, and perhaps Admiral, your testimonies discuss information sharing between TSA and the Coast Guard to identify and manage threats in the maritime transportation system. How do you communicate the threats to the individual ports, and how do you help to manage risk within the MTS?

Admiral MAUGER. Congressman, thanks for that question. So, unity of effort within the Coast Guard is part of our DNA, and so we take a multilevel approach to share information at the speed of cyber here, with the industry. But this is a dynamic threat environment. And going forward, we need to use a combination of both existing tools and new tools, or new methods, to get after the information sharing.

So, for this multilevel approach at the local level, we work through our Area Maritime Security Committees. Each of those have established cyber subcommittees that are responsible for that day-to-day sharing of information, for conducting the exercises, for reviewing best practices, and understanding how to move forward. Those same people, then, are integral to response efforts when they occur in the ports.

At the national level, we work through a number of different means. We have established a Maritime Cyber Readiness Branch within our Coast Guard Cyber Command that really becomes a focal point for threat information, dissemination, technical assistance to the field, and connection to the interagency. We have embedded folks in CISA. We meet regularly with the other Sector Risk Management Agencies. We engage with the MTS Information Sharing and Analysis Center, and we look for every opportunity to continue to share information, communicate threats, and understand the vulnerabilities in this industry, so we can protect the MTS.

Mr. GRAVES OF LOUISIANA. Thank you.

And TSA, anything to update there?

Ms. NEWHOUSE. Thank you, Congressman. And to complement Admiral Mauger's information, I would like to say, yes, the United States Coast Guard has primacy in our Nation's ports. However, TSA plays an important role to support the security of the maritime transportation system.

To that end, we have, actually, developed the TSA exercise training program, which started, frankly, as a port STEP, Security Training and Exercise Program. It started in the maritime sector in the mid-2000s. We have grown that training and exercise program across all modes of transportation.

The U.S. Coast Guard is an important partner, where, as Admiral Mauger mentioned, we can actually exercise at both a national and a local level. And if an entity is not able to participate, we do maintain all of those lessons learned and exercise information in accessible systems to thousands of local operators, first responders, and those law enforcement professionals who support the security of the Nation's ports and other transportation modes.

Congress also generously chartered the Surface Transportation Security Advisory Committee a few years ago. Amongst the members includes, obviously, our stakeholders, our private-sector stakeholders representing a multitude of interests across all surface transportation modes. However, we also have 14 Federal agencies that also serve on that committee as nonvoting, contributing members, so our——

Mr. GRAVES OF LOUISIANA. Ms. Newhouse? Ms. Newhouse, I think my concern is, if we have a very active, very live incident, the ability to quickly communicate and disseminate that information with the ports, I am not sure that the security committees or the apparatus that you are describing allows for that direct and sort of nimble communication to the ports and other potential threatened entities out there. And that is where my concern is.

I just have about 45 seconds left, I wanted to ask one other question of the Coast Guard, and then I am going to follow up with you all through questions for the record.

Admiral, can you tell me whether or not you all are working with FEMA to update the NIMS system to be able to track and follow through on cyber incidents?

Admiral MAUGER. Congressman, in terms of, first of all, communication with the ports, we have 24-hour watches that have access to the information and share that information. But I look forward to your questions, and followup questions.

With regard to incident response, we stand up at the local level a unified command, which is a structure that was established under NIMS to be able to respond to incidents. And we can be happy to provide more information about that, and follow up, or later during this hearing, if you would like.

Mr. GRAVES OF LOUISIANA. That would be great. And maybe NIMS isn't the perfect system, but it seems like there needs to be some type of mechanism like that for tracking accountability.

Thank you, Mr. Chairman, I yield back.

Mr. CARSON. The gentleman yields back.

Ms. Titus?

Ms. TITUS. Thank you very much. I would like to go back and follow up on some of Mr. Carson's comments about coordinating with the private sector.

Mr. Grossman, you mentioned the ISAC, I think. One area that you all didn't talk about, the coordination, is in commercial space. We have been hearing a lot about these billionaire joy rides to outer space, but we know that is an important industry, it can help us take products up to the space station, or launch satellites, so a good potential use there. And there are a variety of companies that are starting to get into this. And I think that that increases the potential for cyber threats.

I wonder if you could talk about how these ISACs work; if you are looking at cyber threats, how we coordinate with the commercial space industry.

Mr. GROSSMAN. Congresswoman, thank you for your question. Unfortunately, that doesn't fall under my purview.

However, I understand FAA's Office of Commercial Space Transportation is heavily involved in the development of the space cybersecurity policies and assisted the development of the ISAC and the space policy directive. That directive established key cybersecurity principles to guide and serve as a foundation for the U.S. approach to cyber protection of space systems.

I could certainly follow up with you, though, to get more information on your question, if you would like.

Ms. TITUS. Well, I would appreciate that, because I realize it is not directly under what you do, but you do a lot of things all around that area, and I think it is something that is worth bringing to the attention of the committee, because it is going to become increasingly at issue, as we do more of this private space adventures, I guess.

I would ask Ms. Newhouse—I know you were instrumental in setting up the whole PreCheck program, so you are very informed on how this works, and you got it off the ground, and we have seen it expand now. The line for PreCheck is longer than the regular line, I think.

But one of the things that we have heard in areas that are—rural communities, is that they have a hard time actually coming in person to get the PreCheck clearance, so there is some attempt to move to remote applications. Could you talk about that, and how that data that could be collected remotely can also be protected?

And do you need legislation for that, or is it something you can just do internally, or through regulation?

Ms. NEWHOUSE. Thank you for your question, Congresswoman, and thank you very much for your support of the TSA PreCheck program. We greatly appreciate the insights that Congress and all of our stakeholders give us on a daily basis.

I can say, at a very high level, I do know that the office that runs that program for TSA has endeavored to expand enrollment capabilities, as you mentioned, Congresswoman, and we are actually in progress of bringing on additional contract support, different vendors to do that in a secure manner.

I am happy to get back to you and your staff with specific answers to those questions on how we are best requiring protection of that information, and how we will oversee that information. Thank you.

Ms. TITUS. Thank you. I would appreciate that. So much of our information is shared in an airport, whether it is through TSA, or just plugging in while you are waiting for your flight, or even on the flight itself.

So, I think that, to be sure that this is all secure, information in the screening process—because the trip begins when you get out of the car at the airport. We want that to all work well, and we want people to feel secure that that information can't be compromised. So, I look forward to getting that from you.

And I will yield back, Mr. Chairman.

Ms. DAVIDS OF KANSAS [presiding]. The gentlewoman yields back. The Chair now recognizes Mr. Weber for 5 minutes.

Mr. WEBER. Thank you, Madam Chairwoman. I appreciate that. I want to talk a minute about pipelines. I appreciated Garret Graves's comments about ports, and we will tie these together.

As you all know, the Colonial Pipeline system was hacked into—I think it was May of this year. It was down for 4 or 5 days. It feeds the Southeastern United States, moves about 2½ million barrels of product a day, which is gasoline and jet fuel, diesel, extremely important to our infrastructure, obviously, energy infrastructure; we would argue national security infrastructure, because we are going to need fuel to move our military stuff.

The Keystone Pipeline comes into our district, it is about one-third [inaudible] without any redundancy of the Keystone Pipeline, or more pipeline security stuff—and many of you all probably know pipelines have a 99-percent safety rating [inaudible] all that [inaudible] with them. They move product the most efficiently and the most safely. All that to say that, from an energy perspective, with vulnerability of being hacked, would it sound like we ought to have a system in place to notify either pipeline operators—I would add ports to it, like Congressman Graves did, as well as other ways that we move energy.

Since we have limited time—and I know we talked about doing it at cyber speed, so to speak, but should there be a process in place to where the greatest amount of energy is protected as early on as possible? I don't know. Is that possible?

Mr. Schachter, I go to you. Is that something that sounds, number one, a good idea; and, number two, possible?

Mr. SCHACHTER. Thank you for that question. If I understand it correctly, we are talking about coordination and communication between the private-sector partners that provide the energy, the fuels, the pipeline operators, as well as the Government, in its regulatory capacity.

Mr. WEBER. Correct.

Mr. SCHACHTER. I believe TSA——

Mr. WEBER. And with ports—let me also say ports, too, because, you know, our country runs on—the economy of our country, it is important, runs on trade. So, let's not leave the ports out.

Mr. SCHACHTER. OK. So the same principles will apply in my answer, thank you.

Mr. WEBER. Right.

Mr. SCHACHTER. TSA has moved aggressively to improve information sharing and incident reporting from all of those private-sector actors, and to coordinate with both DOT and other Government regulatory bodies that have an interest in those areas.

As you probably know, ports, as well as the pipelines, are also privately operated, so that we have to work with those private-sector partners, and try to influence them and advise them to improve their own cybersecurity practices to protect their systems, so that they are less likely to be attacked. Some of that is standard IT access control, but it also moves into operational technology, which are very specialized, and outside the realm of DOT information technology.

Mr. WEBER. But if we had a system to catch that—I know we monitor a lot of stuff—and be able to communicate that as quickly as possible—I know there was some discussion about banks here a while—some years back since I've been in Congress—same thing.

But if we had a system in place where we could at least be a—I don't know what the right term is—co-managing partner, or have a process—I am going to move on to the admiral next—whereby, if we know something is in the making, we can alert them as quickly as possible, and thereby protect our infrastructure, in terms of energy, national security, and the marketplace, if you will, Admiral, what do you think? Sounds like a good idea?

Admiral MAUGER. Congressman, intelligence and understanding what is happening to the threat level is really a critical piece of how we collectively protect the Nation.

And so, we have established procedures by which we can share information rapidly, both through the interagency, down to our field units, and, in several cases, with the private sector, through our Area Maritime Security Committees.

What we are also finding out, though, is that this is a very broad problem. And so, it is important that we get together and collaborate at the lowest level possible. CISA has established a Joint Cyber Defense Collaborative that is bringing private sector and the interagency together at a low level to be able to see those threats and challenges as they evolve, and share those out rapidly, and put the mitigations in place. And so, this is an important issue, and we are getting after it.

Mr. WEBER. Well, thank you for that.

And Madam Chair, I cannot see the clock. How much time do I have left?

Ms. DAVIDS OF KANSAS. The gentleman's time has expired.

Mr. WEBER. Well, let me just end with one quick thing for Ms. Newhouse, for the TSA.

If you can prevent the random disappearance of my wife's TSA number on her airline tickets, it would be worth everything to me in Congress.

[Laughter.]

Mr. WEBER. I appreciate what you all——

Ms. NEWHOUSE. Congressman, we are happy to help. If you have any questions, or any Members here have questions about TSA PreCheck or your family members, please let me know, and I am happy to make sure we solve any issues. Thank you.

Mr. WEBER. Thank you so much.

Thank you, Madam Chair. I yield back.

Ms. DAVIDS OF KANSAS. Thank you. The gentleman yields back. Ms. Brownley is now recognized for 5 minutes.

Ms. BROWNLEY. Thank you, Madam Chair. My first question is to Mr. Dorsey.

Mr. Dorsey, in October your office issued a disturbing report about IT security weaknesses at the Federal Motor Carrier Safety Administration. You placed malware in the network, and the agency failed to detect it.

So, I was curious to know, is this a practice that you do in other agencies? Why was this particular agency selected for this exercise? I am sort of curious of the thought process behind it.

Mr. DORSEY. Thank you very much, Congresswoman, for your question.

Throughout our reviews on an annual basis, we have issued a number of audits with respect to our vulnerability assessments and penetration testing work of the Department's IT infrastructure to determine whether or not the Department has established secure practices to protect and secure its IT infrastructure.

Our review of the Federal Motor Carrier Safety Administration was not our first review of the Department's IT infrastructure. As a matter of fact, it was the third review. We initially started back in 2016, and issued a report on Volpe Center, the Department's research arm, and we followed that up with a review of the Department's MARAD association. And Federal Motor Carriers was just the third in a series of reviews that we are planning to do with respect to assessing the Department's security posture at all of its operating administrations. We just initiated another review of the Federal Highway Administration's IT infrastructure.

And what we are doing that for is to determine whether or not the Department is instituting the proper controls, enforcing oversight of their own policies that they have in place, where we have identified, primarily, persistent security weaknesses that has provided us with a path to actually compromise the Department's IT infrastructure.

Ms. BROWNLEY. Did the Federal Highway Administration fare better?

Mr. DORSEY. We just initiated that review. We normally take about 7 to 10 months to complete our review, and we will be reporting out on the status of that review at that time.

But what we have found in the past is just, primarily, persistent weaknesses in basic things, such as lack of strong passwords, unpatched or what we consider to be software that is not updated in various operating systems. We find a lack of encryption in data. And those persistent weaknesses are how we, primarily, were able to penetrate the Department's IT infrastructure.

Ms. BROWNLEY. Thank you, sir.

Mr. Schachter, I know you have only been in the Department—in your opening comments you said you have been there for 3 months. Certainly, 11 years in the city of New York.

And I guess, you know, I would just like to ask you, what grade would you give yourself at this particular point? Would it be an A, a B, a C, a D, an F? How would you grade yourself right now?

Mr. SCHACHTER. Well, thank you for the question. I don't have enough information yet to provide that sort of an assessment.

What I can tell you, and as Mr. Dorsey mentioned, some of those audit findings do go back to 2016, before DOT created a central operating environment for the purpose of addressing, across DOT, some of the very same findings that OIG found in multiple modes related to access control, vulnerability in patch management. That the common operating environment gives us much better tools to provide that security across all the modes at DOT who use this common operating environment.

So, our performance has already improved, but we have a ways to go. And we are transparently acknowledging that, as I did in my opening statement.

Ms. BROWNLEY. And——

Mr. SCHACHTER. And I think, as—pardon me?

Ms. BROWNLEY. Well, I just wanted to go on to another question, because I only have a few more seconds left.

Mr. SCHACHTER. Sure.

Ms. BROWNLEY. So, you have also mentioned limited resources several times in your answers today. And so, I am wondering, do you have enough resources to do what you think you need to do?

And, if not, are you planning on making further budget requests in the 2023 budget cycle?

Mr. SCHACHTER. Thank you for that question, as well. I am still too new to the position to fully assess whether we have sufficient resources, as needed to address this, or the resources in the right place, or with the right expertise. And I expect, before too long, to be able to share that information.

Ms. BROWNLEY. Thank you, sir. My time is up.

Madam Chair, I yield back.

Ms. DAVIDS OF KANSAS. Thank you. The gentlewoman yields back. The Chair now recognizes Mr. Burchett for 5 minutes.

Mr. BURCHETT. Thank you, Chairlady. This is for Rear Admiral Mauger.

How do you say your name, sir? Is it Mauger or Mauger?

Admiral MAUGER. It is Mauger, Congressman, thank you.

Mr. BURCHETT. All right, all right. And you can call me Tim. Semper paratus, I believe, is your all's motto, if I am correct.

I am really concerned about the Russian efforts to target the undersea fiber optic cables that carry 99 percent of U.S. communications abroad, many of which are operated by private companies.

I understand that a lot of information about our undersea cable system is classified, but, given the Coast Guard's role in protecting the Marine Transportation System, can you comment on our Nation's ability to prevent and respond to cyberattacks against our undersea cable infrastructure?

Admiral MAUGER. Congressman, our maritime transportation critical infrastructure is varied, and it is dependent on other modes of critical infrastructure.

And, as you have highlighted, there are very substantial threats against the maritime critical infrastructure every day. And so that is why we have put together an—that is why we have operationalized our cybersecurity and made it part of our prevention and response framework, to make sure that we are getting after this threat at the speed and pace at which it demands.

I can offer you a followup brief with regard to cables, if you would like, sir.

Mr. BURCHETT. I would really like that.

Just out of curiosity, how many ribbons are on your chest?

[Laughter.]

Admiral MAUGER. Congressman, actually, I don't even know how many ribbons are on my chest here, so——

Mr. BURCHETT. That is very——

Admiral MAUGER. Maybe I can get you that answer for the record.

Mr. BURCHETT. That is all right. No, it is very distracting, but I think it is pretty cool. Thank you, brother, for serving our country.

I will always remember a buddy of mine, Ron Eisenberg, back home, who is a Coastie, and I always remember at the Veterans Day celebration, that everybody gets up and sings their Service anthems, or whatever, and my daddy was an old Marine Corps—so he would sing the Marine Corps hymn. And there is always just one Coastie in all of Knox County that would get up and sing, and he would just scream it out in the back, because he would be by himself. And I always thought that was pretty cool. But thank you.

Hey, this is for Ms. Newhouse at the TSA. I won't get after you for the terrible service sometimes I see people get, because in Knoxville, Tennessee, actually, the group is pretty good. I always gripe about the one up here, in DC, which is, in my opinion, pretty lackluster.

But a couple of months ago the TSA announced plans to issue new cybersecurity regulations for rail and airline companies. Now, how much time did your all's agency give the impacted stakeholders to respond and provide feedback on those directives?

Ms. NEWHOUSE. Thank you, Congressman. And thank you for recognizing our fine transportation security officers, particularly in Tennessee. We are very proud of them, and they are, frankly, amongst our top-performing airports and officers in the country. So, thank you for that compliment.

With respect to the rail and higher risk rail and rail transit directives, along with the aviation security program changes, actually, we have followed a very robust rubric of engagement. I will give you an example. For aviation, we utilize existing security requirements and programs, and provided ample notice and comment, both verbally and in writing in multiple sessions.

And we have also, as I mentioned in my opening to Congressman Crawford, we have taken that feedback and updated definitions of a reportable cybersecurity incident. So, we have taken that seriously.

With respect to my rail partners, as I mentioned earlier in my testimony, we have embarked on a robust engagement at the CEO level, starting with Secretary Mayorkas, Administrator Pekoske, amongst many other DHS senior officials along with our CISA partners, to engage both at the classified level and the unclassified level to describe the known, ongoing, and persistent threats that are driving these policies.

We then provided written copies to the regulated parties to have an opportunity to review these, albeit in certain circumstances we do need to act swiftly, given the persistent threat. However, what we have done, and particularly over this last month, I can personally tell you from my office, the standpoint, we have engaged extensively over these last 4 weeks and have been updated, based on those feedbacks, particularly from our rail partners. Thank you.

Mr. BURCHETT. Has your agency received any concerns from the stakeholders about how the upcoming cybersecurity directives would impact their current operations?

Ms. NEWHOUSE. Thank you, Congressman. Yes. Everything we do every day is about continuous improvement, and one of those areas of continuous improvement is to, first, do no harm and, actually, complement operations while securing those operations.

So, we have heard a number of concerns to ensure that all operators, large and small, can apply these cybersecurity measures in an effective and efficient manner. So, we do take that into consideration, and we continue to solicit feedback. We are not just done when we issue the documents. It is a continuous feedback loop and improvement.

Mr. BURCHETT. Thank——

Ms. NEWHOUSE. And we stand committed to that.

Mr. BURCHETT. Thank you. I have run out of time.

And I yield none of my time back to you, Chairlady. Thank you.

Ms. DAVIDS OF KANSAS. The gentleman yields. The Chair now recognizes Mr. Payne for 5 minutes.

Mr. PAYNE. Thank you, Madam Chair.

And Ms. Newhouse, I am going to contact you outside of this hearing with some respects to PreCheck at Newark International Airport. I received some documents from flyers that flew into Newark that had an issue with the PreCheck. But I will do that at a later time.

Under the Rail Safety Improvement Act of 2008, Congress mandated railroads that carried hazardous materials and passengers to install Positive Train Control systems. Positive Train Control systems work to prevent unsafe movements and accidents by using an information network to regulate trains' positions.

Can you elaborate on the new TSA directive concerning cybersecurity in passenger and freight rail?

And how will this directive help secure PTC systems?

Ms. NEWHOUSE. Thank you for your question, Congressman, and we look forward to receiving the inquiry regarding TSA PreCheck. We are happy to help.

With respect to the new rail security directives—and we have just worked with our partners to implement—it really—with respect to Positive Train Control and any other operational or informational technology systems, those directives apply to all of it.

And, if I may, we have focused very heavily on reporting. We have to know what—even anything that could, really, reasonably impact those operations, whether it is PTC or other IT or OT systems. So, the early warning and indicators are critical. So, that is part of the strategy with these new directives, is to designate that coordinator, have a 24/7 availability to report those incidents to CISA.

As Admiral Mauger mentioned, CISA has a—what we call a clearinghouse. This is central. In addition to multiple—and we don't forestall any other reporting requirements, or reporting channels that operators may have to independent operating agencies, but CISA is central, CISA is the center of the United States Government—to maintain that information, and disseminate it fast. It can go at the national level down to the local level.

Again, with respect to any IT and OT system, we are requiring these rail operators to develop a cybersecurity incident response plan. We are working with them. We are doing that in concert with all of the modal administrations at DOT. We want to make sure that our folks in the field, as you are well familiar with them, have that information, and have that at hand.

Mr. PAYNE. Yes——

Ms. NEWHOUSE. Back to—we are asking the operators to conduct self-assessments, and identify vulnerabilities and gaps, and have us help them close those gaps. Thank you.

Mr. PAYNE. Thank you.

Mr. Marinos, good cyber hygiene is critical to keeping our cyber transportation infrastructure safe and operational. Federal agencies must not be exempt from adhering to cyber hygiene standards.

As chairman of the Railroads, Pipelines, and Hazardous Materials Subcommittee, I have a responsibility to ensure that the Federal Railroad Administration meets the evolving threat of cyberattacks. How can Congress better assist agencies such as FRA to develop and keep good cyber hygiene practices?

Mr. MARINOS. Congressman Payne, I think the best method of doing that is your continued support of the inspectors general community, as well as to GAO and the audits that we conduct. It is extremely helpful, and productive, in particular to have Congress' support, not only during our audits, but also following them, when it comes to recommendations that we have made. And so, we are grateful for that support.

I think the important thing when it comes to, in particular, smaller entities, is to ensure that those departments and agencies that they are part of have the capability to monitor the performance themselves. And likewise, at the more central level, OMB and the Federal CIO and Federal CISA offices are doing everything they can to, likewise, give feedback to big and small agencies in what they need to do to get better at cybersecurity.

Mr. PAYNE. Well, I thank you for that answer.

And, Madam Chair, I will yield back.

Ms. DAVIDS OF KANSAS. I thank you, the gentleman yields back. The Chair now recognizes Mr. Balderson for 5 minutes.

Mr. BALDERSON. Thank you, Madam Chair. My first question is to Mr. Grossman.

Mr. Grossman, good morning, first of all. Last year, the GAO offered six recommendations to the FAA to strengthen its avionics cybersecurity oversight program. The GAO report found that evolving cyber threats and increasing connectivity between airplanes and other systems could put future flight safety at risk if the FAA doesn't prioritize oversight.

Can you discuss what the FAA is doing to ensure these networks and systems are secure from cyber threats?

Mr. GROSSMAN. Good morning, or good afternoon, Congressman, thank you for the question.

Yes, FAA looks at, really, at the whole system of the airplane, once avionics equipment is installed, to assure that there is proper procedures and protections.

The avionics GAO audit that you referenced, the GAO issued six recommendations. We have already proposed closure on two of those. Three of those are scheduled for closure in March. And just one we have not concurred with. So, we welcomed that audit, and made some significant changes.

Mr. BALDERSON. OK, thank you. One of the recommendations that the GAO made, which the FAA did not concur with, was to consider revising its policies and procedures for periodic independent testing. Can you discuss why the FAA disagreed with this recommendation?

Mr. GROSSMAN. Absolutely, sir. It was independent testing on aircraft that are currently flying in the fleet today, and we were concerned that independent testing—or penetration testing is how we had discussed with the GAO—on aircraft that are in the fleet, that are active aircraft, could leave residual damage to the avionics systems, affecting safety.

Mr. BALDERSON. OK, thank you. And I have one more followup for you: Has the FAA developed an avionics cybersecurity training program?

Mr. GROSSMAN. An avionics cybersecurity training program?

Mr. BALDERSON. Yes.

Mr. GROSSMAN. I am not aware of what we have developed, but I can certainly look into that and get back to you.

Mr. BALDERSON. Thank you very much, I appreciate it.

Mr. Marinos, thank you for joining us this afternoon. In December of 2020, GAO reported that none of the 23 agencies in its review had fully implemented key foundational practices for managing information in communications technology supply chains.

Since 2010, GAO has made nearly 80 recommendations to enhance infrastructure cybersecurity. As of November, nearly 50 of those recommendations have not been implemented.

While we don't have time to go over all of these recommendations, could you please discuss which of these unimplemented recommendations should be given priority?

Mr. MARINOS. Yes, Congressman. I appreciate you pointing out the importance of the recommendations that we have outstanding.

In addition to the recommendations that we made within that specific avionics report that you mentioned earlier in your questioning, I believe that the top recommendations with respect to critical infrastructure include making sure that Federal agencies that have sector-specific responsibilities are doing everything they can to assess what the cyber risks are to their respective sectors; put forward plans with stakeholder engagement that makes sense on how they are going to support those sectors; and then execute.

To put it very carefully, most of those recommendations really expressed that in a variety of different ways across sectors that extend beyond transportation to include things like the grid, K through 12, financial services, and other sectors, as well.

We also think it is very important for CISA to continue its effort to reach its full potential. When Congress passed a law in 2018 establishing CISA, the agency that grew out of NPPD took on a large set of activities that it had challenged itself to complete by the end of 2020.

Unfortunately, a report that we issued earlier this year showed that they were not able to achieve quite a few of the important activities related to workforce planning, incident response, identifying essential functions. These are activities that CISA needs to complete as quickly as possible, and we have heard from CISA that there is intent to do many of those things, either by the end of this year or next. The urgency is there for that organization to gain its full potential to be able to provide support, both to infrastructure and to Federal agencies, as well.

Mr. BALDERSON. OK, thank you very much.

Madam Chair, I yield back.

Ms. DAVIDS OF KANSAS. The gentleman yields back. The Chair now recognizes Mr. Malinowski for 5 minutes.

[Pause.]

Ms. DAVIDS OF KANSAS. It looks like Mr. Malinowski might not be on.

Mr. Carter, you are now recognized for 5 minutes.

Mr. CARTER OF LOUISIANA. Thank you, Madam Chair. I greatly appreciate the opportunity. Thank you so much to our participants.

Mr. Marinos and Mr. Dorsey, both of your organizations have provided a lot of oversight of Federal Government cybersecurity strengths and weaknesses. Have either of your organizations looked at how prepared or vulnerable agencies are to potential cybersecurity attacks, specifically around the time of natural disasters?

As you know, my district in Louisiana suffered a substantial storm, one of the largest ever. And my fear is, as we know, that hurricanes come every year, the intensity increases, and my fear is that our critical infrastructure is particularly vulnerable during those periods.

Can you share with me your thoughts on ideas and/or practices to protect our critical infrastructure during natural disasters?

Mr. MARINOS. Yes, I would be happy to, Congressman. And I think that you noted in the previous hearing that the National Association of State CIOs had also identified that as a real threat. And so, I think it does speak to just how important it is to consider, not only when we can be strong at our most resilient state, but also at our weakest points, which can come often with natural disasters.

What I would say is, over the course of the last several decades, GAO has been tasked by Congress to look specifically at how Federal agencies are preparing themselves for man-made or natural disasters through continuity of operations activities. And a key part of continuity planning is to ensure the continual availability of information, and you can't do that without thinking about cybersecurity, as well. I think that is probably a very important part of looking at any cybersecurity program at a Federal agency, is its ability to recover from disasters.

I am not sure if Mr. Dorsey may have more specific DOT-related examples to provide, but I am happy to pass it over to him.

Mr. DORSEY. Thank you for the question, Congressman. And thank you, GAO.

I just wanted to say that we have just recently initiated a review of the Department's high-value assets. And what we found is that the Department's high-value assets program is heavily reliant on the Department of Homeland Security efforts to work with the Department in assessing the Department's high-value assets.

The Department has identified 21 high-value assets. From our understanding, there have been at least four assessments since the Department of Homeland Security has actually initiated its review of DOT's programs, and we are planning to continue our work over the next several months to determine what the actual governance process is that the Department has in place, as well as whether or not they are actually taking the initial steps required to assess and remediate the potential for a threat of any of those high-value assets. And——

Mr. CARTER OF LOUISIANA. How do you disseminate that information with local governments or States, so that they are equipped for future instances?

I understand you guys have several practices or studies that are ongoing, trying to determine best practices. How do you disseminate information so local governments are prepared, are better prepared?

Mr. DORSEY. Our job is primarily to report directly to the department heads, as well as Congress. And how that information is disseminated down to the State and local level, I don't have——

Mr. CARTER OF LOUISIANA. Mr. Marinos, could you respond to that, sir?

Mr. MARINOS. Yes, sir. I think that falls on the shoulders of CISA. We have seen CISA develop its capabilities, especially when it comes to the support it can provide to State and local governments, and to owners and operators that may not have capabilities to do things like assess their own capabilities. Those are offerings and services that CISA has.

One thing that we have seen is an important need for CISA to continue its outreach across the board, whether they are big or small operators, so that there is awareness about what the Federal Government can do ahead of time, so that it can prepare itself to be resilient in the event of a situation like you describe, where natural disaster may coincide with a cyberattack.

Mr. CARTER OF LOUISIANA. It would be very helpful if you would share with us information that we might be able to share with our local governments and States on what to do in the case of hurricanes or wildfires.

You can imagine the devastation if someone took control of our apparatus, and we were not able to dispatch emergency EMS or fire equipment. These are real-life issues that, unfortunately, are becoming far too frequently experienced with local and State governments.

So, thank you very much for your time and attention. Any information that you can share with us on how we, as a committee, can do better, or push buttons further to provide resources or awareness so this information is gotten out, and we are able to be prepared for future instances, as we know, unfortunately, they are becoming far too common.

I yield back, thank you.

Mr. AUCHINCLOSS [presiding]. The gentleman yields. The Chair recognizes Mr. Fitzpatrick for 5 minutes.

Mr. FITZPATRICK. Thank you, Mr. Chairman.

Ms. Newhouse, thank you for being with us today. When the Colonial Pipeline suffered their ransomware attack in May, we saw the grave impacts on our Nation and our infrastructure. TSA's directives to require reporting and incident report plans were needed.

In 2020, the average estimated time to identify a breach was over 200 days.

So, my question, first question, is what more is being done by your agency to identify cyberattacks in a quicker fashion?

Ms. NEWHOUSE. Thank you for your support and your question, Congressman.

Actually, with respect to those security directives to the pipeline industry, we require reporting of the incidents within 12 hours. And that is because of the criticality of our Nation's pipelines, the fact that they carry the majority of—the significant effects that it would have if those were attacked, because they carry the majority of the resources needed to run this country. So that is why we were very forward-leaning in establishing that immediate timeframe. And we have since also updated that definition, as I have mentioned, of what is a reportable cybersecurity incident, in collaboration with industry.

Mr. FITZPATRICK. Secondly, it has been found that well over 80 percent of breaches are financially motivated, and the average ransomware payment rose over one-third in 2020, from 2019 levels, to over $100,000.

Do you believe that American companies should continue to pay ransoms to bad actors?

And if not, do you think that legislation would be needed to, basically, disincentivize or, if not, ban and make illegal ransom payments altogether, and have more of a Federal program to address that?

Ms. NEWHOUSE. As referenced earlier, CISA Director Easterly referenced ransomware as likely the highest level of malicious cyber activity.

I would say that, through the Department of Homeland Security, and CISA in particular, we work very closely with our law enforcement, the FBI, both Federal and State and local law enforcement, to identify those opportunities.

I would defer to my CISA colleagues on how we can best combat ransomware from a technical standpoint, in addition to the financial aspects, as well. I am happy to take that back and coordinate that for you, Congressman.

Mr. FITZPATRICK. Thank you, Ms. Newhouse.

Mr. Chairman, I yield back.

Mr. AUCHINCLOSS. The Chair recognizes Ms. Bourdeaux for a period of 5 minutes.

Ms. BOURDEAUX. Thank you so much, Mr. Chairman.

We have all seen the far-reaching negative implications of cybersecurity attacks on the transportation sector. For example, in May of 2021, the ransomware attack on the Colonial Pipeline resulted in more than 43 percent of gas stations in my home State of Georgia being out of gas.

It is clear from today's testimony that more work needs to be done to strengthen cybersecurity protections in all areas of the transportation sector.

Mr. Grossman, in your written testimony you talk about the value of training through participation exercises or simulations. My district is home to Curiosity Lab at Peachtree Corners, which is a one-of-a-kind living lab designed to provide a real-world test environment to advance next generation intelligence, mobility, and smart city technology.

What kind of simulations do you run to prepare your staff for cybersecurity attacks?

And could you talk a little bit about the benefits of those real-life simulations?

Mr. GROSSMAN. Absolutely, Congresswoman, thank you very much for that question.

As I mentioned in my oral testimony, as well, we have developed a cyber test facility in Atlantic City at our William J. Hughes Technical Center that serves as kind of the cornerstone of some of our exercise activities. We regularly conduct incident response exercises that include both the mission support side, or the normal, IT side of FAA, as well as the operational side, or the NAS, the National Airspace System.

In addition to that, we conduct external exercises with DHS and all of Government. There are cyber exercises.

We have also conducted international exercises with the Caribbean, with Mexico, and several other countries. This year, we have begun looking at cyber ranges, so that we can actually inject real-world cybersecurity threat into our exercises, so that we can get an actual look at what an actual attack would look like.

Typically, when we simulated exercise, it is just the data——

[Audio malfunction.]

Ms. BOURDEAUX. Might have lost——

Mr. GROSSMAN. Yes, I am sorry.

Ms. BOURDEAUX. Yes, I might have lost you for a second there.

Mr. GROSSMAN. I apologize.

Ms. BOURDEAUX. OK. So just to follow up with that, Mr. Schachter at the DOT, are there similar types of exercises that you do that you could talk a little about, and what the value add is of having that kind of real-life simulation?

Mr. SCHACHTER. Well, thank you for that question, because it gives me an opportunity to discuss, actually, one of the most effective and least expensive type of simulation exercises, and that is one where we send, essentially, a test email encouraging people to click on an unknown link, a technique called phishing.

And what we see is, by repeating that on a regular basis, people get much smarter, and become much more cautious about clicking on those links. And, as was mentioned a little while ago, this is a prime way that malware gets introduced into enterprise environments unknowingly by people within the organization.

So, this is a, as I said, a very effective, very inexpensive means of protecting the network, and providing greater access control.

Ms. BOURDEAUX. Thank you very much. I yield back the balance of my time.

Mr. AUCHINCLOSS. The Chair recognizes Mr. Mast for a period of 5 minutes.

Mr. MAST. Thank you.

Admiral, I would love to start with you. Number one, thank you for your service in the United States Coast Guard. I very much appreciate that. I want to talk a little bit about this.

If your men and women are physically attacked, do they return fire?

Admiral MAUGER. Congressman, we have a well-established, well-rehearsed, well-trained process in place for use of force in the Coast Guard. It is not my area of expertise. And so, if you want to go into that in more detail, I would be happy to take that question for the record or set up a briefing for you.

Mr. MAST. Not a lot of detail, just logically and commonsensically, if somebody points the muzzle of a rifle at one of your men or women, and depresses the trigger, and moves around at a couple thousand feet per second towards one of your men and women, are they going to return fire?

Admiral MAUGER. Congressman, they will execute the Coast Guard use of force policy, and so, if fired on by an adversary, they will fire back.

Mr. MAST. That is right. Like I said, that is not meant to be provocative, right? It is common sense that they will.

Again, understanding you are not a shooter by your own admission, do you think that they should shoot until they totally eliminate the threat? Just opinion, I am looking for opinion on this. I understand you are not a shooter.

Admiral MAUGER. Congressman, I think that, in the general sense, our folks need to ensure their own personal protection, and for the protection of their colleagues, and ensure the protection of any members of the public as well. And so, they will carry out and continue with the use of force policy until that local Coast Guard's women or men is sure that things are safe.

Mr. MAST. And we should dispatch the threats, in my opinion, and I have been a part of doing that in a different place.

And I want to layer this on cyberattacks and cyber threats. And the reason that I asked that was to go and layer that on this question: Should we approach a cyberattack in the same way that we would approach a physical attack? Should we go out there?

There is a moment that it turns from defending myself to going out there and seeking a violent course of action to dispatch the threat that is coming against me. And it becomes offensive, and that is not provocative.

Should we be pursuing that in every instance of being shot at in the form of cyber, that we dispatch that threat so that it can never again pose that threat to us again?

Admiral MAUGER. So, Congressman, as we move this into the cyber landscape, it is really important to understand that there are key differences.

There is a big difference between attributing a shooter right in front of you, using force against you that you can see and react to, versus somebody in the cyberspace that might be working through a different adversary, or he might be working through a different venue to get after you. So, attribution in cyberspace is really critical.

That said, the Coast Guard released a cyber strategic outlook in August that puts together three lines of effort: the first line of effort is about defending and operating our networks and DoD networks; the second one is about protecting the maritime transportation system, and we bring together the full spectrum of the prevention and response framework to protect the maritime transportation system; and then the third——

Mr. MAST. Do you——

Admiral MAUGER [continuing]. Element is——

Mr. MAST. Do you believe in making that transition, however, from we were attacked, we are now assessing what happened from the attack, and we are now transitioning to offensive, to eliminate where we assess the origin of that threat?

If you can assess the origin of that threat, do you believe in becoming offensive against that threat?

Admiral MAUGER. Congressman, we are building, with support from Congress in fiscal year 2021, and with support from the administration in the fiscal year 2022 President's budget, we are building out a cyber mission team capability that allows us to take full spectrum operations, provided that we have the right authorities in place, against adversaries.

And so——

Mr. MAST. So, that is a yes.

Admiral MAUGER [continuing]. It is an important part——

Mr. MAST. The full spectrum, meaning——

Admiral MAUGER. It is an important part of our strategy.

Mr. MAST. Full spectrum, meaning yes, you believe you should have that capability to transition to the offensive against where you believe a threat originated from.

Admiral MAUGER. Congressman, that is the key part of our three lines of effort and our strategic outlook. We are aligning our training under the joint DoD standards, so that we can work closely with the Department of Defense to carry out what the Nation needs from their forces.

Mr. MAST. Very good.

Mr. AUCHINCLOSS. The gentleman's time has expired.

Mr. MAST. Thank you, Mr. Chair.

Mr. AUCHINCLOSS. The Chair recognizes himself for 5 minutes.

Last month, we heard from industries on real-world challenges they face, and I look forward to speaking with our witnesses today on how the Federal Government can work with its private-sector partners to protect and strengthen our digital infrastructure, as well.

This question is for, first, Mr. Dorsey, and then Mr. Marinos, in that order, please.

My district in Massachusetts has two leaders, at least, in the cybersecurity industry. Industrial Defender is headquartered in Foxborough, Massachusetts, and CyberArk in Newton. These companies work on security roadmaps and software to protect complex operational technology in line with NIST compliance.

Has the DOT Inspector General's Office and/or the GAO looked at how Federal agencies are interacting with companies like these, and local transportation agencies?

And do you have any recommendations for improving public-private coordination and cooperation?

And these questions are first for Mr. Dorsey, and then for Mr. Marinos.

Mr. DORSEY. Thank you for your question, Congressman. The Department of Transportation Office of Inspector General has not looked at that line of coordination, if you will.

But what I will say is that, as part of our annual assessments through FEMA, we do work with the Department, and ask them a series of questions from the standpoint of a supply chain, a risk management area. And what we do with that line of reasoning is just to go back and determine whether or not the Department has taken appropriate steps with respect to ensuring that any vendor-related software that they get is not associated with any type of counterfeit efforts, or anything like that.

And we also make a determination as to what extent does DOT ensure that products, system components, systems, and services of external providers are consistent with DOT cybersecurity policy.

That is a new requirement that just has been incorporated in the IT system metrics that we have to assess on an annual basis.

Outside of that, that is how we go about communicating with the OMB, as well as how we report to Congress with respect to what the Department's efforts are in that particular arena. Thank you.

Mr. AUCHINCLOSS. Mr. Marinos?

Mr. MARINOS. Yes. So, Congressman, two thoughts here.

One, GAO was tasked by law to evaluate the adequacy of standards that the National Institute of Standards and Technology puts out. So NIST. And the biggest one in this area is the cybersecurity framework.

And as part of the four reviews—we are actually wrapping up the fourth just in the next few months—we looked at how this cyber framework was pulled together, including what kind of engagement NIST had in doing a public exposure draft, and receiving comments from outside stakeholders, and then incorporating them into the framework. They have done this on a couple of iterations of the framework, and they, of course, do it on other special publications, as well.

So, we may not necessarily interact directly with organizations like those that you mentioned, but we certainly evaluate how NIST is taking in information from folks out there, the experts out there on cybersecurity, and whether they can use that to better the framework and the guidance that is being put out.

And then the second thing I just mentioned too, though, is that GAO does engage quite often with State and local audit offices, including the Massachusetts State Auditor's Office, as well. And that has been a really great opportunity, because it gives us a chance to have a better sense of how effective Federal guidance is within their capacity, and what are sort of the threats and the landscape that they are also seeing State and local agencies have to combat, as well.

Mr. AUCHINCLOSS. Thank you to you both. The Chair yields the balance of his time and recognizes Mr. Johnson for 5 minutes.

Mr. JOHNSON OF SOUTH DAKOTA. Mr. Chairman, are you talking about Mr. Johnson of South Dakota?

Mr. AUCHINCLOSS. Yes, sorry.

Mr. JOHNSON OF SOUTH DAKOTA. Very good. No, not a problem. All right, well, I will start with Mr. Grossman.

And Mr. Grossman, I recently had the opportunity to visit an air traffic control facility in Sioux Falls just a couple of weeks ago, and it was fantastic, really dedicated people, for sure. Sean Hennet and others showed me around. But I couldn't help but notice how antiquated some of the computer equipment was. There were some newer systems, but they seemed to be intermingled with some that were older than many of the folks working in the tower.

And so, give me some sense, very quickly, of the kind of challenges that we have keeping these systems safe when they are so antiquated.

Mr. GROSSMAN. Well, thank you for your question, and I appreciate your trip.

I think, from a cyber perspective, those systems, while they appear to be old, we are able to keep them secure. If you are asking about simply replacing those systems, that is really not in my area.

I would have to take your question back to our air traffic organization. But from a cybersecurity perspective, even though they appear old, they are certainly secure.

Mr. JOHNSON OF SOUTH DAKOTA. OK, very good. I appreciate that. And maybe I will shift gears now to Mr. Marinos.

I listened with interest when you noted that GAO has made 3,000 recommendations for improving cybersecurity to Federal agencies, and with even more interest when you noted that there are more than 900 of them that have not been implemented by those agencies.

We haven't had a lot of discussion today about dams, which is under the jurisdiction of this committee. Sir, are you aware of any particular—and obviously, the dams are critically important, both from an electrical generation perspective, as well as a flood control perspective for this country—are you aware of any particular recommendations that have been made to the Department of Homeland Security vis-a-vis cybersecurity for our dam infrastructure that have not been implemented?

Mr. MARINOS. Actually, Congressman, sort of building off of the most recent question that I answered, the NIST cybersecurity framework, obviously, applies to all sectors. And so, as part of the work of the series of four reviews we have done, we have actually gone out to DHS and the other now Sector Risk Management Agencies, and we have asked them whether their respective sectors are finding it useful. You know, are they adopting it?

And so, that would include the dam sector, as well, the subsector, as well.

And so, in those instances, we have seen that Federal agencies are challenged, not only within that sector, within others, to be able to have that kind of dialogue with operators, big and small, within their respective sectors. There are a variety of reasons for that.

One, there may simply not be the appropriate expertise at the operators to be able to interact, to provide that kind of feedback, even to be able to use the framework in the way that it is intended. It is a very expansive set of sort of—it is like—it has been sort of equated to, like, a grocery store. They can go in and pick and choose the cyber protections that you might want to implement.

And so, I think the important thing is for DHS to make sure that it is getting feedback from, not only the dam sector, but others, to make sure that the support and guidance it is providing is actually useful.

Mr. JOHNSON OF SOUTH DAKOTA. So—and I think that is helpful. But, as you alluded to with your last answer, that is more comprehensive, right? It is across all impacted agencies.

Does anything in particular stand out with regard—I mean, we were talking about some of the antiquated IT systems in place for the FAA. I happen to know that that is also the case for the operations of the dam systems with Western Area Power Administration and others. Anything in particular that comes to mind with that subsector?

Mr. MARINOS. Absolutely. And it doesn't just relate to that specific sector. But, as you point out, legacy systems, especially with operational technology, are something that operators need to be thinking about ahead, have a plan for how they intend to modernize.

And as Larry pointed out, as Mr. Grossman pointed out, many of those systems may actually have, in some ways, better protections if they are air-gapped. In other words, if they are not connected to business systems within those respective companies, they may be better suited for the sort of operational control activities that they do.

But the reality is that, again, that connection to the Federal Government—how do those operators know what the greatest threats are? That is going to require a good amount of information sharing, to and from, to kind of know what the posture is within the dam sector, as an example.

Mr. JOHNSON OF SOUTH DAKOTA. Yes, I think that is well said, sir.

Has GAO indicated the investment gap—as we talk about these legacy systems and the need to replace them, has GAO estimated the size of that gap in dollars and cents?

And could you point me toward a particular report that I could review to learn more?

Mr. MARINOS. I am happy to share information from the Federal agency side, and maybe that equates to the private sector. But the Federal Government continues to spend 80 percent of its IT budget on legacy activities, not on modernizing. And so, I think that is an important aspect, as well as—as the DOT CIO mentioned—modernizing with security in mind from the beginning.

Mr. JOHNSON OF SOUTH DAKOTA. Very good. Thank you, Mr. Chairman, and I yield back.

Mr. AUCHINCLOSS. The Chair recognizes Mr. Malinowski for 5 minutes.

Mr. MALINOWSKI. Thank you, Mr. Chairman. I want to zoom out a bit—no pun intended—and talk about the future of transportation, 5, 10, 15 years from now, and get into how the Department is guarding against new and emerging threats. And then I want to ask Mr. Schachter for his thoughts, and Mr. Marinos for his reaction.

I participated a few days ago in a tabletop exercise that simulated a hostile power taking down our GPS system, something that obviously would have incredibly dire implications, even today, for nearly all modes of transportation: air, rail, maritime, and more.

In the consumer automobile context, some of America's largest companies—Tesla, Apple, Alphabet—are investing billions of dollars in autonomous vehicle technology. I was in a meeting just yesterday with Sundar Pichai, the CEO of Alphabet, which owns an autonomous driving startup, Waymo, and he reaffirmed his interest to us in bringing that technology to the market.

So, while there is no expert consensus on precisely when there will be widespread adoption of level 4, level 5 autonomy, I think it is safe to say that we are going to have a huge number of vehicles on the road, certainly by the 2030s, that are heavily or even exclusively reliant on artificial intelligence to make decisions about accelerating, braking, turning, every road decision. And, in fact, today every car is rolling off the assembly line packed with computers. Many have internet-based, internet-enabled entertainment systems that are pre-installed, and there is even more revolutionary technological change to come, including, potentially, cars that are charged by the highways that they drive on themselves.

As all of you know, any product, device, or service that is connected to the internet, or that is otherwise reliant on code, is going to be vulnerable, potentially vulnerable, to compromise. And the stakes are going to be incredibly high when we are talking about software-powered machines that are carrying people at 70 miles or more down the freeway.

So, Mr. Schachter, recognizing your primary focus is on the internal IT management of the Department, that you have only been on the job for a few months, and you are not personally writing the regulations related to autonomy or grid safety, I do want to ask you some big-picture questions about how you and your colleagues are thinking about the threats that are around the corner.

What cyber-related challenges does the Department expect to encounter in 5, 10, 15 years, when the technologies that we are just talking about today become mainstream?

What is going to keep your successor up at night, and what, if anything, are you doing now to prepare?

Mr. SCHACHTER. Well, thank you very much for that question.

GPS and overall positioning, navigation, and timing are very important issues that DOT is studying in multiple places. The best example I can give you actually relates back to my experience in New York City, where we were one of the three national connected vehicle test locations through a Department of Transportation connected vehicle pilot program.

And securely communicating with all of the test vehicles, and standing up a security credential management system so that the vehicles were communicating for basic safety information like emergency braking, or even a traffic signal phase warnings, like when you were about to approach a red signal, we wanted to be sure, and the Federal Government wanted us to be sure, that all of those transmissions were from authenticated actors, and nobody was spoofing actors and potentially causing harm to either the people operating vehicles, or other road users, as well.

So, that is a future technology that is not so far away, but certainly demonstrates the issue involved that you are referencing, that those communications need to be secure, and we need to know, both on the transmitting and receiving end, they are from partners we recognize.

Mr. MALINOWSKI. I guess I am out of time. I yield back.

Mr. AUCHINCLOSS. The Chair recognizes Miss González-Colón for 5 minutes.

Miss GONZÁLEZ-COLÓN. Thank you, Mr. Chair. My question will be to Mr. Larry Grossman. And the question will be—I just want to bring to attention that the FAA decision to utilize section 804 to consolidate air traffic control operations in Miami for the Caribbean Basin, which includes Puerto Rico, and San Juan Airport operates with 1970s technology.

Yet the San Juan Flight Center handles more than 4,000 flights, mostly consistent—all flights, including arrivals, departures, and overflights for Puerto Rico, the U.S. Virgin Islands, the British Virgin Islands, and overflights from South America, due to its 400-

mile-long airspace, which can take commercial airlines an hour to transit through. And this is the same number of flights that Atlanta airspace covers, from Charlotte to Savannah.

So, my question will be, while I understand that this has been done to consolidate operations, and for cost savings, my concern is, what are the assurances that a cyberattack on the FAA facilities in Miami won't affect air traffic control operations in Puerto Rico?

And what type of redundancies are put in place for smaller airports in rural and remote places, should a larger airport's air traffic control operations be affected by a cyberattack, considering that we have the international airport, but, as well, smaller airports around the island?

Mr. GROSSMAN. Well, thank you very much for your question. I am not, as I am sure you know, I am not responsible specifically for facilities consolidation.

But from a cyber perspective, the protections that our air traffic control systems have are virtually identical, whether a facility is local, or whether it is remote and managed through our secure communication protocols, which is a service that we obtain. But that service is the same, whether you are dealing with a local facility or a remote facility. The security parameters are the same.

Miss GONZÁLEZ-COLÓN. Mr. Grossman, you have been talking about the aviation ecosystem. And with this concept in mind, what kind of training do airport and air traffic control workers get on cybersecurity?

Mr. GROSSMAN. Well, I can't speak for airport workers that are not specifically employees or our contractors, but I can tell you that all air traffic controllers are required to take yearly security awareness training, as are all our contract employees, contract tower employees, et cetera. Employees—go ahead, sorry.

Miss GONZÁLEZ-COLÓN. After the first hearing we had on this topic, some employees last month in the hearing said that they were conducting personal business on work computers, or even personal cell phones that exposed the companies they worked for to cyberattacks. How can we ensure that the same does not happen in airports around the country, or while airplanes are in the sky?

Mr. GROSSMAN. Well, I can assure you that there is no personal business done on any mission-critical system or service. Individuals' Government-issued workstations that they get their email on, they are permitted to do limited personal use, and that is very limited, you know, if someone needed to, on their break time, log into the bank, or something like that.

Miss GONZÁLEZ-COLÓN. Thank you.

Mr. Dorsey, if you don't mind, how often does DOT test its security controls as part of the risk management issues the OIG identified in 2021?

And what do those tests include?

And do we have any operating agency experience a full cyberattack with different types of attacks?

Mr. DORSEY. Thank you for the question, Congresswoman.

We assessed the Department's areas in testing cybersecurity controls based on the NIST cybersecurity framework in five different areas. We determined whether or not the Department is adequately testing security controls centered around identifying and managing risk, protecting its IT systems from a configuration management standpoint, from a daily access and management standpoint——

Mr. AUCHINCLOSS. The gentlewoman's time has expired.

Miss GONZÁLEZ-COLÓN. Thank you.

Mr. DORSEY. I will be happy to provide you with an updated response on the record.

Miss GONZÁLEZ-COLÓN. Thank you.

Mr. AUCHINCLOSS. The Chair recognizes Mr. Carbajal for 5 minutes.

Mr. CARBAJAL. Thank you, Mr. Chair.

The shortcomings in our Nation's cybersecurity readiness are apparent, both in the public and the private sectors, as evidenced by the cyberattacks this year, including on the Colonial Pipeline and JBS Foods. We cannot leave ourselves vulnerable enough to allow bad actors to control essential infrastructure such as energy supply, water management, supply chains, and public transit.

Mr. Dorsey, as you noted in your testimony, your office has identified information security as a top management challenge in the Department of Transportation. But yet the DOT has not resolved dozens of open recommendations by your office in the last year.

In the report done by Clifton Larson Allen LLP released in October of this year, they concluded that the DOT must develop and communicate an organizationwide supply chain risk management strategy and implementation plan to guide and govern supply chain risks.

What do you see as barriers to this recommendation being implemented?

And given the supply chain issues we are currently experiencing, how urgently can the Department of Transportation act on this recommendation to avoid future disruptions?

[Pause.]

Mr. CARBAJAL. I think you need to get unmuted.

Mr. DORSEY. Sorry. Thank you for the question, Congressman.

As noted in my testimony, I noted three key areas that the Department needs to take immediate steps to address their cybersecurity issues that we have identified over the years. Similar to addressing supply chain risk management issues, this applies to all of the cybersecurity issues associated with the Department.

And what the Department needs to do, from the start, is solidify its leadership at the Department's Chief Information Security Office level to ensure that, working with the current and new chief information officer, that they establish the right type of framework and controls to ensure the enforcement of the various recommendations that we have made over the years.

The second thing that the Department needs to do is to develop a comprehensive, DOT-wide cybersecurity strategy to address our recurring weaknesses. Until they do so, which we have made a recommendation—we have made an overarching recommendation this year, and to the Department's credit, they agreed to implement that particular recommendation. Once they do that, and they meet the intent of the recommendation, then I think that will go a long way with addressing some of the concerns regarding supply chain risk management.

And the last thing the Department needs to do is to ensure they put the proper controls in place to protect and secure its IT infrastructure. And in regards to supply chain risk management, that is a key area that we focused on during our enterprise-level review this year, and we will continue to report out on that as we move forward. Thank you.

Mr. CARBAJAL. Thank you.

Ms. Newhouse, leaving ourselves open to ransomware and other cyberattacks puts people's lives in jeopardy. It is a national security risk and threatens our economy. There needs to be a better communication between the private sector and Government to ensure we are prepared for future attacks.

In our hearing of November 4th, we heard concerns from industry representatives that reporting mandates would create a flood of information, resulting in pertinent information being lost or skipped over by agencies.

What steps are being taken by the TSA to ensure reporting mandates are collecting and processing pertinent information in an effective manner?

And, two, can you walk me through how TSA takes in reported cyber threats, and then processes the data?

Ms. NEWHOUSE. Thank you, Congressman, I appreciate that. And I am very proud of the fact that we have continued robust engagement, a lot of engagement with a lot of stakeholders, including those who served on the panel, the previous hearing.

Particularly, just myself in this past week, we have had executive-level meetings with senior executives in rail and passenger rail on this very topic. We have received their feedback on what we call our draft security directives, and that better informed our definition of what we were looking for, in terms of a reportable cybersecurity incident. We have made it more effective, less broad. So, it is an actual—or an incident that is reasonably likely to have a devastating impact on any of their systems.

So, it is also important to note that those reports go to what we call CISA Central. The Cybersecurity and Infrastructure Security Agency has a centralized operation center. Our directives mandate reporting of that information to CISA Central.

Mr. CARBAJAL. Thank you. My time is up. I yield back.

Mr. AUCHINCLOSS. The Chair recognizes Ms. Van Duyne for 5 minutes.

Ms. VAN DUYNE. Thank you very much. I want to thank all of you for being with us this morning.

My district is home to Dallas-Fort Worth International Airport, which is also the largest economic driver in the State of Texas, and one of the Nation's most important airline hubs. Over Thanksgiving weekend, we saw passenger numbers exceed 90 percent of pre-pandemic volume throughout the country.

DFW Airport is part of a working group with DHS and TSA, and I have heard that they have benefited from transparency, and have gained valuable information from working together, while also making positive improvements after TSA conducted a review.

Mr. Grossman, many of our airport critical systems, such as radar systems, are hosted by airports around the country. Does the

FAA offer collaboration similar to what we have seen with DHS and TSA for airports?

And the second question would be what more can the FAA do to expand current collaboration and increase information sharing with our airports?

Mr. GROSSMAN. Thank you for those questions. I may have you repeat the first one, but I will answer the second one first.

We collaborate extensively with airports through our Aviation Cyber Initiative, as well as the Aviation Sector Coordinating Council, which has airport authorities and AIA as members. And so, our collaboration with airports is pretty rich in substance. We share best practices with airports and, on many occasions, when there was a vulnerability identified, I believe on an airport lighting system that was a non-FAA component, we immediately shared that across the airport industry.

And I would just ask if you could repeat the first question.

Ms. VAN DUYNE. So, the first question I talked about DHS and TSA, and how they have collaborations in a working group that is focused on transparencies and ways to better collaborate, and I didn't know if—the question was, does the FAA have a similar working group with airports, like the other two do?

Mr. GROSSMAN. Well, we participate with TSA on the airports working group. And so——

Ms. VAN DUYNE. OK. OK. I have got a followup question for Mr. Grossman and for Victoria Newhouse.

Everything that we have heard from airlines is that in 2022, that could be a record-breaking year, in terms of traffic from Europe, the Middle East, and South America, given the pent-up demand.

So, obviously, Omicron can throw a wrench into those plans, but CBP staffing for international arrivals is going to be critical. It could be a significant pinch point, if they are not prepared. So how is the FAA preparing for further disruptions in the system, as we move closer to the busiest travel time of the year?

Mr. GROSSMAN. Well, again, that is—I apologize, that is not a cybersecurity-specific question. I believe our staffing numbers are not going to be impacted by that.

Ms. VAN DUYNE. OK, so are you expecting further disruptions, or no?

Mr. GROSSMAN. I am not expecting any further disruptions, no.

Ms. VAN DUYNE. OK, so there are no preparations being made, then, for the increased travel in 2022?

Mr. GROSSMAN. Well, we are staffed for that increased travel. I guess I am not sure of——

Ms. VAN DUYNE. OK.

Mr. GROSSMAN [continuing]. The question, specifically.

Ms. VAN DUYNE. OK.

Mr. GROSSMAN. So——

Ms. VAN DUYNE. So, Ms. Newhouse, what is the TSA's plan to ensure checkpoints have proper staffing, and wait times are minimized for passengers?

Ms. NEWHOUSE. Congresswoman, we are leaning forward very heavily. As you may have heard from Administrator Pekoske over this past year, we have worked very hard to hire as many officers as we can. It is a very competitive labor market.

But we are also focused on ensuring real-time reporting. We share that with our airline and airport partners daily, and sometimes hourly, to ensure any sort of issues in the system, whether it is equipment or personnel-related, is addressed immediately.

Last, we do have our national deployment force that is ready and able to deploy at a moment's notice to support increased operations around the country. We have seen that successfully for major sporting events, such as the Super Bowl, spring training. Also, in the event of a natural disaster, we are able to put our personnel in to support air operations, while the personnel who are affected on the ground and their families can evacuate safely. Thank you.

Ms. VAN DUYNE. I appreciate that. I, again, have gotten lots of calls and questions from folks who are constituents in the 24th Congressional District. They travel a lot, and there is a lot of frustration that they are feeling like the lines are getting much longer, that there are fewer TSA folks working. So, I just want to make sure that that is a focus that you guys are working on.

Thank you very much, and I yield back.

Mr. AUCHINCLOSS. The Chair recognizes Mr. Lamb for 5 minutes.

Mr. LAMB. Thank you, Mr. Chair, and thank you to all of our witnesses.

Mr. Dorsey, I wanted to start with you. I took from your testimony that, while there are several sort of technological and purely cybersecurity issues at play here, there seems to be, at the foundation, kind of a personnel issue of maintaining consistent leadership in the key roles, and keeping people in place, and bringing people up through the system so that they understand it. And that is very similar to what I have seen on other committees dealing not only with cybersecurity, but also just kind of like talent—or technology acquisition and implementation.

And so, it is not an easy problem to solve. I was just curious if, in your work, you saw any commonalities about why we were losing people, why we were failing to gain them in the first place, or any suggestions about how we could start to fix the personnel side of this.

Mr. DORSEY. Thank you for your question, Congressman.

Our assessments don't necessarily review what the workforce-related issues are, with respect to the Department's cybersecurity posture. So, I will not be able to provide you with a direct answer.

What I will say is that I am very encouraged by the Department's current chief information officer, and the various discussions that I have had with him regarding the effort and his plans, moving forward, with respect to addressing the workforce issues.

What our reviews have found is that there has been inconsistency at the top regarding the Department's leadership from the chief information officer, as well as the chief information security officer. And, as I noted in my testimony, over the last year the Department had an acting chief information security officer who said cybersecurity was not his primary role and responsibility.

But what I will say is I am encouraged by the conversations that I have had with the current chief information officer, and I look forward to working with him, moving forward. Thank you.

Mr. LAMB. I appreciate that, thank you.

Do any of our agency witnesses want to weigh in on this question?

Basically, what I am trying to get at is this is a common problem for us, because, obviously, people with strong cybersecurity management backgrounds are also in very high demand in the private sector. So, I don't know if you have any success stories or suggestions you could make to us about trying to put ourselves on a firmer footing here, from a personnel perspective.

Is that Mr. Schachter from DOT?

You are on mute, it sounds like.

Mr. SCHACHTER. Thank you. Yes, I would like to respond to that, and thank you for the question.

It gives me the opportunity to say that, after having noted that improving cybersecurity at DOT is our number-one priority. Our second priority is investing in our workforce, and that means investing and helping them develop their careers, so that they are not only able to perform at higher levels with their current responsibilities, but they are adequately prepared for future responsibilities.

It also includes recruitment and making sure that we hire in the right people with the greatest potential, and that we are looking at our own people for future professional opportunities.

I will refer back to my experience as CTO and CIO at the New York City Department of Transportation, where I served for 13 years. And in that role, we were able to achieve very low levels of attrition, due to a robust training program that invested in our staff, made them part of the agency's strategic mission, where they felt ownership and empowered. And even though the private sector often came calling with higher salaries, we lost relatively few people.

And I understand, from industry information, that is a frequent problem not only for the Government, but even private-sector companies losing staff to one another as each tries to outdo the others for the best food, or health club, in addition to just cash compensation. And the Government is often at a disadvantage when trying to compete in that arena.

So, I think what we can do, though, is we play to our strengths, which is the importance of our mission, the opportunity for people to make a contribution to improving—and now, in this environment—the United States. And I believe that we will have a compelling story to tell that will both attract good new people, as well as help us keep the good ones that we already have.

Mr. LAMB. I agree. We have to appeal to their patriotism. And I hope, if there is a way that we can help any of your agencies do that, you will let us know, because we know how important it is. Thank you for your participation.

Mr. Chair, I yield back.

Mr. AUCHINCLOSS. The Chair recognizes Mrs. Steel for 5 minutes.

Mrs. STEEL. Thank you very much. Thank you, Mr. Chairman and Ranking Member Graves, for holding this important hearing.

During my tenure, while serving as Orange County Supervisor and on the board of directors for the Orange County Transportation Authority, there was a cyberattack on the OCTA. Hackers froze some of OCTA's computer systems for 2 days and demanded ransom to unfreeze them. We did not pay the ransom, and chose to ignore the demand, and we had staff restore all infected servers. We are very lucky about it.

So, I want to ask Ms. Newhouse, are there ways Federal agencies can improve communication with State and local government to best protect against these cyberattacks?

And do you think the United States has the proper workforce to fight these current and future threats?

These threats are coming in from sometimes China, sometimes North Korea. So, do you have that?

Ms. NEWHOUSE. Thank you, Congresswoman, and we are very proud of our relationships with our both Federal, State, and local partners, many of whom operate critical transportation assets throughout the country.

We have a very robust field operation now in place that focuses solely on surface operations. That is one resource that is available 24/7. Each region of our country—we have divided it up into six regions—has a responsible executive, and an entire team of personnel ready to go to engage one-on-one.

But you are absolutely—you hit it on the nail. That continued collaboration and dissemination of information, it could be anonymized, but it is important that we continue to provide both threat and indicator information to all operators, whether they are State or local or private, and we have established a number of mechanisms to do that through our directives.

We are also looking for [inaudible] reporting so that way we can filter that, and make sure it gets sent out anonymized, and work through CISA and CISA Central to make sure those reports are getting disseminated in a very timely manner. Our TSA Operations Center also serves that—I would call it a redundancy.

Third, we do have what I think are pretty unique information-sharing cells within the United States Government. We actually have groups of individuals, both for surface transportation and aviation, that can actually participate in daily threat briefings with the TSA. They can do it remotely from their locations, and that is another opportunity where we, again, provide that persistent information, both indicators, threat and tools.

We do also have—you point out that the nation-state actors—CISA's security bulletins, just as recently as last week, was issued referencing a nation-state actor. That is where TSA, the DHS enterprise, works very closely with our U.S. intelligence community. We rely closely and heavily on their intelligence and assessments, along with our Federal Bureau of Investigation and other law enforcement entities.

We do have the workforce in place in the United States Government. I have a background in intelligence operations myself, and I can say with personal knowledge that we do have direct access to that intelligence and law enforcement information.

Mrs. STEEL. Thank you very much for your detailed answer.

Admiral, I have a question that—you know, protecting against cyber threats is really critical for the Ports of Long Beach and L.A. Right now, we have a supply chain crisis, as we have about 175 ships waiting to unload. So, it is very important.

So, Congress has made several changes to better integrate cybersecurity planning and response. How is the Coast Guard conducting vulnerability assessments of maritime critical infrastructure?

Can you describe how the Coast Guard builds cyber resilience in the Ports of L.A. and Long Beach to protect this port and others like it from attack?

Admiral MAUGER. Congresswoman, the current supply chain crisis really highlights the importance of the MTS to our national economy, and to our national security, and it really emphasizes the need to put proper protective measures in place, but then also be able to be resilient and respond to attack.

We have put together a comprehensive framework as the lead Federal maritime regulator across the whole prevention and response framework, to make sure that port communities and maritime critical infrastructure are able to prevent attacks, but then are able to respond and be resilient.

The Port Security Grant Program is a key program for building resiliency into the ports. Through funding in fiscal year 2021, we were able to fund 60 projects at about $18 million and provide key ports such as the Ports of L.A. and L.B. the opportunity to increase their assessments.

And I am happy to follow up with a brief for you, ma'am, afterwards, if desired.

Mrs. STEEL. Thank you very much, Admiral. I have one more question, but you know what? I am going to just submit this question.

Thank you. My time is up, and I yield back.

Mr. AUCHINCLOSS. That concludes our hearing.

I would like to thank each of the witnesses for your testimony today. Your comments have been insightful and helpful.

I ask unanimous consent that the record of today's hearing remain open until such time as our witnesses have provided answers to any questions that may have been submitted to them in writing.

I also ask unanimous consent that the record remain open for 15 days for any additional comments and information submitted by Members or witnesses to be included in the record of today's hearing.

Without objection so ordered.

The committee stands adjourned.

[Whereupon, at 1:20 p.m., the committee was adjourned.]

SUBMISSIONS FOR THE RECORD

Prepared Statement of Hon. Frederica S. Wilson, a Representative in Congress from the State of Florida

Thank you, Chairman DeFazio, for today's hearing.

As our nation's critical infrastructure increasingly relies on cutting-edge technology, cybersecurity must be a top priority to avert attacks on facilities and systems, such as the Turkey Point Nuclear Generating Station located in South Florida.

It is imperative that the federal government is a leader in this space to help stakeholders implement the best cybersecurity practices.

Failing to do so will compromise critical systems that can have devastating impacts on our safety, economy, and security.

I am grateful that the Biden administration has taken steps to improve the nation's cybersecurity by issuing Executive Order 14028 to improve the nation's infrastructure.

I am also proud to have supported the roughly $2 billion provided in the Infrastructure Investment and Jobs Act to modernize and secure our critical infrastructure.

I look forward to working with my colleagues and the private sector to enhance cybersecurity preparedness, increase the cybersecurity workforce, and protect citizens.

With that, I have a few questions.

APPENDIX

QUESTIONS FROM HON. FREDERICA S. WILSON TO CORDELL SCHACHTER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF TRANSPORTATION

Question 1. Mr. Schachter: Thank you for your testimony. As you mentioned in your statement, there are multiple open findings from previous cybersecurity audits, which puts DOT at risk. Some of these findings were reported years ago. In some instances, even when recommendations were reported as completed, they were not tested or implemented properly, as was the case with the FTA's financial management systems.

Mr. Schachter: What is the department's long-term plan to expedite the implementation of cybersecurity recommendations and how will current efforts, like the cyber sprints, help?

ANSWER. Thank you for the opportunity to address the issues raised in this question. We take seriously open audit findings that require action. Cyber Sprints accelerate progress by focusing Office of the CIO and Operating Administration information technology staff efforts on priority activities, eliminating obstacles to progress during frequent checkpoints, and engaging additional or leadership resources if needed. Among the criteria of tasks addressed in the sprints are open audit findings.

QUESTION FROM HON. GARRET GRAVES TO CORDELL SCHACHTER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF TRANSPORTATION

Question 2. I've read reports that there are some 500,000 vacancies for cybersecurity professionals in the U.S. workforce, making it nearly impossible for us to get a handle on the next generation of threats. Additionally, we've heard from industry that they feel that talent is relegated to SCIFs in the federal government, fusion centers, and big technology companies—preventing talent from being available to critical infrastructure at the local level. What can we be doing to rethink the workforce model for cybersecurity-specific professionals?

ANSWER. Thank you for the opportunity to address the issues raised in this question. DOT's Office of the Chief Information Officer (OCIO)'s two top priorities are improving DOT's cybersecurity and workforce development of OCIO staff, including recruiting high quality cybersecurity experts. I believe the government mission is a compelling "selling point" to attract new staff. Similarly, working at US DOT and helping protect the nation's critical infrastructure in transportation is another compelling selling point for recruitment. We will also continue working with our commercial and governmental partners to engage the resources we need. Federal cyber workforce training and education initiatives can be found at the Department of Commerce National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NICE), the National Science Foundation's CyberCorps Scholarships for Service, and CISA's National Initiative for Cybersecurity Careers and Studies.

QUESTION FROM HON. SETH MOULTON TO CORDELL SCHACHTER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF TRANSPORTATION

Question 3. Mr. Schachter, America depends critically on GPS for much more than just navigation with our smartphones, and we have no alternative system. This creates a single point of failure, vulnerable to both cyber and kinetic threats. In fact, after their government's November 15 ASAT test, a Russian state television broadcast boasted they could destroy all our GPS satellites at the same time. The National Timing Resilience and Security Act of 2018 mandated the Department Transportation have a backup and alternative system up and running by December 2020, but the previous administration did nothing. What is the Biden administration's Department of Transportation doing to comply with the law and get a GPS complementary and backup system in operation to decrease the severity of threats like these from Russia and China?

ANSWER. Thank you for providing an opportunity to provide a detailed response to this important question. Our Global Positioning System (GPS) is the predominant technology in the field for Positioning, Navigation, and Timing (PNT). It supports critical transportation infrastructure and is essential for national and economic security in many other areas. There are an estimated 900 million GPS receivers across America, including those used for emergency response, transportation safety, general navigation, timing signals, and high-precision instruments for local-area climatology studies, weather prediction, surveying, precision agriculture, machine control, and scientific applications.

DOT conducted a GPS Backup and Complementary PNT Demonstration involving 11 technology vendors in response to a requirement in the FY 2018 National Defense Authorization Act (NDAA). The 2021 DOT Complementary PNT Demonstration Report to Congress recommends that DOT develop requirements, standards, test procedures, and performance monitoring capabilities to ensure that civil PNT services, and the equipment that utilizes them, meet necessary levels of interoperable safety and resilience.

The "Frank LoBiondo Coast Guard Authorization Act of 2018," (P.L. 115–282; December 4, 2018) included Sec. 514, "Backup National Timing System," also known as the "National Timing Resilience and Security Act of 2018."

We support the proposed repeal of the National Timing Resilience and Security Act in the President's FY 2022 Budget Request. This is informed by recent federal analyses, reports, and technology demonstrations, where DOT finds that 1) no single solution for the provision of back-up PNT services can meet the diversity of critical infrastructure application requirements, and 2) it would be inefficient and anti-competitive for the Federal Government to procure or otherwise fund a specific backup PNT solution for non-federal users.

Rather than building or otherwise procuring a new system, DOT, in partnership with the Department of Homeland Security, is better positioned to enable and encourage the owners and operators of critical infrastructure to be responsible users of PNT, leveraging commercially-available PNT technologies to secure access to complementary PNT services.

QUESTIONS FROM HON. MICHAEL GUEST TO CORDELL SCHACHTER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF TRANSPORTATION

Question 4. Each state has a designated CISA "Protective Security Advisor" that coordinates with members of the critical infrastructure community and works to help them prepare/defend against cyber-attacks. Can you tell me about the interface your agencies have with these Advisors and what role they play in your industries?

ANSWER. DOT's Office of Intelligence, Security, and Emergency Response facilitates DOT's role as Co-Sector Risk Management Agency for the Transportation Systems sector infrastructure. It partners with the other Co-Sector Risk Management Agency, the Department of Homeland Security (DHS) and its Transportation Security Administration and U.S. Coast Guard. DOT does directly engage with CISA's Protective Security Advisors (PSAs). During incident response PSAs and DOT may act in parallel. For example, during a hurricane, PSAs based in the region impacted may provide local information about cross-sector infrastructure concerns to DHS for integration with national response efforts led by FEMA. DOT's Office of Intelligence, Security, and Emergency Response may also provide information to inform FEMA's national response.

Question 5. Earlier this year, in discussions with CISA Director Inglis, we discussed the importance of protecting our digital infrastructure, its supply chain, and preventing overdependency of manufacturing critical digital goods by adversarial countries, which they could possibly use against us. How can the FAA and DOT work alongside private sector stakeholders and Congress to strengthen our digital infrastructure supply chain, industry standards, and enforcement of those standards when it comes to high level digital hardware?

ANSWER. The FAA and DOT works in partnership with DHS and DOD through the Aviation Cyber Initiative (ACI) Interagency Task Force in engaging with a range of government, industry, and international stakeholders to identify, assess, and analyze cyber threats, vulnerabilities, and consequences within the aviation ecosystem through research, development, testing, and evaluation initiatives. The ACI mission is to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the Nation's Aviation Ecosystem. We also leverage industry expertise to develop and update industry standards relevant to aviation cybersecurity. An example is RTCA Special Committee SC–216, which is chaired by a representative industry stakeholder and has an FAA policy representative.[1] SC–216 recently revised their Aeronautical Systems Security standard (DO–365A). This past December, the committee also published a new standard, Aeronautical Information System Security Framework Guidance (DO–391). All of our efforts with Standards Development Organizations (SDO) are geared towards developing industry standards that can be used as an acceptable means of compliance to one or more of our certification requirements. SDOs, like RTCA, ASTM and SAE, often have counterpart working groups in the European standards development community, which provides additional expertise and a wider global acceptance of the developed standards.

We also note that Chris Inglis is the National Cyber Director, a position that is different than the Director of CISA. The Director of CISA is Jen Easterly.

Question 6. Director Inglis also emphasized the need for accountability in cybersecurity practices. Each one of you represents a different set of industry stakeholders with vastly different needs in this space. For bad actors within your jurisdiction that allow their cybersecurity measures to fall below public or industry standards, what are ways that Congress and your agencies can hold those folks accountable? Many stakeholders mention that they are more robust in developing cybersecurity measures and have been for decades. So, what are ways to hold bad actors accountable without installing mandates that may limit the private sector's own work in this space?

ANSWER. Thank you for the opportunity to address the issues raised in this question. The Department of Homeland Security (DHS) and the Department of Transportation (DOT) are designated as the Co-Sector Risk Management Agencies (SRMAs) for the Transportation Systems Sector. DHS, specifically through the Transportation Security Administration (TSA), worked with DOT and its Operating Administrations (OAs) to coordinate industry outreach efforts aimed at informing and receiving feedback from stakeholders on available cybersecurity training and resources; and more recently, TSA's Security Directives and security program amendments on cybersecurity. Additionally, TSA spearheads the developments of the National Strategy for Transportation Security as the lead for DHS. Further, TSA has worked extensively with CISA to assess sector cyber risk, including the Pipeline Cybersecurity Initiative (PCI) and the ACI, which conduct Validated Architecture Design Review assessments of major pipeline and airport systems.

DOT is working closely with TSA, CISA, and the Department of Energy in the implementation of the President's Industrial Control System Cybersecurity Initiative for natural gas pipelines. The Initiative is a voluntary effort by government and critical infrastructure owners and operators. DOT is also participating in the CISA and NIST led effort to develop cybersecurity performance goals for control systems and critical infrastructure, as outlined in National Security Memorandum 5 (NSM–5) issued by President Biden last July. However, voluntary measures alone in some cases may be inadequate to address the rapidly evolving threat facing the critical infrastructure every American relies on. TSA has issued cybersecurity-related Security Directives and Information Circulars (IC) for critical elements of surface transportation—including pipelines—and has also issued Security Program Changes and an IC for aviation elements.

We have balanced responsibility with flexibility by prioritizing certain operator practices as requirements and others as recommendations using our authorities. These include each operator designating a cybersecurity coordinator, implementing specific mitigations measures to reduce cybersecurity risk, and developing plans to minimize disruption in the event of a malicious cyber intrusion.

Question 7. Many industry stakeholders utilize early notification networks. However, the public sector lacks a robust system to alert private carriers or shippers of an attack across the system. To critical infrastructure, the ability to limit damage seems crucial. Can you expand on how early notification networks are used by the private sector and why coordination with a federal government system is so important?

ANSWER. CISA and FBI periodically issue joint Cybersecurity Advisories (CSAs) which are posted on the CISA Alerts webpage. These Alerts are also pushed to a wide-range of stakeholders, to include the Sector Risk Management Agencies and Information Sharing and Analysis Centers (ISACs) for further dissemination to sector stakeholders. There are also several private companies who offer similar notification products. The US Coast Guard and CISA are responsible for notifications to the Maritime subsector.

[1] https://www.rtca.org/sc-216/.

In the railroad subsector, the Association of American Railroads (AAR) utilizes the Railway Alert Network (RAN) to provide early notifications to the private sector. Separately, when Federal Railroad Administration (FRA) reporting is either required or deemed necessary, the agency provides situational reports to AAR, the American Short Line and Regional Railroad Association (ASLRRA), the Transportation Security Administration (TSA), and the Surface Deployment and Distribution Command (SDDC). These situational reports are generally disseminated to the carriers participating in RAN.

In the commercial motor vehicle subsector, FMCSA leverages GovDelivery, a web-based e-mail subscription management system, for providing news and information emails and posts notifications about jurisdiction-specific changes and updates in processes and guidelines. Notifications can span the following subtopics: Announcements & News, Registration & Licensing, Rules & Regulations, Rulemaking, Rulemaking Notices, and Outreach.

Question from Hon. Nikema Williams to Cordell Schachter, Chief Information Officer, U.S. Department of Transportation

Question 8. In last month's hearing on this topic, we heard about the need for local transportation agencies to assess their own level of "cyber maturity"—understanding what cyber protections they have and what protections they need. Drawing both on your experience in federal and local government, how can local transportation agencies best access support and resources from the Department of Transportation to assess and strengthen their own cyber protections?

Answer. Thank you for the opportunity to address the issues raised in this question. DOT has many resources publicly available to local transportation agencies to assess and strengthen their own cyber protections. For example, the following webpage lists documents with guidance on multiple cyber topics. https://rosap.ntl.bts.gov/gsearch?terms=cyber&maxResults=50&start=0

DOT's Federal Highway Administration (FHWA) regularly provides information about best practices gathered from agencies such as TSA and the National Institute of Standards and Technology. FHWA supports its stakeholders' work to improve their cybersecurity including reporting and responding to cybersecurity incidents and providing training and reference materials.

DOT has also been collaborating with CISA on establishing a common baseline of cyber performance goals for critical infrastructure control systems which will be finalized this summer. DOT will also be contributing to the transportation sector-specific cybersecurity performance goals which will build upon the common baseline and include goals specific to the transportation sector and subsectors. More information can be found here: https://www.cisa.gov/control-systems-goals-and-objectives

Questions from Hon. Frederica S. Wilson to Larry Grossman, Chief Information Security Officer, Federal Aviation Administration

Question 1. Mr. Grossman, in your statement, you mentioned the National Academy of Sciences study on the FAA's cybersecurity workforce, which was directed by Congress. The results of this study were received in June 2021. Please elaborate on the study's recommendations to increase workforce diversity and what specific objectives and action items the FAA has in place to achieve that goal.

Answer. The Federal Aviation Administration (FAA) recognizes the importance of recruiting efforts to attract a diverse pool of qualified employees. The agency's current initiatives include cybersecurity as part of a broader aviation-focused engagement. In the FAA's Science, Technology, Engineering, and Math (STEM) Aviation and Space Education (AVSED) program, youth from diverse backgrounds are inspired to pursue aerospace careers, including those that are cybersecurity-focused. The FAA currently leverages several federal hiring and personnel management authorities afforded to cyber-specific employees, such as on-the-spot hiring.

Pursuant to Section 549 of the FAA Reauthorization Act of 2018 (PL 115–254), the National Academy of Sciences (NAS) published a report examining the FAA's cybersecurity workforce challenges, reviewing the current strategy for meeting those challenges, and recommending ways to strengthen the FAA's cybersecurity workforce titled: "Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration".[1] FAA reviewed the NAS report and recently provided a report to Congress regarding the results of the study.[2] The challenges identified in the study,

[1] https://www.nap.edu/catalog/26105/looking-ahead-at-the-cybersecurity-workforce-at-the-federal-aviation-administration#.

[2] https://www.faa.gov/sites/faa.gov/files/2022-01/PL__115-254__Sec549__FAA__Response__to__Nat__Academy__Sciences__study__FAA__Cybersecurity__Workforce.pdf.

along with opportunities and recommendations, have validated existing FAA cyber workforce initiatives and inspired potential new initiatives. Through the six strategic outcomes, continued investment in existing initiatives, and promoting new programs developed as a result of this study, the FAA will strengthen its cybersecurity workforce today and in the future.

Question from Hon. Garret Graves to Larry Grossman, Chief Information Security Officer, Federal Aviation Administration

Question 2. I've read reports that there are some 500,000 vacancies for cybersecurity professionals in the U.S. workforce, making it nearly impossible for us to get a handle on the next generation of threats. Additionally, we've heard from industry that they feel that talent is relegated to SCIFs in the federal government, fusion centers, and big technology companies—preventing talent from being available to critical infrastructure at the local level. What can we be doing to rethink the workforce model for cybersecurity-specific professionals?

Answer. The Federal Aviation Administration (FAA) recognizes the challenging cybersecurity labor market, similar to many other organizations seeking to hire and retain cyber personnel. There are many programs in place in the federal government to accelerate and simplify the hiring process for cybersecurity personnel.

The FAA recognizes the importance of recruiting efforts to attract a diverse pool of qualified employees. The agency's current initiatives include cybersecurity as part of a broader aviation-focused engagement. In the FAA's Science, Technology, Engineering, and Math (STEM) Aviation and Space Education (AVSED) program, youth from diverse backgrounds are inspired to pursue aerospace careers. The program seeks to create a consistent pipeline of aerospace professionals for the workforce of the future, including those that are cybersecurity-focused.

While the FAA has some employees who work in a Sensitive Compartmented Information Facility (SCIF) environment very few members of our cybersecurity workforce are relegated to a SCIF, rather they will enter the SCIF only for classified discussions, then leave the secure area to engage with other FAA staff and aviation stakeholders as needed. Pursuant to Section 549 of the FAA Reauthorization Act of 2018 (PL 115–254), the National Academy of Sciences (NAS) published a report examining the FAA's cybersecurity workforce challenges, reviewing the current strategy for meeting those challenges, and recommending ways to strengthen the FAA's cybersecurity workforce titled: "Looking Ahead at the Cybersecurity Workforce at the Federal Aviation Administration".[3] FAA reviewed the NAS report and recently provided a report to Congress regarding the results of the study.[4] The challenges identified in the study, along with opportunities and recommendations, have validated existing FAA cyber workforce initiatives and inspired potential new initiatives. Through the six strategic outcomes, continued investment in existing initiatives, and promoting new programs developed as a result of this study, the FAA will strengthen its cybersecurity workforce today and in the future.

Questions from Hon. Michael Guest to Larry Grossman, Chief Information Security Officer, Federal Aviation Administration

Question 3. Each state has a designated CISA "Protective Security Advisor" that coordinates with members of the critical infrastructure community and works to help them prepare/defend against cyber-attacks. Can you tell me about the interface your agencies have with these Advisors and what role they play in your industries?

Answer. The Cybersecurity and Infrastructure Security Agency (CISA) Protective Security Advisor program is within the Department of Homeland Security (DHS). DHS serves as a tri-chair of the Aviation Cyber Initiative (ACI) with the Department of Defense and the Department of Transportation (DOT), with the Federal Aviation Administration (FAA) representing DOT. Through this partnership, we coordinate and collaborate with government and industry to improve cybersecurity protections and response capabilities. ACI focuses on cybersecurity protections within the aviation sub-sector of the critical infrastructure community and includes an active Community of Interest (COI) that includes over 1000 participants across the aviation ecosystem from both the public and private sector. COI participants include airlines and airfreight, aircraft and avionics manufacturers, aviation industry associations and service providers, academia, and Federally Funded Research and Development Centers. ACI includes both domestic and international participants as cy-

[3] https://www.nap.edu/catalog/26105/looking-ahead-at-the-cybersecurity-workforce-at-the-federal-aviation-administration#.

[4] https://www.faa.gov/sites/faa.gov/files/2022-01/PL__115-254__Sec549__FAA__Response__to__Nat__Academy__Sciences__study__FAA__Cybersecurity__Workforce.pdf.

bersecurity protections within the aviation community are a global concern. Current priorities of ACI include aviation cybersecurity risk mitigation efforts, cyber research and development, information sharing, cybersecurity training specific to the unique aspects of the aviation environment, and aviation cybersecurity exercises.

Question 4. Earlier this year, in discussions with CISA Director Inglis, we discussed the importance of protecting our digital infrastructure, its supply chain, and preventing overdependency of manufacturing critical digital goods by adversarial countries, which they could possibly use against us. How can the FAA and DOT work alongside private sector stakeholders and Congress to strengthen our digital infrastructure supply chain, industry standards, and enforcement of those standards when it comes to high level digital hardware?

ANSWER. The FAA and DOT continue to work in partnership with DHS and CISA through the ACI Tri-Chair relationship to create a balance between government and private partnerships. We also leverage industry expertise to develop and update industry standards relevant to aviation cybersecurity. An example is RTCA Special Committee SC–216, which is chaired by a representative industry stakeholder and has an FAA policy representative.[5] SC–216 recently revised their Aeronautical Systems Security standard (DO–365A). This past December, the committee also published a new standard, Aeronautical Information System Security Framework Guidance (DO–391). All of our efforts with Standards Development Organizations (SDO) are geared towards developing industry standards that can be used as an acceptable means of compliance to one or more of our certification requirements. SDOs, like RTCA, ASTM and SAE, often have counterpart working groups in the European standards development community, which provides additional expertise and a wider global acceptance of the developed standards.

Question 5. Director Inglis also emphasized the need for accountability in cybersecurity practices. Each one of you represents a different set of industry stakeholders with vastly different needs in this space. For bad actors within your jurisdiction that allow their cybersecurity measures to fall below public or industry standards, what are ways that Congress and your agencies can hold those folks accountable? Many stakeholders mention that they are more robust in developing cybersecurity measures and have been for decades. So, what are ways to hold bad actors accountable without installing mandates that may limit the private sector's own work in this space?

ANSWER. The FAA advises a cautious approach when considering any potential aviation-related cybersecurity mandates and highlights that any such mandates would need to provide sufficient flexibility, in terms of measures and timelines for implementing enhancements, to allow industry participants to appropriately protect the diverse range of systems used in the aviation sub-sector. The expected improvement to the industry's defenses from any mandate must also be carefully weighed against its associated costs, taking into account the highly sophisticated nature of some attacks.

Within the realm of the FAA's responsibility as the aviation safety regulator and air navigation service provider for the U.S., the FAA finds it much more successful to engage with our industry stakeholders to encourage the voluntary adoption of successful cyber-hygiene protocols. Our stakeholders are highly motivated to keep their systems secure from cyber-attacks, as breaches of vulnerable systems can equate to economic loss, loss of public trust, loss of efficiency and loss of market share. We must also remember that our stakeholders' systems and security needs vary widely and security solutions must be tailored—one size does not fit all.

Question 6. Many industry stakeholders utilize early notification networks. However, the public sector lacks a robust system to alert private carriers or shippers of an attack across the system. To critical infrastructure, the ability to limit damage seems crucial. Can you expand on how early notification networks are used by the private sector and why coordination with a federal government system is so important?

ANSWER. FAA regulations require reporting of a variety of aviation safety-related issues, but are generally agnostic as to their potential cause, which may be unknown at the time of initial reporting. DHS is the lead agency to receive private sector reports of cybersecurity incidents and to facilitate individual asset or whole of government response during a significant cyber incident. DHS's National Cybersecurity and Communications Center shares information across the public and private sectors (including the Aviation Information Sharing and Analysis Center) to protect against similar incidents in the future. The sharing of information is usually

[5] https://www.rtca.org/sc-216/.

in the form of Alerts/Advisories and Bulletins, Initial Network Analysis Reports and/or Cybersecurity Coordination Action and Response calls. These early notifications provide an opportunity for the government and private sector partners to minimize the impact of a cyberattack by proactively implementing protection mechanisms to block attacks while focusing monitoring on those assets that are potentially the most vulnerable.

The Department of Justice, through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, is the lead agency for threat response during a significant incident. With respect to aviation specifically, recent Transportation Security Administration updates to airport and aircraft operator security program requirements established cybersecurity incident reporting requirements for airports and aircraft operators with the relevant types of security programs.

QUESTIONS FROM HON. NIKEMA WILLIAMS TO LARRY GROSSMAN, CHIEF INFORMATION SECURITY OFFICER, FEDERAL AVIATION ADMINISTRATION

Question 7. Mr. Grossman, millions depend on both the services and economic activity from transportation systems in my district, and a disruption to one part of the system can impact the rest. A disruption to the Hartsfield Jackson Atlanta International Airport could reach from Delta Airlines to international travelers to aviation workers who live in my district. Could you please describe how the Federal Aviation Administration supports and shares information with airports like mine to help safeguard the transportation system that depends on them from a cyberattack?

ANSWER. The Federal Aviation Administration (FAA) participates in a variety of airport safety and security government partnerships and initiatives that identify and mitigate cyber threats to the nation's airports and collaborate with partner agencies to disseminate airport-related cyber threat information. In addition, Department of Homeland Security's (DHS) National Cybersecurity and Communications Center shares information across the public and private sectors to protect against cybersecurity incidents. Moreover, the Transportation Security Administration (TSA) recently published updated requirements regarding cybersecurity information sharing for the nation's airports. In addition, the FAA is one of the tri-chairs of the Aviation Cyber Initiative, and the FAA works collaboratively with DHS and Department of Defense to improve cybersecurity across the Aviation Ecosystem. This collaboration includes participants across the airports community.

Question 8. Mr. Grossman, Internet access is an airport essential. In 2018, Hartsfield-Jackson Atlanta International Airport's Wi-Fi connectivity had to be taken down amidst a city-wide cyberattack. Do you have any recommendations that will ensure airports can provide Internet access to travelers while minimizing their networks' vulnerability to cyberattacks?

ANSWER. While outside of FAA's mission set, FAA supports and encourages industry efforts for the development of cybersecurity risk management programs, information security standards and best practices consistent with the National Institute of Standards and Technology Cybersecurity Framework. The city-wide cyberattack in Atlanta was indeed a surprising and widespread outage. During a cyberattack, sometimes user connectivity may be affected for the protection of both the users and systems, any response to an event must be aligned with the potential impact associated with that event. TSA, who does have statutory authority over airport cybersecurity operations, recently published guidance for the nation's airports regarding cybersecurity. The Office of Airports, along with the rest of the FAA, is working closely with TSA to support their efforts.

QUESTION FROM HON. STEVE COHEN TO VICTORIA NEWHOUSE, DEPUTY ASSISTANT ADMINISTRATOR FOR POLICY, PLANS, AND ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Question 1. When traveling—especially while in airports, train stations, or buses—people often make use of public Wi-Fi connections, public charging ports, and other resources to keep their devices charged and connected to the internet. What precautions is TSA taking to oversee these services to prevent cyberattacks through public networks or to stop cybercriminals from setting up networks that mimic the genuine ones?

ANSWER. The Transportation Security Administration (TSA) recently issued cybersecurity requirements to operators in the aviation, surface, and pipeline modes of transportation, including cybersecurity incident reporting requirements. While these requirements vary to some extent based on the operational requirements of each mode, all are aimed at establishing a baseline of cybersecurity protection. To the extent a public-facing Wi-Fi network is under the control of a covered owner/operator, it may be subject to the new requirements.

Public networks, Wi-Fi connections, or other internet connections provided, operated, and maintained by persons who are not covered by the cybersecurity requirements noted above are not regulated by TSA.

The federal government continues to review and analyze cybersecurity requirements within the various transportation modes. To the extent not covered by existing requirements for aviation and surface operators, we may consider additional measures to ensure Information Technology and Operational Technology systems operated and maintained by third-party vendors and contractor meet appropriate security standards.

QUESTIONS FROM HON. SAM GRAVES TO VICTORIA NEWHOUSE, DEPUTY ASSISTANT ADMINISTRATOR FOR POLICY, PLANS, AND ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Question 2. Now that TSA has issued its security directive for railroads, transit, and passenger rail, will TSA work with the affected industries to develop guidance and other helpful materials to ensure the contents and requirements of the Security Directives are well understood and to support compliance with their mandated actions and measures? How will this be done?

ANSWER. TSA offers assistance to surface transportation owners/operators in understanding and complying with the security measures identified within the Security Directives (SDs) through a variety of means. TSA has and will continue to host industry calls with surface transportation owner/operators discussing the provisions within the SDs. The calls provide an opportunity for TSA to answer questions to ensure understanding of the requirements and support compliance with the defined security measures. Within each SD, an email address is provided to allow industry to contact TSA should they have questions. As common-themed questions are identified, TSA issues Frequently Asked Questions (FAQs) to all applicable owner/operators. TSA also has developed and will supplement guidance documents to provide additional support to covered entities. TSA will also work with the trade associations representing the covered owner/operators to provide informational webinars and share best practices for implementing the provisions of the SDs.

Question 3. TSA's *Security Directive Pipeline—2021–02: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (SD 02) requires covered pipeline owner/operators to implement mitigation measures by certain dates. To better understand TSA's implementation of this program, operator compliance with its requirements, the feasibility of TSA's program and the ability of TSA to implement it as designed, please provide performance data for the following metrics:

a. The number of covered pipeline owner/operators (operators);

ANSWER. 97

b. The number of operators in full compliance with measures with a 30-day implementation due date, a 90-day implementation due date, and a 120-day implementation due date;

ANSWER. 63 compliant with 30 days; 22 compliant with 90 days; 30 compliant with 120 days. 11 compliant with all measures (30, 90, and 120-day).

c. The number of operators proposing alternative measures for measures with a 30-day implementation due date;

ANSWER. 12

d. The number of alternative measure proposals for measures with a 30-day implementation due date;

ANSWER. 15

e. The number of alternative measure proposals for measures with a 30-day implementation due date that TSA has accepted;

ANSWER. 0

f. The number of alternative measures proposals for measures with a 30-day implementation due date that TSA has rejected;

ANSWER. 2

g. The number of alternative measures proposals for measures with a 30-day implementation due date that TSA is still reviewing;

ANSWER. 13

h. The number of operators proposing alternative measures for measures with a 90-day implementation due date:

ANSWER. 44

i. The number of alternative measures proposals for measures with a 90-day implementation due date:
ANSWER. 93

j. The number of alternative measures proposals for measures with a 90-day implementation that TSA has started reviewing;
ANSWER. 93

k. The number of alternative measures proposals for measures with a 90-day implementation due date that TSA has accepted;
ANSWER. 3

l. The number of alternative measures proposed for measures with a 90-day implementation due date that TSA has rejected:
ANSWER. 0

m. The number of alternative measures proposed for measures with a 90-day implementation due date that TSA is still reviewing:
ANSWER. 93

n. The number of operators proposing alternative measures for measures with a 120-day implementation due date;
ANSWER. 20

o. The number of alternative measures proposals for measures with a 120-day implementation due date;
ANSWER. 21

p. The number of alternative measures proposals for measures with a 120-day implementation that TSA has started reviewing:
ANSWER. 21

q. The number of alternative measures proposals for measures with a 120-day implementation due date that TSA has accepted;
ANSWER. 0

r. The number of alternative measures proposed for measures with a 120-day implementation due date that TSA has rejected;
ANSWER. 0

s. The number of alternative measures proposed for measures with a 120-day implementation due date that TSA is still reviewing;
ANSWER. 21

t. The number of operators requesting additional time for measures with a 30-day implementation due date;
ANSWER. 37

u. The number of requests for additional time for measures with a 30-day implementation due date:
ANSWER. 55

v. The number of requests for additional time for measures with a 30-day implementation due date that TSA has accepted;
ANSWER. 55

w. The number of requests for additional time for measures with a 30-day implementation due date that TSA has rejected:
ANSWER. 0

x. The number of requests for additional time for measures with a 30-day implementation due date that TSA is still reviewing:
ANSWER. 0

y. The number of operators requesting additional time for measures with a 90-day implementation due date:
ANSWER. 65

z. The number of requests for additional time for measures with a 90-day implementation due date:
ANSWER. 361 (total measures from 65 companies).

aa. The number of requests for additional time for measures with a 90-day implementation that TSA has started reviewing:
ANSWER. 361

bb. The number of requests for additional time for measures with a 90-day implementation due date that TSA has accepted;

ANSWER. 284 (Action Plan Letters have been sent)

cc. The number of requests for additional time for measures with a 90-day implementation due date that TSA has rejected;

ANSWER. 0

dd. The number of requests for additional time for measures with a 90-day implementation due date that TSA is still reviewing

ANSWER. 77 (Action Plan letters still need to be drafted).

ee. The number of operators requesting additional time for measures with a 120-day implementation due date;

ANSWER. 57

ff. The number of requests for additional time for measures with a 120-day implementation due date;

ANSWER. 99

gg. The number of requests for additional time for measures with a 120-day implementation that TSA has started reviewing;

ANSWER. 99

hh. The number of requests for additional time for measures with a 120-day implementation due date that TSA has accepted;

ANSWER. 22

ii. The number of requests for additional time for measures with a 120-day implementation due date that TSA has rejected; and,

ANSWER. 0

jj. The number of requests for additional time for measures with a 120-day implementation due date that TSA is still reviewing.

ANSWER. 77

QUESTIONS FROM HON. ERIC A. "RICK" CRAWFORD TO VICTORIA NEWHOUSE, DEPUTY ASSISTANT ADMINISTRATOR FOR POLICY, PLANS, AND ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Question 4. A major concern we've heard about the pipeline security directives was that they were developed without meaningful input from stakeholders with expertise in pipeline safety and operations, creating implementation issues. For instance, some pipelines need to shut down operations to implement the requirements. When the Colonial pipeline shut down, the effects were felt across the entire southeast when energy prices increased as people lost access to critical energy products.

a. How is TSA ensuring it will have the resources and technical expertise to address technical issues for these and potential future rulemakings and security directives?

ANSWER. TSA partnered with the Cybersecurity and Infrastructure Security Agency (CISA), the United States Coast Guard (USCG), the U.S. Department of Energy (DOE), and the Pipeline and Hazardous Materials Safety Administration (PHMSA) of the U.S. Department of Transportation (DOT) in the development of SDs to ensure the utilization of high-level technical expertise from other federal agencies. In addition to interagency support, TSA has and will continue to seek input from subject matter experts from the pipeline industry.

CISA remains engaged in providing cybersecurity subject matter expertise in support of the SD implementation process. TSA is leveraging CISA guidance and assessments to conduct further mode-specific research and identify mechanisms to obtain stakeholder cyber measures, determine gaps, and work with the National Risk Management Center to develop a prioritized list of cyber risks. In addition, TSA has recently hired cybersecurity specialists to work both in policy and operations.

- Between October and November 2021, TSA Security Operations, Surface Operations established a new Cybersecurity Branch to conduct and facilitate surface cybersecurity related assessments and outreach efforts. Ten of the eleven cybersecurity expert positions have been filled. In addition to the establishment of this Branch, there are five Transportation Security Inspectors currently undergoing cybersecurity specialized training to become cyber assessors.
- TSA created a Cybersecurity section within the Policy, Plans, and Engagement Surface Policy Division, Industry Engagement Branch. This section is led by one Section Chief and supported by seven cybersecurity specialists. This section coordinates with Surface Operation's new Cybersecurity Branch, CISA, and other

subject matter experts to ensure vulnerability information, guidance, and mitigation measures are shared as appropriate.

b. How is TSA leveraging the expertise of other federal agencies, such as DOT, in development and implementation of its security directives and cybersecurity requirements for the transportation sectors?

ANSWER. TSA continues to leverage the subject matter expertise within the Department of Homeland Security, including CISA, as well as the DOT's modal administrations for both surface and aviation transportation. All of these federal partners provided crucial input into the development of the TSA Cyber SDs and Information Circular. Furthermore, all parties provided detailed information on the specifics of these Cyber SDs and Information Circular to surface transportation stakeholders through numerous conference calls and other industry engagements. TSA, CISA, DOT, and other partners continue to provide opportunities for industry to raise concerns, ask questions, or request additional clarification through direct contact with TSA. TSA coordinates the appropriate responses with federal partners to ensure the industry receives responses needed to support successful implementation of the Cyber SDs and Information Circular actions.

In the case of pipelines, TSA partnered with CISA, USCG, DOE, and PHMSA in the development of those SDs. The SDs include a provision that allows operators to raise any safety concerns associated with SD implementation, which are then shared with PHMSA for review and feedback.

Question 5. The previous mandatory directives for pipelines followed the Colonial Pipeline ransomware attack. What incident or security threats are necessitating a mandatory security directive and requirements for freight rail, transit, and aviation? How does TSA plan to ensure ongoing timely and secure communications about cyber threats to the transportation and infrastructure sectors?

ANSWER. Cyber threats from attackers remain acute. Attackers use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure. The Director of National Intelligence has stated that our adversaries and strategic competitors possess cyberattack capabilities they could use against U.S. critical infrastructure, including U.S. transportation. Additionally, nation states' increasing use of cyber operations as a tool of national power, including increasing use by militaries around the world, raises the prospect of more destructive and disruptive cyber activity against all U.S. critical infrastructure, including transportation.

We remain concerned about the disruptive impacts of ransomware attacks, as demonstrated by the Colonial Pipeline attack. The U.S. Department of Homeland Security (DHS) stated in late 2020 that ransomware attacks—which have at least doubled since 2017—are often directed against critical infrastructure entities at the state and local level by exploiting gaps in cybersecurity, and that cybercriminals will increasingly target U.S. critical infrastructure to generate profit, including through ransomware.

Cyber actors have demonstrated their willingness to conduct cyber-attacks against critical infrastructure by exploiting the vulnerability of Internet-accessible Operational Technology (OT) assets and Information Technology (IT) systems. As shown by recent ransomware attacks, the United States' adversaries and strategic competitors will continue to use cyber espionage and cyberattacks to seek political, economic, and military advantage over the United States and its allies and partners.

Cybersecurity incidents affecting surface transportation are a growing threat. Given the multitude of connected devices already in use by the surface transportation industry and the vast amount of data generated (with more coming online soon), protecting the higher-risk freight railroads, passenger railroads, and rail transit systems has become an increasing critically important and complex undertaking to protect critical infrastructure from malicious cyber-attack and other cybersecurity-related threats.

As an example: In April 2021, hackers breached several computer systems of the Metropolitan Transportation Authority, the nation's largest mass transit agency that transports millions of people in and around New York City every day. The intrusion was discovered in late April when hackers linked to the Chinese government exploited security flaws in Pulse Connect Secure, a Virtual Personal Network that allows employees to connect remotely to their employer's network. The cyberattack impacted three of the transit agency's 18 systems.

TSA also continues to share the most relevant and timely information with surface transportation stakeholders to counter this persistent threat. Most recently, a joint cybersecurity advisory from the Federal Bureau of Investigation (FBI), CISA, the Australian Cyber Security Centre, and the United Kingdom's National Cyber Security Centre highlighted ongoing malicious cyber activity by an advanced persistent threat (APT) group associated with the government of Iran. The advisory cited: "The Iranian government-sponsored APT actors are actively targeting a broad range of victims across multiple U.S. critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector, as well as Australian organizations."

TSA has a number of methods to provide timely security communications to regulated parties. The primary means is through the Homeland Security Information Network (HSIN), by which regulated entities have access to their appropriate security web-board. These web-boards house security requirements, intelligence reports, frequently asked questions, information circulars, advisories, and other communications. TSA also routinely invites impacted regulated parties to receive classified and unclassified briefings on ongoing threats. TSA also has a number of working groups through which information is shared.

With regard to ensuring ongoing and timely communications about cyber threats are provided to the transportation and infrastructure sectors, TSA continues to bolster its intelligence information sharing efforts. TSA has also partnered with aviation and surface stakeholders to increase two-way sharing of cyber security threats to critical infrastructure. This includes the creation and resourcing of two full-time threat intelligence cells: the Aviation Domain Intelligence Integration & Analysis Cell and the Surface Information Sharing Cell. TSA's Field Intelligence Officers also routinely engage with stakeholders around the country directly by passing threat information and providing tailored classified and unclassified threat briefings.

Since the issuance of the SDs, TSA collaborated with the White House National Security Council and the Office of Director of National Intelligence to provide SD-impacted pipeline senior executives with classified threat information. TSA also provided classified briefings to pipeline Chief Executive Officers and Chief Information Officers/Chief Information Security Officers at TSA Headquarters. The TSA Headquarters briefings were a combined effort between TSA, CISA, and FBI. TSA will continue to provide classified briefings twice a year for pipeline owner/operators.

TSA also provided a security briefing to members of the Freight Rail and Passenger Rail industries impacted by the Rail SDs. Plans call for additional security briefings for rail industry representatives on a recurring basis.

With respect to airport operators and aircraft operators, TSA, under 49 CFR sections 1542.303(a) and 1544.305(a), has the ability to issue mandatory measures when the agency determines that "additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation." In the case of aviation requirements, TSA is opting to issue new requirements under TSA's standard "Amendment by TSA" process (see 49 CFR sections 1542.105(c) and 1544.105(c)). An Amendment by TSA may be issued "if the safety and the public interest require an amendment." This process does not require there to be an imminent security threat or incident to have occurred to issue new security measures.

Question 6. Does TSA or other federal agencies share any analysis of information provided by the transportation and infrastructure sectors on cyber incidents, threats, or vulnerabilities? Will the information these industries are required to report to DHS be analyzed and shared to help bolster their cyber risk management?

ANSWER. Presidential Policy Directive (PPD) 41 calls for Federal cyber incident response agencies to share incident information with each other to achieve unity of governmental effort (see PPD–41 § III.D). Information provided to CISA pursuant to the SDs will be shared by CISA with TSA and also shared with the National Response Center and other agencies as appropriate.

TSA is leveraging CISA guidance and assessments to conduct further mode-specific research and identify mechanisms to obtain stakeholder cyber measures, determine gaps, and work with the National Risk Management Center to develop a prioritized list of cyber risks.

TSA has shared lessons learned from the first pipeline Security Directive (SD01) with industry representatives via stakeholder calls and trade association meetings.

When TSA issued the requirements for reporting cybersecurity incidents, the regulated parties were told that the information provided to the CISA and to TSA may be used in reports. Specifically, it said "TSA may use the information, with company-specific data redacted, for TSA's intelligence-derived reports. TSA and CISA also may use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents."

TSA has a number of methods to communicate timely and secure communications to regulated parties. The primary means is through the HSIN, by which regulated entities have access to their appropriate security web-board. These web-boards house security requirements, intelligence reports, frequently asked questions, information circulars, advisories, and other communications. TSA also routinely invites impacted regulated parties to receive classified and unclassified briefings on ongoing threats. TSA also has a number of outlets by which to share information such as trade associations and their cybersecurity workgroups, sector coordinating councils, and information sharing and analysis centers. Through the use of HSIN, briefings, and those various information sharing outlets, industry stakeholders are provided with multiple facets to increase awareness of current events, and identified cybersecurity threats and vulnerabilities.

QUESTIONS FROM HON. SETH MOULTON TO VICTORIA NEWHOUSE, DEPUTY ASSISTANT ADMINISTRATOR FOR POLICY, PLANS, AND ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Question 7. Ms. Newhouse, new cybersecurity requirements for rail carriers were announced the day of this hearing, which includes designating a cybersecurity coordinator, reporting hacking incidents within 24 hours, conducting a vulnerability assessment, and developing an incident-response plan for breaches. During our previous cybersecurity hearing, the rail industry representative seemed opposed to federal regulations regarding cybersecurity mandates in the private sector. Can you explain why the rail industry is considered high-risk and in need of this directive? What benefits do you expect from mandating these new measures compared to voluntary guidance?

ANSWER. Cybersecurity incidents affecting surface transportation entities are a growing threat that pose a risk to the national and economic security of the United States. The cybersecurity security directives were issued to the rail industry (higher risk freight railroads, passenger railroads, and rail transit agencies) due to their criticality to the nation's economy and national defense. These entities transport the largest volumes of cargo and people and have been the targets of cyber threat actors. While many of these entities have initiated protective measures for enhanced cybersecurity, TSA determined that there was a need to establish a baseline of practices such as those included in the security directives.

The surface transportation industry utilizes a multitude of connected devices and generates vast amounts of data. Malicious actors have increasingly demonstrated the capability to conduct cyber-attacks exploiting the vulnerabilities of Internet-accessible OT assets and IT systems. In recent years, cyber attackers have maliciously targeted the critical infrastructure of surface transportation modes in the U.S., including freight railroads, passenger railroads, and rail transit systems, with multiple cyberattack and cyber espionage campaigns.[1] By targeting the integrated cyber and physical infrastructure of surface transportation entities, these actions threaten the safe, secure, and uninterrupted daily operation of surface transportation systems relied upon by the U.S. economy with potential to cause nation-wide impact. Given the significant ongoing threat to the surface transportation sector, protecting the higher-risk freight railroads, passenger railroads, and rail transit systems from malicious cyber-attack and other cybersecurity-related threats is critically important to safeguarding the nation's critical infrastructure. To counter this threat, TSA determined that the requirements of Security Directive 1580–21–01 and Security Directive 1582–21–01 were urgently needed to protect the surface transportation sector by mitigating and eliminating cybersecurity vulnerabilities.

Congress granted the TSA Administrator broad statutory responsibility and authority with respect to the security of the transportation system. Under the authorities of 49 U.S.C. section 114, TSA may take immediate action to impose measures to protect transportation security without providing notice or an opportunity for comment. This provision specifically recognizes that there are times when action is necessary that does not provide for the rather lengthy process necessary to issue a notice of proposed rulemaking and finalize a rule.

[1] These activities include the April 2021 breach of New York City's Metropolitan Transportation Authority (the nation's largest mass transit agency) by hackers linked to the Chinese government; the December 2020 "Sunburst" attack on transit agencies; the August 2020 attack on the Southeastern Pennsylvania Transportation Authority; the 2017 ransomware attack on the Sacramento Regional Transit District; and the November 2016 ransomware attack on the San Francisco Municipal Transportation agency. This threat is ongoing: on November 17, 2021 the FBI, CISA, the Australian Cyber Security Centre, and the United Kingdom's National Cyber Security Centre issued a joint cybersecurity advisory highlighting ongoing malicious cyber activity by an APT that these agencies associated with the government of Iran. The advisory states that "The Iranian government-sponsored APT actors are actively targeting a broad range of victims across multiple U.S. critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector, as well as Australian organizations." Alert AA21–321A (November 17, 2021).

TSA's regulations identify higher-risk owner/operators of freight railroads, passenger railroads, and rail transit operations. These determinations align with DHS's official definition of risk as the "potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence." TSA has determined that the higher-risk freight railroads are those designated as Class I based on their revenue (over $72.9 billion in 2013), as well as any freight railroad that transports one or more of the categories of Rail Security-Sensitive Materials in a high threat urban area. The Nation depends on these systems to move freight in support of critical sectors and passengers.

TSA has determined the higher-risk rail transit systems and passenger railroads in the context of resource allocations under the Transit Security Grant Program using a model approved by the DHS Secretary and vetted by Congress. These systems are all located in high threat urban areas and carry the most passengers as a percentage of daily ridership totals.

Although TSA continues to work with these industries to develop and implement cybersecurity measures voluntarily, the industries have not achieved 100 percent adoption of the recommended measures. To establish a baseline of behavior for higher-risk operations to protect against cyber-actors and ongoing cyberattacks against the transportation sector, TSA worked with both private-sector and public-sector partners to identify existing vulnerabilities, develop mitigation strategies and cybersecurity measures, and install response and restore protocols to more quickly address immediate threats through security directives. Entities not covered by the security directives are still recommended to implement the same measures through voluntary actions.

In accordance with the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (Jul 29, 2021), TSA has issued these Security Directives due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to prevent against the significant harm to the national and economic security of the United States that could result from the "degradation, destruction, or malfunction of systems that control this infrastructure." In order to mitigate these threats, TSA believes mandatory measures will ensure industry is taking appropriate actions to mitigate potential vulnerabilities from the ongoing cybersecurity threats.

QUESTIONS FROM HON. GARRET GRAVES TO VICTORIA NEWHOUSE, DEPUTY ASSISTANT ADMINISTRATOR FOR POLICY, PLANS, AND ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Question 8. Your testimony discusses information sharing between TSA and the USCG to identify and manage threats in the Maritime Transportation System (MTS). How does TSA communicate threats to our individual ports as part of the effort to manage risks in the MTS?

ANSWER. USCG has primary responsibility to manage threats in the Maritime Transportation System (MTS). If TSA has relevant threat information affecting the MTS, it is made available to the USCG. TSA also receives relevant threat information from the USCG for awareness. TSA Surface inspectors and Field Intelligence Officers participate in the quarterly Area Maritime Security Committee meetings, which include facility security officers and other maritime stakeholders to share intelligence and current maritime security and safety issues. Surface inspectors also attend other maritime-related association meetings at the local ports where similar information is shared.

Question 9. I've read reports that there are some 500,000 vacancies for cybersecurity professionals in the U.S. workforce, making it nearly impossible for us to get a handle on the next generation of threats. Additionally, we've heard from industry that they feel that talent is relegated to SCIFs in the federal government, fusion centers, and big technology companies—preventing talent from being available to critical infrastructure at the local level. What can we be doing to rethink the workforce model for cybersecurity-specific professionals?

ANSWER. Cybersecurity touches all modes of critical infrastructure, including transportation. TSA is working to expand the cybersecurity workforce in a number of capacities including hiring cybersecurity professionals to our Policy and Operational teams. Expanding TSA's cyber threat analysis footprint supports TSA efforts to enhance cyber-related intelligence analyses and products covering all modes of transportation; strengthen cyber threat analysis by developing integrated, repeatable processes for identification, analysis and sharing of cyber incidents; and increase the engagement and sharing of intelligence with stakeholders. Moving forward, the goal of all federal agencies is to assist efforts private industry and at state and local levels by ensuring information is classified at the lowest possible level, which make information more accessible.

While DHS and TSA cannot directly influence the ability of transportation providers to hire and retain cybersecurity professionals, there may be options to create training and educational opportunities that transportation providers could leverage to assist in the development of their own workforces.

QUESTIONS FROM HON. MICHAEL GUEST TO VICTORIA NEWHOUSE, DEPUTY ASSISTANT ADMINISTRATOR FOR POLICY, PLANS, AND ENGAGEMENT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Question 10. Each state has a designated CISA "Protective Security Advisor" that coordinates with members of the critical infrastructure community and works to help them prepare/defend against cyber-attacks. Can you tell me about the interface your agencies have with these Advisors and what role they play in your industries?

ANSWER. TSA works with both Protective Security Advisors (PSA) and Cybersecurity Advisors (CSA) from CISA. TSA partnerships with regional CSAs across the U.S. allow for an expanded coordination of expertise and outreach into the transportation sector community. TSA has collaborated at the regional level with CSAs in conducting a wide variety of stakeholder and trade association cybersecurity related workshops. Along with the CSA relationships, TSA is establishing a surface transportation cyber information sharing network through the development of the Surface Information Sharing Cell serving as the hub, with spokes assuring engagement with organizations, including CISA and voluntary industry partnerships, in each surface transportation mode with necessary analytical support.

In one specific example of recent coordination, TSA partnered with CISA PSAs to help raise industry awareness and to promote pipeline owner/operators' participation in the Validated Architecture Design Review program.

Question 11. Many industry stakeholders utilize early notification networks. However, the public sector lacks a robust system to alert private carriers or shippers of an attack across the system. To critical infrastructure, the ability to limit damage seems crucial. Can you expand on how early notification networks are used by the private sector and why coordination with a federal government system is so important?

ANSWER. Public/private partnerships are critical to prevent, protect, mitigate, respond, and recover from cyber-actors' attempts to disrupt the transportation sector or from ongoing cyberattacks to IT and OT systems. These partnerships are important for a number of reasons. First, information sharing. As a repository to collect information on cybersecurity incidents, the federal government is able to effectively analyze the information and send it out to other impacted or potentially impacted parties. This may help to mitigate the impact of an incident. Second, understanding incident impact/scope. From the point of view of the impacted party, it may be difficult to understand the scope of an incident. By sharing, the federal government is able to piece together disparate pieces of information and fully understand the full impact of an incident. Third, coordinated response. The federal government's role in a cybersecurity incident will be to coordinate the response effectively at the federal level, and all the way down to the local level. In each of these cases, it is important to keep in mind that all of this is possible due to the relationships built between government agencies, as well as with private companies.

TSA continues to work with federal government partners and private-sector transportation stakeholders to limit cyber related disruptions. TSA routinely coordinates the sharing of both non-classified and classified security information as appropriate with its transportation sector partners. This includes the identification of new vulnerabilities and the sharing of known mitigation measures to close the identified security gaps.

Additionally, as recommended by the Surface Transportation Security Advisory Committee to the TSA Administrator, TSA has begun to establish a surface transportation cyber information sharing network on threats, incidents, and security concerns and related alerts, advisories, analyses, and assessments. This includes the establishment of the Surface Information Sharing Cell to serve as the hub, with spokes assuring engagement with organizations in each surface transportation mode, for the exchange of reporting, analyses, advisories, and alerts on cyber threats, incidents, and security concerns—with necessary analytical support.

QUESTIONS FROM HON. FREDERICA S. WILSON TO REAR ADMIRAL JOHN W. MAUGER, ASSISTANT COMMANDANT FOR PREVENTION POLICY, U.S. COAST GUARD

Question 1. Admiral Mauger: Thank you for your service and today's testimony. As chair of the Florida Ports Caucus and a strong supporter of PortMiami in South Florida, protecting the maritime industry is very important to me. You mentioned that MTSA-regulated vessels and facilities are required to report transportation security incidents, breaches of security, and suspicious activity without delay. How effective has this provision been in helping the Coast Guard protect our maritime industry and could similar provisions help improve cybersecurity in other transportation sectors?

ANSWER. The timely reporting of Transportation Security Incidents (TSI), Breaches of Security, and Suspicious Activity, to include cyber incidents, by regulated vessels and facilities has proven effective and allowed the Coast Guard to respond and, where necessary, deploy resources, while also coordinating with other agencies as appropriate. In 2016, the Coast Guard released a policy letter expanding on the regulatory requirement for cyber incident reporting, which includes more information on how to identify whether a cyber-incident is considered a TSI, Breach of Security, or Suspicious Activity. This policy letter also outlines that Coast Guard regulated entities can report incidents to the Cybersecurity and Infrastructure Security Agency (CISA) in lieu of the Coast Guard. This is similar to the reporting mechanism established through the Transportation Security Administration's security directives. This policy remains in effect today, and the Coast Guard may further refine it as government and industry experience with cyber incident reporting continues to grow. Details from a reported cyber incident, after vetting, may be incorporated into a Maritime Cyber Alert or other suitable messaging to share with the broader community to raise awareness of potential threats, vulnerabilities, and consequences to the Marine Transportation System (MTS), or through CISA to all sectors of critical infrastructure.

The provisions are only mandatory for vessels and facilities subject to Maritime Transportation Security Act of 2002 (MTSA), which does not capture all components of the MTS. Similar provisions could improve cybersecurity awareness in other transportation sectors, or for a broader portion of the MTS, so long as reporting requirements are clear. This is particularly the case if multiple agencies have a role in regulations and oversight of a transportation sector. The Administration also supports efforts to mandate the reporting of cyber incidents to critical infrastructure and the timely sharing of those incidents with Sector Risk Management Agencies.

QUESTIONS FROM HON. GARRET GRAVES TO REAR ADMIRAL JOHN W. MAUGER, ASSISTANT COMMANDANT FOR PREVENTION POLICY, U.S. COAST GUARD

Question 2. Your testimony discusses information sharing between the U.S. Coast Guard and TSA to identify and manage threats in the Maritime Transportation System (MTS). How does the USCG communicate threats to our individual ports as part of the effort to manage risks in the MTS?

ANSWER. The Coast Guard leverages several mechanisms for communicating threats to our ports and MTS stakeholders, whether the threats are to the MTS at-large, or to specific stakeholders. Communication can take the shape of Marine Safety Information Bulletins, Maritime Cyber Alerts, Coast Guard messages, articles, etc. Dissemination of the information, regardless of form, can go through multiple avenues based on need. These include Area Maritime Security Committees, Port Security Specialists and Cyber Coordinators/Advisors at the Area, District, and Sector level to pass information to their network of contacts, CISA, the Maritime Transportation System Information Sharing and Analysis Center (MTS–ISAC), Partners within the Government Coordinating Council and Sector Coordinating Council, and through other Sector Risk Management Agencies.

Question 3. Lack of resources and personnel has been a hurdle for the U.S. Coast Guard to adapt to securing the MTS from cyber threats as opposed to traditional facilities security. Has the U.S. Coast Guard investigated opportunities to coordinate (and consolidate) its existing cybersecurity initiatives across U.S. Coast Guard mission areas?

ANSWER. The Coast Guard continually reviews opportunities to coordinate and consolidate new and existing cybersecurity initiatives across mission areas. The Service recently published the 2021 Cyber Strategic Outlook (CSO), which charts the path to meet the challenges of a rapidly evolving cyber domain. Key to the CSO are three lines of effort: (1) Defend and Operate the Enterprise Mission Platform, (2) Protect the Marine Transportation System, and (3) Operate In and Through Cyberspace. The Coast Guard continues to operationalize Marine Transportation

System cyber risk management from the headquarters program level to the port level, including the incorporation of cybersecurity into the Service's prevention and response framework.

Question 4. The U.S. Coast Guard uses the FEMA National Incident Management System (NIMS) for physical security. Is the Coast Guard working with FEMA to update NIMS to respond to cyber incidents?

ANSWER. Yes. The Coast Guard is working with other U.S. Department of Homeland Security components, including the Federal Emergency Management Agency and CISA, to examine the application of the National Incident Management System as well as the National Cyber Incident Response Plan to cyber incident response.

Question 5. It is my understanding that there is a current U.S. Coast Guard-led Research and Development effort to develop a Threat Intelligence Partnership for the Maritime Transportation System. Could you provide an update on this partnership and detail how this system is anticipated to be deployed to protect the MTS?

ANSWER. The Threat Intelligence Partnership is a Research and Development effort to develop technology that improves data analytics and information systems to better inform Marine Transportation System entities of threats and provide recommended actionable improvements to security. The system concept is in the early stages of development with additional analysis required to determine when a production system might be available. The project, and the experience of developing it thus far, has confirmed a need to improve collaboration with U.S. Government partners in the areas of critical infrastructure, cybersecurity, homeland security, and maritime commerce.

This project is sponsored by Coast Guard Intelligence, funded by the Naval Information Warfare Command, contracted through the Naval Research Laboratories, and involves Louisiana State University and the Stevenson Technology Corporation.

Question 6. The Maritime Transportation System community wants actionable guidance from the U.S. Coast Guard on what they need to be doing to protect against an ever more diverse set of cyber threats. Has the U.S. Coast Guard investigated opportunities to provide (or require) cybersecurity training to our maritime industries and ports, as the U.S. Coast Guard currently requires trainings on physical and facilities security?

ANSWER. Per Title 33 of the Code of Federal Regulations, vessel and facility security personnel and non-security personnel can obtain baseline security knowledge requirements through training or equivalent job experience. Existing guidance in NVIC 01–20 "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities" recommends that Facility Security Plans describe how cybersecurity is included as part of personnel training, policies, and procedures, and how this material will be kept current and monitored for effectiveness.

There is no Coast Guard-developed or approved cybersecurity training for industry. The Coast Guard shares local training opportunities through Area Maritime Security Committees at the port level.

The Coast Guard will consider training requirements as it evaluates future cyber regulations for the marine transportation system.

Question 7. I've read reports that there are some 500,000 vacancies for cybersecurity professionals in the U.S. workforce, making it nearly impossible for us to get a handle on the next generation of threats. Additionally, we've heard from industry that they feel that talent is relegated to SCIFs in the federal government, fusion centers, and big technology companies—preventing talent from being available to critical infrastructure at the local level. What can we be doing to rethink the workforce model for cybersecurity-specific professionals?

ANSWER. The Coast Guard is working to ensure the Service's cyber workforce is well-trained, effective, and retains talent using workforce retention interventions (bonuses) for active duty and civilian members to provide compensation commensurate to civilian counterparts. Additionally, the Coast Guard is augmenting the cyber workforce with Reserve and Auxiliary members to ensure adequate surge capacity and providing opportunities to attain sought after certifications and training opportunities within the Cyberspace operations. The Coast Guard's workforce management initiatives continue to evolve to meet the demands of a fast paced and growing cyber community and our cyber professionals are fully prepared to meet the Service's needs.

QUESTIONS FROM HON. MICHAEL GUEST TO REAR ADMIRAL JOHN W. MAUGER, ASSISTANT COMMANDANT FOR PREVENTION POLICY, U.S. COAST GUARD

Question 8. In your testimony you reference a shared responsibility between Coast Guard and private industry. You list "conducting vulnerability assessments," "Exercising plans," and "reporting cyber incidents" as ways Coast Guard CYBER interacts with industry stakeholders to boost or assess cybersecurity plans. On October 1, the Coast Guard launched reviews of Facility Security Assessments and Facility Security Plans of MTSA-regulated facilities (Maritime Transportation Security Act).

a. Prior to this initiative, could you give me a percentage of facilities that actively cooperated with Coast Guard on these plans?

ANSWER. Beginning October 1st, 2021, facilities were required to have cybersecurity incorporated, along with physical security, at their first annual audit. Before that, the Coast Guard did not have clear visibility as to whether or not facilities incorporated cybersecurity into their overall security posture. Some facilities opted to include cybersecurity in their required Facility Security Assessments and Facility Security Plans, but the number is estimated to be less than 2 percent, and the degree to which cybersecurity was incorporated varied from facility to facility. Additionally, a lack of cybersecurity inclusion in Facility Security Assessments (FSA) and Facility Security Plans (FSP) does not necessarily mean that some facilities were not still considering cybersecurity.

b. Additionally, is there any incentive or penalties for facilities if they do not conduct assessments or adhere to industry standards if they are attacked, especially for MTSA-regulated facilities?

ANSWER. Facilities were provided with a 1-year period, ending September 30, 2022, to incorporate cybersecurity into their FSAs and FSPs, since no previous guidance existed. Beginning October 1, 2022, all facilities must be in compliance, and will be subject to action by Captains of the Ports (COTP) in cases of non-compliance. Options available to COTPs include issuing deficiencies, imposing fines, and civil penalties. The COTP may place operational controls on the facility and/or seek enforcement actions (Letter of Warning, Notice of Violation, Civil Penalty) on the owner/operator of the MTSA-regulated facility.

Question 9. The National Cyber Director, Director Chris Inglis, also emphasized the need for accountability in cybersecurity practices. Each one of you represents a different set of industry stakeholders with vastly different needs in this space.

a. For bad actors within your jurisdiction that allow their cybersecurity measures to fall below public or industry standards, what are ways that Congress and your agencies can hold those folks accountable?

ANSWER. Title 33, Code of Federal Regulations parts 105 and 106, which implement MTSA of 2002, require regulated facilities to maintain an approved FSP. Existing regulations require owners and operators of MTSA-regulated facilities to analyze vulnerabilities associated with radio and telecommunication equipment, including computer systems and networks, otherwise known as cybersecurity. When cybersecurity vulnerabilities are identified, an owner or operator demonstrates compliance by providing its cybersecurity mitigation procedures in the FSP. When a MTSA-regulated facility is found to not be following the measures or procedures noted in their FSP, or are otherwise not in compliance with the relevant regulations, the Captain of the Port may place operational controls on the facility and/or seek enforcement actions (Letter of Warning, Notice of Violation, Civil Penalty) on the owner/operator of the MTSA-regulated facility.

b. Many stakeholders mention that they are more robust in developing cybersecurity measures and have been for decades. So, what are ways to hold bad actors accountable without installing mandates that may limit the private sector's own work in this space?

ANSWER. Although the MTSA regulations in 33 CFR parts 105 and 106 are mandatory, it is up to each facility to determine how to identify, assess, and address the vulnerabilities of their computer systems and networks. While there is a baseline of what is required, this does not limit individual facilities from implementing additional protective measures. For example, each individual facility should determine the organizational structure; number of employees; the employee roles, responsibilities, and access permissions; and, the employee training needed so that its security personnel can address the facility's cyber security risks. Each facility should also determine how, and where, its data is stored and, if it is stored offsite, whether the data has a critical link to the safety and/or security functions of the facility. If such a critical link exists, the facility should address any vulnerabilities. Other motivating efforts include engaging stakeholders through multi-agency, multi-stakeholder initiatives such as Area Maritime Security Committees, Harbor Safety Committees, and others that encourage mutual efforts to bolster cyber risk management throughout the MTS.

Question 10. Each state has a designated CISA "Protective Security Advisor" that coordinates with members of the critical infrastructure community and works to help them prepare/defend against cyber-attacks. Can you tell me about the interface your agencies have with these Advisors and what role they play in your industries?

ANSWER. The Coast Guard interfaces with CISA Protective Security Advisors (PSA), Cybersecurity Advisors (CSA), and other CISA regional personnel through the Area Maritime Security Committees (AMSCs) as well as other Coast Guard points of contact. AMSCs are required by federal regulations and serve an essential coordinating function during normal operations and emergency response. They are comprised of government agency and maritime industry leaders, and serve as the primary local means to jointly evaluate cyber risks, share threat information, and participate in cyber preparedness exercises. Coast Guard field personnel work collaboratively with PSAs, CSAs, and other regional personnel as needed, the AMSC, during Regional Resiliency Assessment Programs, interagency/stakeholder meetings, local exercises, training offerings, incidents, and special events. As there is a cyber-physical security convergence with many threats we face as a country, the PSAs and CSAs work together to bring that combined expertise, as well as tools and resources, to our maritime partners.

Question 11. Many industry stakeholders utilize early notification networks. However, the public sector lacks a robust system to alert private carriers or shippers of an attack across the system. To critical infrastructure, the ability to limit damage seems crucial. Can you expand on how early notification networks are used by the private sector and why coordination with a federal government system is so important?

ANSWER. The evolving nature of cyber threats and vulnerabilities includes the fact that incidents affecting one component of the MTS, or other critical infrastructure sectors, could quickly and easily affect other components. Early and detailed notifications enable responding agencies and stakeholders to quickly assess, respond to, and recover from a cybersecurity incident while allowing others to take appropriate steps to prepare for and mitigate such incidents. Multiple government agencies respond to cybersecurity incidents, which necessitates timely reporting and shared information to facilitate a coordinated response.

Early notifications enable Coast Guard COTP to evaluate risks associated with a cybersecurity incident and deploy resources or impose appropriate operational controls when necessary (i.e. halt transfer operations, require tug boats to assist a ship, etc.). Early notifications also allow the Coast Guard's Cyber Command to support the impacted company remotely or deploy a specialized Cyber Protection Team to help them with the technical aspects of their assessment and response.

Notification networks include the Coast Guard's National Response Center, where MTSA-regulated facilities are required to report Transportation Security Incidents, Breaches of Security, and Suspicious Activity, to include cybersecurity events. Additionally, CISA receives and shares reports of cybersecurity incidents. In addition to agency messaging, the MTS–ISAC assists in the dissemination of key information to stakeholders.

QUESTIONS FROM HON. FREDERICA S. WILSON TO KEVIN DORSEY, ASSISTANT INSPECTOR GENERAL FOR INFORMATION TECHNOLOGY AUDITS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF TRANSPORTATION

Question 1. Mr. Dorsey, in your testimony, you highlighted that DOT's weaknesses can be attributed to its lack of progress in addressing previous audit recommendations. Between 2017 and 2020, the number of weaknesses more than doubled to over 10,000 under the previous administration. How will the $2 billion that was provided under the Infrastructure and Investment Jobs Act help the Biden administration address this problem and how can DOT prevent such a sharp increase in the future?

ANSWER. While the Act provides $2 billion for funding cybersecurity improvements and other critical infrastructure needs, we do not have any ongoing work that would allow us to assess how this funding may help address the weaknesses identified in my testimony. As my testimony stated, we made an overarching recommendation to DOT to require the Office of the Chief Information Officer to develop a multiyear strategy and approach—complete with objective milestones and resource commitments—to implement the necessary corrective actions to address these weaknesses and ensure an effective information security program. Implementing this recommendation will allow the Department to prioritize these weaknesses and calculate the resources necessary for resolving recurring cybersecurity issues while also addressing new concerns as they arise. An effective information security program will help DOT mitigate risks of cyberattacks and prevent such a sharp increase of recurring cybersecurity issues in the future.

QUESTION FROM HON. GARRET GRAVES TO KEVIN DORSEY, ASSISTANT INSPECTOR GENERAL FOR INFORMATION TECHNOLOGY AUDITS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF TRANSPORTATION

Question 2. I've read reports that there are some 500,000 vacancies for cybersecurity professionals in the U.S. workforce, making it nearly impossible for us to get a handle on the next generation of threats. Additionally, we've heard from industry that they feel that talent is relegated to SCIFs in the federal government, fusion centers, and big technology companies—preventing talent from being available to critical infrastructure at the local level. What can we be doing to rethink the workforce model for cybersecurity-specific professionals?

ANSWER. While DOT OIG does not have any ongoing work regarding the workforce model for cybersecurity-specific professionals, this challenge is not unique to DOT. GAO has recognized cybersecurity among the mission-critical skills gaps that contribute to the placement of Strategic Human Capital Management on its annual High Risk List report. Moreover, as illustrated by the examples of cyberattacks on local government and private infrastructure noted in my testimony, there is an acute need for cybersecurity talent outside the Federal Government. As to the Federal workforce, the Department of Homeland Security (DHS) recently launched the Cybersecurity Talent Management System (CTMS) to help it recruit, develop, and retain top cybersecurity professionals. If proven successful, this could serve as a model to be adopted elsewhere.

QUESTIONS FROM HON. MICHAEL GUEST TO KEVIN DORSEY, ASSISTANT INSPECTOR GENERAL FOR INFORMATION TECHNOLOGY AUDITS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF TRANSPORTATION

Question 3. Each state has a designated CISA "Protective Security Advisor" that coordinates with members of the critical infrastructure community and works to help them prepare/defend against cyber-attacks. Can you tell me about the interface your agencies have with these Advisors and what role they play in your industries?

ANSWER. The CISA Protective Security Advisor meets with Department staff. Given the Office of Inspector General's independent role, we do not interface with the advisor. This question would be best answered by someone at the Department level.

Question 4. Many industry stakeholders utilize early notification networks. However, the public sector lacks a robust system to alert private carriers or shippers of an attack across the system. To critical infrastructure, the ability to limit damage seems crucial. Can you expand on how early notification networks are used by the private sector and why coordination with a federal government system is so important?

ANSWER. While our office does not have any ongoing work specifically related to early notification networks used by the private sector, the importance of DOT's coordination with the private sector to enhance cybersecurity is clear. As I stated in my testimony, DOT is a lead agency, along with DHS, in protecting the critical infrastructure of the Nation's transportation sector. As such, DOT must partner effectively with other Federal agencies and the private sector to mitigate vulnerabilities and ensure a robust cybersecurity posture. For example, the FAA Extension, Safety, and Security Act of 2016 directs FAA to develop a comprehensive, strategic framework to reduce cybersecurity risks to civil aviation. FAA's efforts to implement this framework involve coordinating and collaborating on aviation cybersecurity with DHS and the Department of Defense through the Aviation Cyber Initiative. Protecting flight-critical systems—and the safety of the flying public—from rapidly evolving cyber-based threats also requires the cooperation of aviation stakeholders from industry, airlines, airports, and manufacturers. This is a good start, but it is only one step in what will be necessary for the development of a robust coordination effort between the private sector and the Federal Government to protect the transportation sector's critical infrastructure.

QUESTIONS FROM HON. STEVE COHEN TO NICK MARINOS, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Question 1. In July, GAO highlighted pipeline-related weaknesses that stemmed from TSA's own internal policies, which included conducting risk assessments with incomplete information and using protocols for responding to pipeline incidents that had not been revised since 2010. Is there anything you would like to add regarding GAO's review of these issues?

ANSWER. In July 2021, we testified that the Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), had not fully addressed pipeline cybersecurity-related weaknesses that GAO had previously identified, such as incomplete information for pipeline risk assessments and aged protocols for responding to pipeline security incidents.[1] Fully addressing our recommendations will better ensure that TSA's actions are well-coordinated with other federal agencies in response to a pipeline-related physical or cyber incident, and that pipeline stakeholders understand federal agencies' roles and responsibilities in helping pipeline owner/operators to restore service after a pipeline-related physical or cyber incident.

Specifically, GAO reports in 2018 and 2019 identified weaknesses in TSA's oversight and guidance, and made 13 recommendations to address those weaknesses.[2] TSA concurred with GAO's recommendations. As of November 2021, TSA had implemented 10 of the 13 recommendations but had not implemented the following:

1. In 2018, we recommended that TSA should identify or develop other data sources relevant to threat, vulnerability, and consequence consistent with DHS's critical infrastructure risk mitigation priorities and incorporate that data into the Pipeline Relative Risk Ranking Tool to assess relative risk of critical pipeline systems. As of July 2021, TSA officials reported meeting with representatives from DHS and the Federal Emergency Management Agency (FEMA) to obtain their input on the identification of sources relevant to threat, vulnerability and consequence consistent with DHS's priorities. According to TSA officials, further action on this recommendation had been limited due to the agency's work on the pandemic response and the lack of funding for contractor support.
2. In 2018, we also recommended that TSA should take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool. As of July 2021, DHS officials stated that TSA intends to take steps to coordinate an independent, external peer review of its Pipeline Relative Risk Ranking Tool after the agency has addressed the above-mentioned open recommendation.
3. In 2019, we recommended that TSA periodically review, and as appropriate, update the 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure the plan reflects relevant changes in pipeline security threats (including those related to cybersecurity), technology, federal law and policy, and any other factors relevant to the security of the nation's pipeline systems. According to TSA officials, as of August 2021, the agency had completed a review of the 2010 Pipeline Security and Incident Recovery Protocol Plan and determined that updates were needed.

We will continue to monitor TSA's efforts to implement our recommendations.

Question 2. We have heard numerous reports of local governments being targeted by ransomware and other cybersecurity threats. Local agencies may be especially under-prepared to respond to the increasing level of risk. As you know, the bipartisan infrastructure bill we passed into law allocates $1 billion to improve state and local government cybersecurity through a new Department of Homeland Security grant program. Can you discuss how this funding may impact local transportation agencies and if you have any recommendations for how the federal government can better assist or coordinate with state and local governments' cybersecurity efforts?

ANSWER. Increased funding may help to improve cybersecurity and critical infrastructure for transportation agencies through grants to states, local, tribal, and territorial governments from the State and Local Cybersecurity Grant Program estab-

[1] GAO, *Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses*, GAO–21–105263 (Washington, D.C.: July 27, 2021).

[2] GAO, *Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment*, GAO–19–426 (Washington, D.C.: June 5, 2019) and *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO–19–48 (Washington, D.C.: Dec. 18, 2018).

lished by the Infrastructure Investment and Jobs Act.[3] The act also calls for the establishment of the Safety Data Initiative to promote the use of data integration, data visualization, and advanced analytics for surface transportation safety through the development of innovative practices and products for use by federal, state, and local entities. This initiative is designed to encourage the sharing of data between and among federal, state, and local transportation agencies.

Additionally, the act also requires GAO to conduct a review of the State and Local Cybersecurity Grant Program including the grant selection process by DHS and a sample of grants awarded. In light of your interest in state and local governments' cybersecurity efforts, we will reach out to your office during our review of the program.

On the subject of federal assistance to state and local governments' cybersecurity efforts, DHS's Cybersecurity and Infrastructure Security Agency (CISA) created CISA Central to be a unified portal and point of contact for critical infrastructure partners and stakeholders to contact CISA and request assistance.[4] Furthermore, as the lead agency responsible for overseeing domestic critical infrastructure protection efforts, CISA's ability to effectively coordinate and consult with federal agencies; state, local, territorial, and tribal governments; and the private sector is critical. Consequently, in March 2021, we reported on CISA's organizational transformation initiative and its ability to coordinate effectively with stakeholders.[5] Among other things, we reported on a number of challenges that selected government and private-sector stakeholders had noted when coordinating with CISA, including the lack of stakeholder involvement in developing guidance.

To address these and other weaknesses, we made 11 recommendations to DHS. Of these, three recommendations directly related to challenges reported by stakeholders. The department concurred with our recommendations and, as of September 2021, reported that it intends to implement them by the end of calendar year 2022. As part of our ongoing work, we will continue to monitor CISA's efforts to carry out its mission to identify and respond to cyber and other risks to our nation's infrastructure.

Questions from Hon. Garret Graves to Nick Marinos, Director, Information Technology and Cybersecurity, U.S. Government Accountability Office

Question 3. I've read reports that there are some 500,000 vacancies for cybersecurity professionals in the U.S. workforce, making it nearly impossible for us to get a handle on the next generation of threats. Additionally, we've heard from industry that they feel that talent is relegated to SCIFs in the federal government, fusion centers, and big technology companies—preventing talent from being available to critical infrastructure at the local level. What can we be doing to rethink the workforce model for cybersecurity-specific professionals?

Answer. Prior GAO reports have pointed out that the federal government and private industry face a persistent shortage of cybersecurity-specific professionals to combat cyber threats.[6] In November 2021, we reported that a potential method for developing a talented and diverse cadre of digital-ready, tech-savvy federal employees is the creation of a digital service academy—similar to military academies—to train future civil servants in the digital skills needed to modernize government.[7] For example, staff with knowledge, skills, and abilities to secure digital services could help agencies more effectively manage risks associated with the cybersecurity of systems in a cloud environment.

The Cyberspace Solarium Commission has made recommendations related to cybersecurity workforce management challenges, including that the U.S. government should take a number of cyber-oriented actions, such as expanding federal cyber training programs.[8] Particularly, the Commission recommended that DHS, the National Science Foundation, and the Office of Personnel Management expand the

[3] Infrastructure Investment and Jobs Act, Pub. L. No 117–58, 135 Stat. 429, 1272, § 70612 (2021).

[4] https://www.cisa.gov/central.

[5] GAO, *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, GAO–21–236 (Washington, D.C.: Mar. 10, 2021).

[6] See, for example, GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO–21–288 (Washington, D.C.: Mar. 24, 2021).

[7] GAO, *Digital Services: Considerations for a Federal Academy to Develop a Pipeline of Digital Staff*, GAO–22–105388 (Washington, D.C.: Nov. 19, 2021).

[8] U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

CyberCorps: Scholarship for Service program, which agencies could use to increase the supply of cybersecurity talent. This program provides scholarships and stipends to undergraduate and graduate students who are pursuing information security-related degrees, in exchange for up to three years of federal service after graduation.[9] In particular, the program is designed to recruit and train the next generation of IT professionals to meet the needs of the cybersecurity mission for federal, state, local, and tribal governments.

Question 4. DOD has been implementing the Cybersecurity Maturity Model Certification (CMMC), requiring CMMC credentials to qualify a bidder for a federal contract and therefore providing additional security to our federal systems. However, a downside to the CMMC system is the financial burden of obtaining credentials, which hurts small businesses in their efforts to receive DOD Contracts. As credentialing spreads across other areas of the federal government, including to DOT, do you have any suggestions for how other agencies can learn from the DOD CMMC process to ensure a high degree of cyber security for our contractors, while ensuring that small businesses have an opportunity to participate in federal contracting?

ANSWER. In December 2021, we reported that the Department of Defense's (DOD) Cybersecurity Maturity Model Certification (CMMC) process is ongoing due, in part, to delays in certifying assessors as well as concerns from small businesses.[10] The scope of the work we have conducted so far has not directly related to how other federal agencies can learn from the DOD CMMC process and ensure small businesses have opportunities to participate in federal contracting.

Nevertheless, during the course of our review of DOD's implementation of CMMC, government and industry representatives raised a number of issues that are important to the future course of CMMC. They include CMMC adoption by other federal agencies. In particular, monitoring efforts other federal agencies are considering or taking to adopt CMMC or similar requirements for their supply chains. In addition, industry—especially, small businesses—expressed a range of concerns about CMMC implementation, such as costs and assessment consistency. For example, during our discussion group with small defense contractors, a participant told us that small businesses may consider the added cost and competitive uncertainty as incentives to exit the government contracts marketplace. While DOD engaged with industry in refining early versions of CMMC, it had not provided sufficient details and timely communication on implementation. Until DOD improves this communication, industry will be challenged to implement protections for DOD's sensitive data.

QUESTIONS FROM HON. MICHAEL GUEST TO NICK MARINOS, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Question 5. Each state has a designated CISA "Protective Security Advisor" that coordinates with members of the critical infrastructure community and works to help them prepare/defend against cyber-attacks. Can you tell me about the interface your agencies have with these Advisors and what role they play in your industries?

ANSWER. As a legislative branch agency, GAO does not interface with CISA's Protective Security Advisor (PSA) program unless there is a request by congressional committees or subcommittees, or is statutorily required by public laws or committee reports.

For fiscal year 2020, CISA's PSA program expended approximately $38.5 million and had 127 staff. Specifically, CISA is increasing its presence in the form of staff who work directly with critical infrastructure partners and communities at the regional, state, tribal, and local level. These staff include local and regional Protective Security Advisors and Cybersecurity Advisors, among other personnel, based in 10 regional offices.[11] These advisors support critical infrastructure owners and operators by providing products and services, such as assessments, training, exercises, and workshops. For example, Cybersecurity Advisors provide briefings and assessments of cybersecurity and resilience for owners and operators.[12] In addition, Pro-

[9] https://www.sfs.opm.gov.

[10] GAO, *Defense Contractor Cybersecurity: Stakeholder Communication and Performance Goals Could Improve Certification Framework*, GAO–22–104679 (Washington, D.C.: Dec. 8, 2021).

[11] CISA's regional offices also include Emergency Communications Coordinators who support federal, state, local, tribal, and territorial government public safety communications mission partners.

[12] A cyber resilience review assessment is a nontechnical assessment to evaluate an organization's operational resilience and cybersecurity practices.

tective Security Advisors, complete surveys and assessments that help identify the security and resilience of individual owners' and operators' facilities.

Question 6. Many industry stakeholders utilize early notification networks. However, the public sector lacks a robust system to alert private carriers or shippers of an attack across the system. To critical infrastructure, the ability to limit damage seems crucial. Can you expand on how early notification networks are used by the private sector and why coordination with a federal government system is so important?

ANSWER. The importance of having early notification that a cybersecurity incident is occurring on a network is highlighted in the May 2021 Executive Order 14028, *Improving the Nation's Cybersecurity*, issued by the White House.[13] The executive order requires the federal government to employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. While this topic of how early notification networks are being used by the private sector is outside the scope of the work we have conducted so far, we will be glad to discuss a potential request for future work on this topic with your staff.

On the subject of federal coordination with the private sector, in November 2021, we reported that CISA has a leadership role in coordinating federal efforts intended to aid in the resilience of the Communications Sector, an integral component of the U.S. economy, which faces serious cyber-related threats that could affect the operations of local, regional, and national level networks.[14] The agency fulfills its responsibilities to private sector owners and operators through a variety of programs and services, including incident management and information sharing. With respect to incident management, CISA is responsible for coordinating federal activities to support Communications Sector infrastructure owners and operators during incidents, such as outages caused by severe weather. With respect to information sharing, in addition to managing federal coordination during incidents impacting the Communications Sector, CISA shares information with sector stakeholders to enhance their cybersecurity and improve interoperability, situational awareness, and preparedness for responding to and managing incidents.

We found that CISA had not assessed the effectiveness of such activities, despite DHS recommending that they to do so every four years. As such, we made three recommendations to CISA, including that the agency assess the effectiveness of support provided to the sector, and revise the sector plan to include new and emerging threats and risks, among other things. DHS concurred with the recommendations and described initial actions under way and plans to address them in response to our report.

○

[13] The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[14] GAO, *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector*, GAO–22–104462 (Washington, D.C.: Nov. 23, 2021).