SOLARWINDS AND BEYOND: IMPROVING THE CYBERSECURITY OF SOFTWARE SUPPLY CHAINS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MAY 25, 2021

Serial No. 117–17

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
44–636PDF WASHINGTON : 2021

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. EDDIE BERNICE JOHNSON, Texas, *Chairwoman*

ZOE LOFGREN, California
SUZANNE BONAMICI, Oregon
AMI BERA, California
HALEY STEVENS, Michigan, *Vice Chair*
MIKIE SHERRILL, New Jersey
JAMAAL BOWMAN, New York
BRAD SHERMAN, California
ED PERLMUTTER, Colorado
JERRY MCNERNEY, California
PAUL TONKO, New York
BILL FOSTER, Illinois
DONALD NORCROSS, New Jersey
DON BEYER, Virginia
CHARLIE CRIST, Florida
SEAN CASTEN, Illinois
CONOR LAMB, Pennsylvania
DEBORAH ROSS, North Carolina
GWEN MOORE, Wisconsin
DAN KILDEE, Michigan
SUSAN WILD, Pennsylvania
LIZZIE FLETCHER, Texas
VACANCY

FRANK LUCAS, Oklahoma, *Ranking Member*
MO BROOKS, Alabama
BILL POSEY, Florida
RANDY WEBER, Texas
BRIAN BABIN, Texas
ANTHONY GONZALEZ, Ohio
MICHAEL WALTZ, Florida
JAMES R. BAIRD, Indiana
PETE SESSIONS, Texas
DANIEL WEBSTER, Florida
MIKE GARCIA, California
STEPHANIE I. BICE, Oklahoma
YOUNG KIM, California
RANDY FEENSTRA, Iowa
JAKE LATURNER, Kansas
CARLOS A. GIMENEZ, Florida
JAY OBERNOLTE, California
PETER MEIJER, Michigan
VACANCY

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HON. BILL FOSTER, Illinois, *Chairman*

ED PERLMUTTER, Colorado
AMI BERA, California
GWEN MOORE, Wisconsin
SEAN CASTEN, Illinois

JAY OBERNOLTE, California, *Ranking Member*
PETE SESSIONS, Texas
VACANCY

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. HALEY STEVENS, Michigan, *Chairwoman*

PAUL TONKO, New York
GWEN MOORE, Wisconsin
SUSAN WILD, Pennsylvania
BILL FOSTER, Illinois
DON BEYER, Virginia
CONOR LAMB, Pennsylvania
DEBORAH ROSS, North Carolina

MICHAEL WALTZ, Florida, *Ranking Member*
ANTHONY GONZALEZ, Ohio
JAMES R. BAIRD, Indiana
PETE SESSIONS, Texas
JAKE LATURNER, Kansas
PETER MEIJER, Michigan

C O N T E N T S

May 25, 2021

SOLARWINDS AND BEYOND: IMPROVING THE CYBERSECURITY OF SOFTWARE SUPPLY CHAINS

TUESDAY, MAY 25, 2021

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT,
JOINT WITH THE SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to notice, at 2:03 p.m., via Zoom, Hon. Bill Foster [Chairman of the Subcommittee on Investigations and Oversight] presiding.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY JOINT HEARING

HEARING CHARTER

SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains

Tuesday, May 25, 2021
2:00 p.m. EDT – 4:00 p.m. EDT
Zoom

PURPOSE

The purpose of this hearing is to examine the causes and impacts of recent supply chain attacks on Federal agencies, explore how Federal agencies currently mitigate their software supply chain risks, and consider how best to improve software supply chain security. The Subcommittees will examine the challenges of Federal agency compliance with standards and best practices, and hear recommendations on next steps to secure the software supply chain for Federal agencies, especially through improvements to the efficacy of guidance provided by the National Institute of Standards and Technology (NIST). The Subcommittees will further explore how the Federal Government can help facilitate the adoption of supply chain standards and best practices within the private sector.

WITNESSES

- **Mr. Matthew Scholl,** Chief, Computer Security Division of the Information Technology Laboratory, National Institute of Standards and Technology (NIST)
- **Dr. Trey Herr**, Director, Cyber Statecraft Initiative, Atlantic Council
- **Ms. Katie Moussouris,** Founder and CEO, Luta Security
- **Mr. Vijay D'Souza,** Director, Information Technology and Cybersecurity, Government Accountability Office (GAO)

OVERARCHING QUESTIONS

- Including SolarWinds, what are the recent trends regarding supply chain attacks on Federal Government systems or industry networks?
- What challenges limit the capacity of both the private and public sector to respond to these attacks and remediate their vulnerabilities?
- How are Federal agencies meeting existing software supply chain risk management standards and best practices?
- What guidance, tools, and technical assistance does NIST offer public and private sector entities to improve their software supply chain risk management?
- What policy changes can improve the adoption and efficacy of NIST standards and guidance by Federal agencies?

What is a Supply Chain Attack?

Modern computer networks are comprised of hundreds or thousands of pieces of hardware and software from different sources with different levels of access, update timelines, and functions. A cyber supply chain attack occurs when a bad actor infiltrates a network through hardware or software component that has been granted access or incorporated into that network. Similar to other forms of malware, this can result in stolen data or damage to systems. What sets supply chain attacks apart is that the vulnerability enters the network through a trusted source, such as a third-party provider or contractor—no clicking on a bad link or downloading an infected file is required. Supply chain attacks are often harder to detect, prevent, and remediate than traditional malware. System owners and operators may depend on the detection and response capabilities of the third-party source of the infected component. Since it is not feasible for organizations to avoid third-party software entirely, users must have supply chain risk management best practices in place to mitigate the damage supply chain attacks can cause.

SolarWinds

SolarWinds is a software company that gained notoriety when its Orion platform was used in a massive supply chain attack which garnered nationwide press. The SolarWinds attack – also referred to as *Solorigate*, *Sunburst*, and *SolarStorm* – was committed by the Russian intelligence service and occurred in several stages. The attackers initiated reconnaissance on SolarWinds as early as January 2019[1]. By the fall of 2019, they had compromised the SolarWinds network to access the company process for updating their software, inserting a backdoor to allow later access. The attacker then hid its presence and remained dormant while the company spread an infected software update to its customers. The update was distributed to customers in spring of 2020, several months after the initial infection.

The infected Orion software update was downloaded by an estimated 18,000 organizations. However, 18,000 organizations did not suffer impacts. Not all of them installed the update, and of those that did, not all were chosen for further compromise by the attacker. The Orion compromise sent information on the host network back to a server owned by the attacker, allowing them to pick and choose among targets for introducing additional malware. In a sense, the Orion compromise let the hacker make tiny cracks in the walls of houses to peek through and select the ones they wanted to come back and burgle. Of the additional pieces of malware, *Teardrop* served as a second backdoor to help hide how the attacker got into the software, and *Cobalt Strike* allowed the attackers to steal data. The attacker also exploited other vulnerabilities, including those within Microsoft Office 365 and Microsoft Azure, to steal data from many of these systems.

The length of the intrusion varied by victim, but in some cases lasted for months. The supply chain attack was finally detected in December of 2020 by the cybersecurity company FireEye and quickly attributed to Russia, though public confirmation from the White House confirmation took months.[2][3] FireEye realized

[1] https://www.rsaconference.com/Library/presentation/USA/2021/solarwinds-what-really-happened
[2] https://www.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia/index.html
[3] https://www.reuters.com/business/white-house-blames-russian-spy-agency-svr-solarwinds-hack-statement-2021-04-15/

their own network had been accessed and later tracked the original intrusion back to the infected Orion update.

Information on the reach of this attack has been slow to emerge. Of the 100 companies impacted relatively few were publicly identified. In May of 2021 was it revealed that 37 of the companies were part of the defense industrial base[4]. Nine Federal agencies had data stolen from their systems, and several more were vulnerable but not targeted with secondary malware by the attacker. Per the latest briefings received by the Science Committee, Federal agencies have completed immediate remediation, but a full analysis of the attack is still ongoing.

Recent Trends in Supply Chain Attacks

The SolarWinds attack is uncommon in scope, but the avenue of attack is not rare. The Atlantic Council's *Breaking Trust* project grappled with the landscape of software supply chain intrusions and assembled a dataset of supply chain attacks stretching back to 2010.[5] This dataset is not comprehensive, as it relies on public disclosure of the supply chain attack in English language news sources, but it does illustrate the growing frequency of supply chain attacks.

Over eight months in 2019-2020, 23 supply chain attacks were added to the *Breaking Trust* dataset, increasing the total count from 115 to 138. In addition, most of the attacks occurred in the latter half of the decade. The report suggests that the quantity of supply chain attacks is likely increasing.

The damage caused by supply chain attacks can also be extensive. The 2017 *NotPetya* malware that shut down computers across the world and caused billions in damage was spread through a supply chain attack on a Ukrainian tax accounting application.[6] Other attacks, such as the 2017 compromise of CCleaner or the 2016 *Kingslayer* attack on a Windows IT admin application, had millions of victims, including networks at high value targets such as Federal agencies, banks, and telecoms[7]. Both *NotPetya* and *Kingslayer* were attributed to nation-state actors, Russia and China respectively. In fact, 30 of the attacks in the Atlantic Council dataset were linked to nation-state actors. This is likely because supply chain attacks are highly effective as espionage tools or for the theft of high-value data. They are also relatively cheap on the scale of nations. The President of Microsoft, Brad Smith, estimated that the SolarWinds attack required on the order of 1000 engineers to carry out, a quantity easily within the reach of Russia or China[8].

Federal Information Security Management Act (FISMA)

The *Federal Information Security Management Act of 2002 (FISMA)* established a framework for protecting federal information systems. FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program for information security systems supported or

[4] https://www.fedscoop.com/solarwinds-defense-industrial-base-hack-dod/
[5] https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/
[6] https://www.wired.com/story/white-house-russia-notpetya-attribution/
[7] https://www.dni.gov/files/NCSC/documents/supplychain/20190327-Software-Supply-Chain-Attacks02.pdf
[8] https://www.csis.org/events/lessons-learned-cyberattack-conversation-solarwinds-part-1-2

managed by the agency. Under FISMA, there is no centralized enforcement authority. Rather, each agency is responsible for its own FISMA compliance. The *Federal Information Security Modernization Act of 2014* updated FISMA to streamline reporting, update breach notification policies, and clarify the roles of different agencies. However, the appropriate roles of different agencies in responding to cyber-attacks remain on ongoing topic of debate.

The House Committee on Science, Space, and Technology is one of three House committees that agencies, under *FISMA,* are required to notify within seven days of a major cyber incident. Agency compliance with *FISMA* in the case of SolarWinds was mixed. Most agencies offered briefings and followed through on information sharing as the investigation proceeded. However, relatively few provided official *FISMA* notification at any point in the process. When pressed, agencies – including some that had data stolen – claimed that because there was no demonstrable harm the breach did not qualify as a major incident and notification was not required. In some cases, this decision may have been correct. Even with significant levels of access the attacker was not always successful in stealing data, and where they were it was not always sensitive data. However, agencies often underestimate future harms that may result from data stolen during the breach when considering whether to label it a "major incident" and thus properly report it to the committees of jurisdiction. Ambiguity in the definition of "major incident" may have resulted in an uneven agency response to Congressional overseers.

Assessing Federal Agency Supply Chain Cybersecurity

The relative prevalence of supply chain attacks, both in general and as a tool of nation-state actors, highlights the importance of securing Federal Agency systems against this threat where possible, including by employing risk management best practices. To that end, in December 2020 the GAO published a report with the alarming title: *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks.*[9] The report identified several foundational practices for Information Communications Technology (ICT) Supply Chain Risk Management (SCRM) that Federal agencies needed to implement. Of the 23 agencies surveyed, none had yet implemented all foundational practices, none had implemented a process to conduct agency-wide assessments of their supply chains, and 14 of the agencies had implemented none of the practices. To their credit, a large majority of agencies concurred with GAO's recommendations, and expressed their intent to implement the foundational practices. Almost half of the agencies reported they were waiting for additional Federal guidance before enacting some or all of the foundational practices.[10] However, agencies have been required by the Office of Management and Budget (OMB) since 2016 to adopt NIST guidance to mitigate supply chain risks (discussed in detail below).[11] The gap between recommendation and implementation was large, and in some cases the agency timeline for completing the recommendations stretched to 2024.

Federal Activities for Software Supply Chain Risk Management

There are several agencies in charge of producing guidance to prevent and respond to software supply chain vulnerabilities and attacks:

[9] https://www.gao.gov/assets/gao-21-171.pdf
[10] This anticipated guidance is from the Federal Acquisition Security Council (FASC), which will recommend NIST standards.
[11] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

The Cybersecurity and Infrastructure Security Agency

The Department of Homeland Security's CISA helps Federal civilian agencies, critical infrastructure entities, and the private sector share cybersecurity information and respond to emerging incidents. CISA, the Federal Bureau of Investigation and the Office of the Director of National Intelligence led the Federal response to SolarWinds.[12] Throughout the response, CISA remained in regular contact with affected public and private sector entities, publishing guidance and forensics capabilities to help network defenders identity and mitigate the threat.[13] In briefings with Committee staff, all affected agencies spoke highly of the support they received from CISA.

The agency has also conducted several activities to improve the Nation's supply chain security risk management. Launched in 2019, CISA's Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force is a public-private partnership created to improve the Nation's collective ability to assess and mitigate threats to the ICT supply chain and improve the security and resilience of those supply chain elements and systems.[14] The task force is made up of industry representatives from the information technology and communications sectors as well as Federal partners like NIST. The task force has released several reports regarding both software and communications technology risk management.[15]

National Institute of Standards and Technology

NIST is the agency primarily in charge of the nation's cybersecurity standards and best practices. In February 2013, President Obama signed an Executive Order on critical infrastructure cybersecurity. In 2014, after convening public and private sector stakeholders, NIST published a voluntary framework for reducing cybersecurity risks to critical infrastructure. NIST has since updated and expanded its guidance to apply to new scenarios, such as supply chain risk management. For example, NIST published SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,*[16] which offers guidance for organizations to manage the increasing risk of cyber supply chain compromise, whether intentional or unintentional. NIST is currently working to revise this publication. By statute, Federal agencies must use NIST's cybersecurity standards and guidelines to protect non-national security Federal information and communications infrastructure. After the development of a standard or framework, NIST works with OMB to publish a final rule, requiring agencies to adopt the standard.

In addition to supply chain risk management, NIST has also worked with stakeholders to develop other critical frameworks and guidance for securing software. For example, NIST has produced guidance for vulnerability remediation.[17] The agency has also developed *The Secure Software Development Framework* to help software developers reduce the number of vulnerabilities released in software.[18]

---

[12] https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
[13] https://www.cisa.gov/supply-chain-compromise
[14] https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf
[15] https://www.cisa.gov/ict-supply-chain-toolkit
[16] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
[17] https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final
[18] https://csrc.nist.gov/Projects/ssdf

However, to date relatively little attention has been paid to the lifecycle of software after it has been deployed. As the SolarWinds incident shows, risks remain throughout a piece of software's lifecycle.

National Telecommunications and Information Administration

Modern software products are often an aggregation of multiple software components from different developers, code repositories, and other sources. Suppliers of software components also use different naming schemes for the same software components. As a result, identifying which vulnerabilities compromise which products can be a challenging technical feat. To address this challenge and promote transparency in software supply chains, the NTIA at the Department of Commerce is leading a multi-stakeholder initiative called the Software Bill of Materials (SBOM).[19] The goal of this effort is to create a machine readable inventory that will enable software developers and users to track software components and dependencies and make responding to vulnerabilities in the event of an incident more straightforward.

Federal Acquisition Security Council

In 2017, DHS concluded that software products from the Russian cybersecurity firm, Kaspersky Laboratories, were a security threat to government networks. However, because no government agency had the clear jurisdiction to immediately address this concern, DHS was forced to issue a binding directive to require agencies to remove the software.[20] This authority, granted under FISMA 2014, was not designed to address individual software or companies.

To address this issue, Congress passed the *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act* in 2018.[21] This act created the Federal Acquisition Security Council (FASC), to provide a process by which the Federal government could address threats posed by specific products. The FASC is made up of seven executive branch agencies, including NIST. It is charged with recommending supply-chain risk management standards, developed by NIST, and establishing criteria for sharing information on supply-chain risks between Federal agencies and other entities. In addition, if the FASC believes that a certain product in Federal supply chains is a threat to Federal systems, it can recommend Federal agencies exclude that product from agency procurement or remove it from agency networks. As of May 2021, the FASC is still working to initiate its strategy and processes, and it was not fully operational during the SolarWinds response.

Executive Order 14028: Improving the Nation's Cybersecurity

On May 12, the Biden Administration released an Executive Order, "Improving the Nation's Cybersecurity."[22] The goal of this Executive Order is to address government supply chain security deficiencies in the wake of SolarWinds. The most relevant for this hearing is Section 4, which primarily tasks NIST to work with public and private sector entities to conduct several activities to improve Federal guidance for software supply chain security.[23] Each of these activities has an aggressive timeline.

---

[19] https://www.ntia.gov/SBOM
[20] https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01
[21] https://www.congress.gov/bill/115th-congress/house-bill/7327/text
[22] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[23] Ibid.

- Within 90 days, NIST must identify or develop standards, procedures, or criteria that enhance the security of the software supply chain, including criteria that can be used to evaluate software security and provide SBOMs to all software purchasers.
- Within 45 days, NIST must publish a definition of the term "critical software," which the Executive Order nominally defines as "software that performs functions critical to trust."
- Within 60 days, NIST must publish guidance for critical software security measures.
- Within 60 days, NIST must recommend minimum standards for vendors' testing of their software source code.
- NIST is also tasked with identifying criteria and initiating pilot programs for labeling to promote transparency in the security of consumer products, such as Internet of Things devices and software development.

Notably, the Executive Order also calls for all executive agencies to develop plans to implement Zero Trust Architecture, systems that treat all users as potential threats and prevent access until the users can be properly authenticated and their access authorized. Agencies are required to adopt NIST standards and guidance to accomplish this task. Implementing zero trust architectures is expensive and time consuming, and agencies may not comply without sufficient appropriations or technical assistance from NIST and DHS.

Chairman FOSTER. All right, this hearing will now come to order. And, without objection, the Chair is authorized to declare recess at any time. But before I deliver my opening remarks, I wanted to note the circumstances under which we're meeting today. Pursuant to *House Resolution 8*, the Subcommittee is meeting virtually. I have a couple of reminders for Members about the conduct of this remote hearing. First, Members should keep their video feed on as long as they are present at the hearing. Members are responsible for their own microphones. And please also keep your microphones muted unless you are speaking. And finally, if Members have documents that they wish to submit for the record, please e-mail them to the Committee Clerk, whose e-mail addresses was circulated prior to the hearing.

Well, good afternoon, and welcome to our Members and panelists. Thank you for joining us for this important hearing on supply chain cybersecurity. We're focusing on the software supply chain today, and cybersecurity attacks throughout the software supply chain are especially insidious. A company can deploy a digitally signed software update from a trusted partner, but unless they are willing to do a complete cybersecurity analysis of that update, they are wide open to any significant breach of cyber hygiene in their trusted provider. So supply chain attacks are harder to detect, to prevent, and to remediate than traditional malware. And, once an adversary is in the system, they can deploy multiple types of attacks to maintain access and steal data. They run—might run amok on your system for a long time once they're in because the access came through a trusted partner, and can be reinstalled.

In the case of SolarWinds, the Russian intelligence service embedded a back door in the company's Orion software in the fall of 2019, and customers were downloading that infected software by the spring. 18,000 organizations did this over the course of 2020, and not one of them realized that they had a company on their network—had company on their networks until FireEye detected the breach of their own systems and sounded the alarm in December. I want to thank FireEye for moving quickly to alert public officials to what it had discovered. This is a well-regarded cybersecurity company that was itself breached by a malicious actor. They might have worried about how news of the hack could affect the company's reputation, but they did the right thing anyway. And we are all aware of the fact that FireEye could have just as easily kept quiet to protect their reputation, because there is no requirement for private companies to disclose a cybersecurity breach to the Federal Government. If a reputable company—cybersecurity company like FiberEye—FireEye can be breached by an attack like this, any organization can. As we will hear from our Atlantic Council witness, Dr. Herr, the supply chain cyberattacks are ticking up. In fact, we've seen several alarming incidents reported even since the SolarWinds breach was disclosed in December.

As a semi-separate item I have concerns about whether the Federal agencies are doing enough to enforce best practices to reduce their exposure to cyber risks, and whether they have systems in place to respond quickly enough to a significant breach. Last summer Microsoft discovered a serious vulnerability called Zerologon that made it possible for the hackers to impersonate any computer

on the network, including the system designed to identify and authenticate trusted people on the network. And I have to say that when I read the technical description of that flaw, I found that its existence in such a crucial piece of software, and the simplicity of the attack, sort of breathtaking. This was very different than, say, the technical details of the Meltdown and Spectre flaws of a couple of years back, when I was, frankly, blown away by their sophistication and complexity. It's clear to me that we need some mechanism to put more eyes on such commonly used and critical software. But the Federal issue here is that Microsoft issued the first of two patches on August 11 of last year, and by late September some Federal agencies still had failed to update their systems. The DHS (Department of Homeland Security) Cybersecurity Office, CISA (Cybersecurity and Infrastructure Security Agency), had to issue an emergency order to force agencies to patch or disable affected Windows servers. Meanwhile, it was discovered that the breach was already being exploited in the wild by at least Iranian and Russian hackers.

Malicious actors with a creative flair for exploiting technology are working every day to put Americans at risk, but engineers at NIST (National Institute of Standards and Technology) and other Federal agencies are innovating too. President Biden has recently released an Executive order (EO) on improving Federal cybersecurity that calls on agencies to take bold actions to address the challenge of software supply chain security and other items. I look forward to hearing today about the likely effectiveness of this Executive order, and how Federal science—the Federal science apparatus can do more to help understand the threat, and help private and public sectors mitigate that risk.

And, finally, as the only Ph.D. physicist, though not the only Ph.D. scientist on this Committee and in Congress, and also an integrated circuit designer, I have to say how glad I am to be able to partner with Ranking Member Obernolte on this important matter. I believe he's the first and only Member of Congress with an advanced degree in artificial intelligence, and I'll ask him to put his Caltech electrical engineering and information technology executive pants back on today to help us get near the heart of this matter. I thank him and his staff for their partnership, and I yield to him for an opening statement.

[The prepared statement of Chairman Foster follows:]

Good morning, and welcome to our members and panelists. Thank you for joining us for this important hearing on supply chain cybersecurity. We're focusing on the software supply chain today. And cybersecurity attacks through the software supply chain are a special kind of insidious. Supply chain attacks are harder to detect, to prevent, and to remediate than traditional malware.

And once an adversary is in the system, they can deploy multiple types of attacks to maintain access and steal data. They might run amok on your system for a long time once they're in, because their access came through a trusted partner. In the case of SolarWinds, the Russian intelligence service embedded a backdoor in the company's Orion software in the fall of 2019. Customers were downloading the infected software by the spring. 18,000 organizations did this over the course of 2020. And not one of them realized that they had company on their networks until FireEye detected the breach on their own systems and sounded the alarm in December.

I want to thank FireEye for moving quickly to alert public officials to what it had discovered. This is an esteemed cybersecurity company that was itself breached by a malicious actor. They might have worried about how news of the hack could affect

the company's reputation, but did the right thing anyway. And we have since woken up to the fact that FireEye could have just as easily kept quiet, because there is no requirement for private companies to disclose a cybersecurity breach to the Federal government.

If a reputable cybersecurity company like FireEye can be breached by an attack like this, any organization can. And as we will hear from our Atlantic Council witness, Dr. Herr, supply chain cyber attacks are ticking up. In fact, we've seen several alarming incidents reported even since the SolarWinds breach was discovered in December.

And I have concerns about whether Federal agencies are doing enough to reduce their exposure to cyber risks, and whether they have systems in place to respond quickly to a breach. Last summer, Microsoft discovered a serious vulnerability called Zerologon that made it possible for the hackers to impersonate any computer on a network, including the system designed to identify and authenticate trusted people on the network. Microsoft issued the first of two patches on August 11. But by late September, some Federal agencies had still failed to update their systems. The DHS Cybersecurity office, CISA, had to issue an emergency order to force agencies to patch or disable affected Windows servers. Meanwhile, it was discovered that the breach was already being exploited in the wild by Iranian and Russian hackers.

Malicious actors with a creative flair for exploiting technology are working every day to put Americans at risk. But the engineers at NIST and other Federal agencies are innovating, too. President Biden has released an Executive Order on improving Federal cybersecurity that calls on agencies to take bold actions to address the challenge of software supply chain security. I look forward to hearing today about how the Federal science apparatus can do more to understand the threat and help the private and public sectors mitigate their risk.

I'm also glad to partner with Ranking Member Obernolte on this important matter. I believe he is the first and only Member of Congress with an advanced degree in artificial intelligence. I'll ask him to put his technology executive hat back on today to help us get to the heart of the matter. I thank him and his staff for their partnership, and I yield for his opening statement.

Mr. OBERNOLTE. Well, thank you very much, Chairman Foster, and thank you for holding this hearing on an extremely important topic. I found the GAO (Government Accountability Office) report on supply chain risk management (SCRM) from December to be truly alarming. And the thing that stood out to me about that report was the finding that, of the organizations the GAO looked at, they identified core supply chain risk management best practices, and then went through 23 different agencies looking at how many of those best practices were being implemented, and this is what stood out to me. For over half of the organizations, none of the best practices were being implemented. So, to me, that points to a failure of governance, and I think that we are at an important position here, to build on the Executive order, and to call attention to this problem, and this hearing is a critical part of doing that. So, for myself, what I'm hoping to get out of this hearing is the answer to three different questions, one of which is why isn't the guidance being followed, the second of which is how can the guidance be easier to implement, and the third of which is how does the guidance need to change to meet these emerging threats? And I think recent events have shown just how vulnerable our supply chain can be.

I think as we conduct this hearing we're going to find that our organizations fall into three different categories. We have organizations that are Federal agencies, we have organizations that Federal agencies contract with, and then we have organizations that are private industry organizations, but still have a significant impact on our supply chain, and I think that those organizations also need to be included in this discussion. That Colonial Pipeline incident

over the last couple of weeks I think really graphically illustrates just how big those risks are.

And, in closing, I want to point out that if the outcome of this whole process is just another PDF or another spreadsheet, I think we will have failed, because that's not going to make the change that we need to make. I really think we're going to have to take a more active approach in highlighting what the vulnerabilities are, you know, and at helping organizations evaluate for themselves which of those best practices and guidance are being followed, and which are not. And I'm hopeful that we can do that in a way that really doesn't resemble overregulation, but is really government being helpful. So, again, thank you very much, Chairman Foster, and I'm looking forward to hearing from our witnesses. I yield back.

[The prepared statement of Mr. Obernolte follows:]

Thank you, Chairman Foster and Chairwoman Stevens, for holding today's hearing on improving the cybersecurity of software supply chains. And thank you to the panel of expert witnesses for taking time to help educate us on this very timely and important topic.

Recent cyber incidents like SolarWinds, Microsoft Exchange, and Colonial Pipeline have thrust the issue of cybersecurity into the limelight. The most notorious and perhaps the most pernicious of these incidents is SolarWinds - a software supply chain attack that impacted roughly 100 organizations and at least 9 Federal agencies.

Although analysis and investigation into this incident is ongoing, the details that have emerged thus far paint a troubling picture for the state of Federal cybersecurity.

Advanced cyber actors infiltrated SolarWinds' build environment, surreptitiously implanted malicious code into a an otherwise valid software update, and then waited for that update to be downloaded. Ultimately, the actors responsible for this software supply chain attack abused the trusted relationship that SolarWinds had with its customers—including federal entities-by compromising the software update with a "backdoor" that could be leveraged against the actors' intended targets, like the 9 federal agencies impacted by this incident. The update was then made available for download by SolarWinds' customers, with no indication to them that the update had been tainted by cyber adversaries.

The amount of time that this actor was able to lie dormant, undetected in federal networks is particularly concerning - it took almost two years before Federal agencies discovered the intrusion. And only then with the help of the cybersecurity firm FireEye. The SolarWinds incident makes clear that the Federal government must do more to secure its software supply chains.

In December 2020, GAO published a report based on its investigation into federal agency implementation of Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) foundational practices. The findings are disturbing.

GAO found that none of the federal agencies it reviewed had fully implemented foundational practices for ICT SCRM, and that roughly 60% of the agencies reviewed had not implemented any of the foundational ICT SCRM practices. This is unacceptable.

In May, the Biden Administration signed Executive Order 14028 on improving the nation's cybersecurity. The EO, among other things, tasks NIST with identifying existing or developing new guidance to help improve the security of software supply chains.

While this is a step in the right direction, proper implementation is critical to its success. For example, NIST has several products to inform Federal agency ICT SCRM practices. In fact, the GAO report I referenced earlier derived its seven foundational ICT SCRM practices from NIST guidance. Nevertheless, the reason most frequently cited by agencies for their failure to implement identified practices was a lack of clear Federal guidance. Without proper implementation by Federal agencies, more guidance, best practices, and other resources will be useless.

To that end, we need to find a better way to conduct oversight of agencies' implementation of this guidance, and agencies must be more accountable for their responsibilities under *FISMA* to secure the information and systems for which they are responsible.

I look forward to learning more from our witnesses today about how we can get agencies the implementable guidance that they need to shore up the security of their software supply chains, and the resources needed to see implementation is carried out across the board.

Thank you to our panelists for being here today. And thank you again to Chairman Foster and Chairwoman Stevens for holding this important hearing. I yield back the balance of my time.

Chairman FOSTER. Thank you. And the Chair will now recognize Ms. Stevens for an opening statement.

Ms. STEVENS. Yeah. Thank you so much, Congressman and Dr. Foster. Thank you to you and Congressman Obernolte for holding today's hearing, and I'm pleased to give opening remarks on behalf of the Research and Technology Subcommittee that has direct oversight of the National Institute of Standards and Technology, which we're certainly going to be talking about today, as it relates to our supply chain vulnerability, something that we know very well here in Michigan. It's very real. Right across from me is a poster from the Michigan Manufacturing Technology Center, our NIST MEP (Manufacturing Extension Partnership) Center, located just a few short miles from where I sit right now, on our Cybersecurity and Industry 4.0 Imperative. So it's—is clear that this hearing is coming at a critical and an auspicious time.

President Biden's recent Executive order improving the Nation's cybersecurity represents what I hope to be a sea change in how the Federal Government approaches cybersecurity, from modernizing Federal IT systems, to strengthening how the government responds to cyber threats from our adversaries. The Executive order also focuses heavily on software supply chain issues, which is the topic of this hearing. It—the Executive order seeks to help software developers identify vulnerabilities before they release their software, and helps consumers better understand the security, and certainly the best practices, that are going to be a huge part of setting the standards and level setting industries of scale here.

It should not be a surprise that, you know, we're ready to lean in on the NIST component and have NIST represented here on this panel to talk about their leadership in cybersecurity. I was bragging about NIST cybersecurity initiatives earlier today. NIST has played a huge role in the implementation of the Executive order I just referenced. The agency is going to develop a broad set of standards for the security of the supply chain within 90 days. Within 60 days the agency is also going to identify and define what constitutes as critical software, and create special standards to protect it. Also within 60 days, NIST will develop standards so that software developers can test their source code.

This is something Dr. Baird and I explored and sat down together on in the—in a meeting. It wasn't a hearing, it was a meeting, last legislative session of Congress. These are certainly aggressive timelines, and I only mentioned some of the things that NIST is going to be doing, but it's, again, just a reminder of the important and critical role they play that is highly respected in incorporating input from private and public sector partners to develop effective cybersecurity standards. This work is certainly going to take time and resources, no doubt about that. NIST's entire cybersecurity and privacy portfolio was funded at only $78 million in the last year's budget, and, you know, we think about the eco-

nomic ramifications of cybersecurity attacks, those bills tally up to that number, you know, it—within seconds should there be a cybersecurity attack, so I do worry that we are increasingly asking NIST experts to do exponentially more work more quickly, without necessarily the adequate resources.

We've referenced and talked about the GAO. They have found that Federal agencies are not adopting the guidelines already on the books to deal with software supply chain threats. We're certainly seeing this across industries. I've had these conversations here in Michigan, particularly in our manufacturing sectors, automotive, defense, aerospace. Additional guidance is maybe going to be necessary, but we also must ensure agencies prioritize the implementation of the guidance that already exists, and provides adequate resources for them to do so. Congress, and the Biden Administration, must and will think creatively about modernizing the Federal Government's approach to cybersecurity. I welcome the recommendations of this expert panel on how we can ensure that cybersecurity guidance is developed as part of the Executive order that is operational, effective, and relatively easy to adopt. I want to thank our witnesses again, as well as our other Subcommittee Chair, for helping us tackle these issues, and with that, I yield back.

[The prepared statement of Chairwoman Stevens follows:]

Good morning and welcome to this joint hearing of the Subcommittee on Research and Technology and the Subcommittee on Investigations and Oversight. I would like to thank my esteemed colleagues, Chairman Foster and Ranking Member Obernolte, for leading this joint hearing. As the SolarWinds incident revealed, software supply chain issues are a threat to our Federal agencies and businesses across the country, including my district in Michigan.

This hearing comes at an auspicious time. President Biden's recent Executive Order "Improving the Nation's Cybersecurity" represents what I hope to be a sea change in how the Federal government approaches cybersecurity, from modernizing Federal IT systems to strengthening how the government responds to cyber threats from our adversaries.

The Executive Order focuses heavily on software supply chain issues, the topic of this hearing. It seeks to help software developers identity vulnerabilities before they release their software and help consumers better understand the security of the products they buy.

It should not be a surprise that I am excited to have NIST represented on this panel to talk about their leadership in cybersecurity standards and best practices.

NIST has a big role to play in the implementation of the Executive Order. The agency must develop broad standards for the security of the software supply chain within 90 days. Within 60 days, the agency must also identify and define what constitutes "critical software" and create special standards to protect it. Also within 60 days, NIST must develop standards so that software developers can test their source code. These timelines are aggressive, and I only mentioned some of the things that NIST is being asked to do.

NIST is highly respected for its role in incorporating input from its private and public sector partners to develop effective cybersecurity standards. But this work takes time and resources. NIST's entire cybersecurity and privacy portfolio was funded at only $78 million in last year's budget. I worry that we are increasingly asking NIST's experts to do exponentially more work, more quickly, with inadequate resources.

Moreover, GAO has found that Federal agencies are not adopting the guidance already on the books to deal with software supply chain threats. Additional guidance may be necessary, but we must also ensure agencies prioritize implementation of the guidance that already exists, and provide adequate resources for them to do so.

Congress and the Biden Administration must think creatively about modernizing the Federal government's approach to cybersecurity. I welcome the recommendations of this expert panel on how we can ensure that cybersecurity guidance devel-

oped as part of the Executive Order is operational, effective, and relatively easy to adopt.

I want to again thank the witnesses for being here today to help us tackle these challenging issues. I yield back.

Chairman FOSTER. Thank you. And the chair will now recognize Mr. Waltz for an opening statement.

Mr. WALTZ. Hey, thank you. Thank you, Chairman Foster, and Chairwoman Stevens, for holding this joint hearing. I also want to thank our panel of witnesses for their participation, and I am looking forward to hearing their testimony today. And I hope we will all be able to use this opportunity to learn more about software supply chain attacks, impacts on Federal agencies, and I share everyone's sentiments on how to improve our Nation's software supply chain security.

So—the Committee on Science, Space, and Technology has held several hearings over the years. Some of them have been mentioned, on bolstering the Federal Government's cybersecurity posture. I'm pleased to see that this Committee is playing such an active role in that posture. Obviously the recent SolarWinds, Microsoft Exchange, Colonial Pipeline incidents make it clear that the United States is being continuously targeted with malicious cyberattacks. When I was in business, there was the saying, those that have been attacked, and those that don't know they've been attacked, by various criminal actors and nation-states.

So, unfortunately, these attacks were not the first. They won't be the last. I share the Chairwoman's focus on NIST as the primary Federal agency responsible for setting standards and guidelines for Federal agencies, and providing voluntary best practices for private industry. It's worth noting that in 2014 NIST published a voluntary risk-based cybersecurity framework with a set of industry standards and best practices to help organizations manage these risks. NIST also established guidance specifically related to supply chain security, including the Cyber Supply Chain Risk Management, the CSRM Framework, and the Secure Software Development Framework, to help identify, assess, and mitigate these risks.

On May of this year, as Chairwoman Stevens mentioned, the president issued his EO on improving the Nation's cybersecurity, entrust multiple Federal agencies, including NIST, with strengthening the security of software supply chain. I think it's worth noting Section Four of the EO directs the Secretary of Commerce, through NIST, to consult with Federal agencies, private sector, academia, all of the stakeholders, to identify or develop standards, tools, best practices, and other guidelines to enhance our supply chain security. And, based on my experience, 25 years now in the National Guard, I would encourage NIST, and would love to see them consult with the cyber talent within the Guard and the Reserve in executing Section Four of the EO. The Guard and the Reserve really does retain elite cyber talent from Silicon Valley, the private sector, as well as the Pentagon, and truly can serve as a bridge between the private sector and Federal Government with their various authorities. I think the EO is a good starting point for addressing these vulnerabilities in our Nation's software supply chain, but obviously we have a long way to go, a lot more work to do.

As has been mentioned, the recent GAO report, it really is alarming, and assessing that Federal information and communication supply chain risk management practices, and the findings that none of the Federal agencies reviewed had implemented the recommended practices. 60 percent of these agencies had not implemented any of the practices. I'm sorry, none have fully implemented those practices. And, as a result, GAO identifies 145 recommendations for agencies to fully implement foundational practices in their approach to ICT (information and communications technology) SCRM.

Moving forward, I do think we need to provide agencies with the resources, and push them, frankly, to move more quickly to close the gap between these recommendations and implementations of foundational practices. Cyber frameworks are otherwise useless, frankly, unless proper fundings were available to fully implement them. Additionally, the National Science Foundation's Cyber Corps, Scholarship for Service Program, should receive consideration by the Committee for enhancing the Federal Government's cybersecurity workforce. Time truly is of the essence here. It's imperative that we modernize these defenses and get ahead of our adversaries. We cannot afford to continue to allow foreign adversaries, and criminals, often working together, witting and unwitting, to take advantages of our weaknesses in software supply chains. I think we've seen in recent days that the consequences truly can be catastrophic and detrimental to the economic and national security of the United States. Thank you, Mr. Chairman. I yield back.

[The prepared statement of Mr. Waltz follows:]

Thank you, Chairman Foster and Chairwoman Stevens for holding today's joint subcommittee hearing.

I also want to thank our distinguished panel of witnesses for their participation today. I am looking forward to hearing your expert testimony. I hope we will use this opportunity to learn more about software supply chain attacks and their impacts on federal agencies and examine how to improve our nation's software supply chain security. The Committee on Science, Space, and Technology has held several hearings over the years on bolstering the federal government's cybersecurity, and I am pleased to see that the Committee is still playing an active role in enhancing our nation's cybersecurity posture.

The recent SolarWinds, Microsoft Exchange, and Colonial Pipeline incidents make it clear that the United States is continuously being targeted with malicious cyberattacks by nation-states and criminal actors. China, Russia, Iran, and other malign actors are focusing on cyber capabilities. Unfortunately, these attacks are not the first, and certainly will not be the last of their kind.

The National Institute of Standards and Technology (NIST) is the primary federal agency responsible for setting standards and guidelines for federal agencies and provides voluntary best practices for private industry. In 2014, NIST published a voluntary risk-based Cybersecurity Framework with a set of industry standards and best practices to help organizations manage cybersecurity risks. Additionally, NIST has established guidance specifically related to supply chain security, including the Cyber Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework (SSDF) to help identify, assess, and mitigate supply chain risks.

On May 12, 2021, the President issued an Executive Order (EO) on Improving the Nation's Cybersecurity, which entrusts multiple federal agencies, including NIST, with strengthening the security of the software supply chain. Section 4 of the EO directs the Secretary of Commerce, through NIST, to consult with federal agencies, the private sector, academia, and other stakeholders and to identify or develop standards, tools, best practices, and other guidelines to enhance software supply chain security.

Based on my experience in the National Guard, I would like to see NIST consult with the cyber talent within the Guard when executing Section 4 of the EO. The National Guard and Reserve retains elite cyber talent from both Silicon Valley and the Pentagon and can effectively serve as a bridge between the private sector and federal government.

This EO is a good starting point for addressing vulnerabilities in our nation's software supply chain, but there is more work to be done.

A recent Government Accountability Office (GAO) report assessed federal information and communications (ICT) supply chain risk management (SCRM) practices and the findings are alarming. None of the federal agencies reviewed had fully implemented the SCRM practices, and approximately 60 percent of these agencies had not implemented any of the practices. As a result, GAO identifies 145 recommendations for agencies to fully implement foundational practices in their approach to ICT SCRM.

Moving forward, we must work diligently to provide agencies with the resources to move swiftly to close the gap between recommendations and implementation of foundational practices. Cybersecurity frameworks are otherwise useless unless proper funding and support are available to fully implement them.

Additionally, NSF's CyberCorps: Scholarship for Service program should receive consideration by the committee for enhancing the federal government's cybersecurity workforce.

Time is of the essence, and it is imperative that modernized cyber defenses are implemented to get ahead of the next cyber-attack from China, Russia, Iran and other adversaries. We cannot afford to let foreign adversaries and cyber criminals take advantage of weaknesses in software supply chains as the consequences can be detrimental to the national and economic security of the United States.

Thank you, and I yield back.

Chairman FOSTER. Thank you. And if there are any other Members who wish to submit additional opening statements, your statements will be added to the record at this point.

[The prepared statement of Chairwoman Johnson follows:]

Good afternoon to our witnesses and thank you for joining us here today.

Securing Federal government systems from cyberattack is an evolving challenge. We have repeatedly seen the importance of getting it right, and the painful consequences of getting it wrong. As SolarWinds and other recent attacks have shown, the software supply chain is especially challenging to protect. We must ensure that the Federal Government is coordinating effectively to secure our IT systems.

Jurisdiction over cybersecurity is widely shared across Congressional committees and Federal agencies. I want to affirm the Science Committee's role on cybersecurity matters. The scope of jurisdiction for authorizing committees in the technology space was last changed significantly in 2002. That's when Congress created the House Homeland Security Committee and the Department of Homeland Security in response to 9/11.

That same year, Congress passed the *Federal Information Security Management Act*, or *FISMA*. *FISMA* was updated in 2014 and became the Federal Information Security Modernization Act. *FISMA* called on Federal agencies to develop information security programs to protect themselves. The Science Committee focus is on developing tools for prevention. Specifically, we are responsible for directing and overseeing the National Institute of Standards and Technology's role in cybersecurity. Under *FISMA*, NIST creates cybersecurity standards and guidance for the government. The Science Committee is one of the three House Committees that receives cyber incident reports under *FISMA*.

It's hard to comprehend how much the cybersecurity landscape has changed since 2002. The threats that Federal agencies and the private sector face today are sophisticated and relentless. Recent attacks have shown that existing oversight mechanisms are not enough. After the SolarWinds attack was revealed, information was slow to emerge. Briefings and reports to Congress were unpredictable in their timing and their content. Federal agencies reported that they were not able to share information with other agencies. Determinations of whether the incident was reportable to Congress or not were based on a one-size-fits-all form. I worry we are not capturing the full extent of the potential harm from attacks on our Federal systems.

We must do better, both in mitigating attacks after they happen and in preventing them in the first place.

This has been and will continue to be a bipartisan concern on this Committee. I look forward to continuing to work with Ranking Member Lucas and our colleagues on the Committee to reinforce NIST's role in cybersecurity.

There is simply so much work to be done on cybersecurity—both for policymakers and for practitioners in the field. I am glad that the witnesses here today offer a wide range of expertise to help us chart our next steps.

Thank you, and I yield back.

Chairman FOSTER. And at this time I'd like to introduce our witnesses. Our first witness is Mr. Matthew Scholl. Mr. Scholl is the Chief of the Computer Security Division of the Information Technology Laboratory at NIST. He—his research program cultivates trust in information technology through standards and measurements, and by testing the interoperability, security, and reliability of cybersecurity systems. The guidance produced by his program is widely used by Federal agencies and U.S. industry. He also co-leads NIST's participation with cybersecurity national and international standards development organizations.

After Mr. Scholl is Dr. Trey Herr. Dr. Herr is the Director of the Cyber Statecraft Initiative at the Atlantic Council. His team works on a range of cybersecurity issues, including cloud computing, the security of the internet, supply chain policy, and growing a more capable cybersecurity policy workforce. Previously he was a Senior Security Strategist at Microsoft, working on cloud computing and the supply chain—and supply chain security policy. Dr. Herr also served as a fellow at the Belfer Cyber Security Project at Harvard's Kennedy School, and a non-resident fellow with the Hoover Institution at Stanford University.

Our third witness is Ms. Katie Moussouris. Ms. Moussouris is Founder and CEO (chief executive officer) of the cybersecurity company Luta Security. She led the launch of the first bug bounty programs at both Microsoft and the Department of Defense, and has also helped start Microsoft's Supply Chain Vulnerability Program. She is a co-author of documentation on vulnerability disclosure and vulnerability handling processes for the International Organization for Standardization (ISO). Ms. Moussouris is a visiting scholar with the MIT (Massachusetts Institute of Technology) Sloan School, a Harvard Belfer affiliate, and advisor to the Center for Democracy and Technology.

Our final witness is Mr. Vijay D'Souza. Mr. D'Souza is the Director of the—Information Technology and Cybersecurity at the GAO, where he leads a diverse set of evaluations and—on government cybersecurity and IT issues. His current work focuses on the SolarWinds breach, use of the NIST cybersecurity framework, and IT modernization efforts at USDA (United States Department of Agriculture). Mr. D'Souza also leads GAO's Center for Enhanced Cybersecurity, which provides advanced technical support for GAO's Cybersecurity Office.

And, as our witnesses should know, each of you have five minutes for your spoken testimony. Your written testimony will be included in the record for the hearing, and when you've all completed your spoken testimony, we will begin with questions. Each Member will have five minutes to question the panel. And I will also mention that at the end of our hearing here, after I gavel it closed, any of our witnesses and Members who wish are welcome to sort of hang around and talk informally, which is often a very valuable part of hearings that we do informally at the end when we're meet-

ing in the non-virtual world. And we will start now with Mr. Scholl. You are now recognized for five minutes.

**TESTIMONY OF MR. MATTHEW SCHOLL,
CHIEF, COMPUTER SECURITY DIVISION
OF THE INFORMATION TECHNOLOGY LABORATORY,
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY (NIST)**

Mr. SCHOLL. Thank you. Chairwoman Stevens, Ranking Member Waltz, Chairman Foster, Ranking Member Obernolte, and Members of the Subcommittee, I am Matt Scholl, the Chief of the Computer Security Division at the National Institute of Standards and Technology, known as NIST. Thank you for the opportunity to testify today on improving the cybersecurity of software supply chains. NIST has nearly a 50-year history working in cybersecurity. Most recently, threat activity has highlighted the IT supply chain as a major cybersecurity vulnerability. Cybersecurity risks associated with extended supply chains and supply ecosystems are significant, and the scope of these risks must be understood by companies and organizations as they continue to expand their use of digital technologies.

To address the ever-challenging issues related to this cybersecurity risk, on May 12 President Biden signed Executive Order 14028 to improve the Nation's cybersecurity and to protect Federal Government networks. Recent cybersecurity incidents, such as the SolarWinds type of incident we are discussing here, are a sobering reminder that U.S. public and private sector entities face increasingly sophisticated malicious cyber activity from both nation-state actors, as well as cyber criminals. NIST's role in this Executive order will be to develop standards, tools, best practices, references, and other key guidance for use by any organization to enhance their software supply chain security.

Specifically, NIST will address identifying and securing critical software. We will identify secure software development life cycles and practices for securing development environments. We will also identify security measures for the Federal Government in using critical software, and requirements for testing software. In addition, NIST will initiate two pilot labeling programs to assist consumers in understanding the security properties in products that we all use. NIST will respond to these responsibilities in ways that are effective in reducing risks to our supply chain, while also continuing to facilitate the innovation and economic growth that a secure software ecosystem can provide.

NIST's arsenal in the defense against cyberattacks is large and growing. NIST is responsible for developing reliable and practical standards, guidelines tests, and metrics to help organizations with their cyber supply chain risk management. The public and private sector can use these NIST resources to create and conduct their cyber supply chain risk management programs. NIST also continues to work directly with Federal agencies through practice guides, tools, models, best practices, quora, as well as membership on the Federal Acquisition Security Council (FASC).

NIST provides a series of documentary guidance, data reference, tools, and testing as part of its program to specifically work on im-

proving the efficiency, reliability, and security of software. Two specific examples of resources that NIST provides are the National Vulnerability Database and the National Software Reference Library. The National Vulnerability Database is a repository of all known and publicly reported IT vulnerabilities, and is the authoritative source for standardized information on security, vulnerabilities which NIST updates daily. The National Software Reference Library creates unique digital signatures of software so that any organization can efficiently search for that software, and determine if and where it might be deployed within its ecosystems. Another critical resource at NIST is the National Cybersecurity Center of Excellence. This collaborative hub is a place where industry organizations, government agencies, and academic institutions work together to address business's most pressing cybersecurity issues. We produce practical cybersecurity solutions that benefit large and small businesses and third-party service providers alike.

In conclusion, NIST is proud of its role in establishing and improving cybersecurity solutions, as well as our longstanding and robust collaborations with our Federal Government partners, private sector collaborators, and international colleagues. NIST has continued to be committed to apply its expertise and help to solve the critical cybersecurity issues that face our Nation now, as well as in the future. I thank you for the opportunity to testify today, and I will be pleased to answer any questions that you might have.

[The prepared statement of Mr. Scholl follows:]

Testimony of

Mr. Matthew A Scholl.
Chief
Computer Security Division
Information Technology Laboratory

National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space and Technology
Subcommittee on Research and Technology
and
Subcommittee on Investigations and Oversight

"SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains"

May 25, 2021

Chairwoman Stevens, Ranking Member Waltz, Chairman Foster, Ranking Member Obernolte and Members of the Subcommittee, I am Matthew Scholl, the Chief of the Computer Security Division, of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology – known as NIST. Thank you for the opportunity to testify today on SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains, which is of critical importance to the security and economic well-being of America.

NIST is home to five Nobel Prize winners, with programs focused on national priorities such as artificial intelligence, advanced manufacturing, the digital economy, precision metrology, quantum science, biosciences and, of course, cybersecurity. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST has a long history of working in support of cybersecurity including securing the nation's supply chains. There are many risks that need to be managed in supply chains. This includes availability of product, shipping, component availability, quality, interoperability, costs, delivery and now –more than ever – cybersecurity. As we have gotten better at understanding threat actors, managing cybersecurity risks and identifying vulnerabilities, our adversaries have improved their ability to compromise the confidentiality, availability and integrity of our information and information systems. Recent threat activity has highlighted the IT supply chain as one of these vulnerabilities. The ability to participate in the digital economy is available to almost everyone who can write software and participate in an opensource project. This enables the world to benefit from innovation, entrepreneurial spirit, expertise, and imagination at a scale never before seen, but the risks need to be understood and managed along with these benefits.

Organizations increasingly rely on an array of suppliers to support their critical functions and business missions. All organizations rely on acquiring products and services, and most organizations also supply products and services to individuals, groups, or other organizations. Supply chain management is an established discipline and is one of the key capabilities for enabling economic growth. These trends have resulted in organizations that no longer fully control the supply ecosystems of the products that they produce and procure, or the services that they rely on or deliver.

Cybersecurity risks associated with extended supply chains and supply ecosystems are significant, and those risks are difficult to understand by many organizations as they continue to expand their use of digital technologies to support critical functions or create digital products for their customers.

President's Executive Order on Cybersecurity – EO 14028

To address the ever-challenging issues related to cybersecurity, on May 12th, President Biden signed a critical Executive Order to improve the nation's cybersecurity and protect federal government networks. Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident that we are discussing at this hearing are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. These incidents share commonalities,

including insufficient cybersecurity defenses that leave public and private sector entities more vulnerable to incidents.

The President's Executive Order makes a significant contribution toward modernizing cybersecurity defenses by protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur. It is the first of many ambitious steps the Administration is taking to modernize national cyber defenses. However, the Colonial Pipeline incident is a reminder that federal action alone is not enough. Much of our domestic critical infrastructure is owned and operated by the private sector, and the tools and resources NIST produces can be used by the private sector when determining their own cybersecurity risk and the management of that risk throughout supply chains.

Specifically, section 4 of the order directs the Secretary of Commerce, through NIST, to solicit input from federal agencies, the private sector, academia, and other stakeholders and to identify or develop standards, tools, best practices, and other guidelines to enhance software supply chain security. NIST's work will address identifying and securing critical software, secure software development lifecycles and secure development environments, security measures for federal government, and requirements for testing software.

The EO assigns additional responsibilities to NIST, including initiating two pilot labeling programs related to secure software development practices and the Internet of Things to inform consumers about the security of their products. NIST will conduct these programs working closely with other government agencies and private and public sector organizations and individuals through our open, transparent and inclusive processes. Our goal is to respond to these responsibilities in ways that are effective in reducing risks to our software supply chains while continuing to facilitate the innovation and economic growth that a secure software ecosystem can provide.

NIST's arsenal in the defense against cyber attacks is large and growing. The rest of my testimony will cover the tool and products we have developed in support of the nation's strong cyber stance.

NIST's Role in Cybersecurity

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it helped develop and published the Data Encryption Standard, which enabled efficiencies with security, like the electronic banking that we all enjoy today. NIST's role is to provide standards, guidance, tools, data references, and testing methods to protect information systems against threats to the confidentiality, integrity, and availability of information and services. This role was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies as well as businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-the-art, and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

Cyber Supply Chain Risk Management

When a device's supply chain is compromised, its security can no longer be assured, whether it is a chip, laptop, server, or any other technology. NIST is responsible for developing reliable and practical standards, guidelines, tests, and metrics to help organizations with their Cyber Supply Chain Risk Management (C-SCRM). The private and public sector can use these NIST-produced resources to create and conduct Cyber Supply Chain Risk Management Programs. That includes organizations developing or using information, communications, and operational technologies that depend upon complex, globally distributed, and interconnected supply chains. These supply chains cover the life cycle of technology—from research and development, design, and manufacturing to acquisition, delivery, integration, operations and maintenance, and disposal.

NIST's Cyber Supply Chain Risk Management Program

Managing cyber supply chain risk requires ensuring the integrity, security, quality, and resilience of the supply chain and its products and services. In order to assure this, NIST focuses on:

- **Foundational Practices**: C-SCRM lies at the intersection of information security and supply chain management. Existing supply chain and cybersecurity practices provide a foundation for building an effective risk management program.
- **Enterprise-Wide Practices**: Effective C-SCRM is an enterprise-wide activity that involves each tier (Organization, Mission/Business Processes, and Information Systems) and is implemented throughout the system development life cycle.
- **Risk Management Processes**: C-SCRM should be implemented as part of overall risk management activities. That involves identifying and assessing applicable risks and determining appropriate response actions, developing a C-SCRM Strategy and Implementation Plan to record selected response actions, and monitoring performance against that plan.
- **Critical Systems**: Cost-effective supply chain risk mitigation requires organizations to identify those systems/components that are most vulnerable and will cause the largest organizational impact if compromised

NIST has collaborated with public and private sector stakeholders to research and develop C-SCRM tools and metrics, producing case studies and widely used guidelines on mitigation strategies. These multiple sources reflect the complex global marketplace and assist federal agencies, companies, and others to manage supply chain risks which threaten their information

systems and organizations. The SECURE Technology Act and FASC Interim Final Rule gave NIST a specific role in developing C-SCRM guidelines.

Focusing on federal agencies – while also engaging with and providing resources useful to other levels of government and the private sector – NIST:

- Produced *Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP 800-161)* to guide organizations in identifying, assessing, and responding to supply chain risks at all levels. It is flexible and builds on organizations' existing information security practices. NIST is currently updating this primary technical resource using feedback from federal and industry partners.
- Participates in the Federal Acquisition Security Council, or FASC, created by law in 2018. The Council is authorized to develop policies and processes for agencies to use when purchasing technology products and services, and to recommend C-SCRM standards, guidelines, and practices that NIST should develop.
- Issued *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks (NISTIR 8272)*, which describes a prototype solution for filling the gap between an organization's risk appetite and supply chain risk posture by providing a basic measurement of the potential impact on a cyber supply chain.
- Released *Criticality Analysis Process Model: Prioritizing Systems and Components (NISTIR 8179)*, aimed at identifying systems and components that are most vital and may need additional security or other protections.
- Finalized *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (NISTIR 8276)*, summarizing practices foundational to an effective C-SCRM program.
- Hosts the Federal C-SCRM Forum, which fosters collaboration and the exchange of information among federal organizations to improve the security of their supply chains. It includes those responsible for C-SCRM in the federal ecosystem, among them the Office of Management and Budget (OMB), Department of Defense (DOD), Office of the Director for National Intelligence (ODNI), Cybersecurity and Infrastructure Security Agency (CISA), General Services Administration (GSA), and NIST.
- Co-leads the Software and Supply Chain Assurance Forum with DOD, the Department of Homeland Security (DHS), and GSA. The Forum provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding software and supply chain risks, effective practices and mitigation strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.

Software Security

NIST provides a series of documentary guidance, data references, tools and testing as part of its program to work on improving the efficiency, reliability and security of software. Below are highlighted a few of these items that are used across the different areas of a software lifecycle.

The National Vulnerability Database

Protecting information technology is critical and NIST plays a key role in this area by maintaining the repository of all known and publicly reported information technology vulnerabilities, called the National Vulnerability Database (NVD). The NVD is an authoritative source for standardized information on security vulnerabilities that NIST updates regularly.

The vulnerabilities catalogued in the NVD are weaknesses in coding found in software and hardware that, if exploited, can impact the confidentiality, integrity, or availability of information or information systems. The NVD tracks vulnerabilities over time and allows users to assess changes in vulnerability discovery rates within specific products or specific types of vulnerabilities.

The NVD is the second most frequently accessed website at NIST, after the NIST time service, and is used across the country by the IT and cybersecurity industry, by cybersecurity tools and scanners, by other nations and by computer emergency response teams around the world.

National Software Reference Library
NIST hosts the National Software Reference Library (NSRL). The NSRL creates digital signatures of software so that an organization can efficiently search its networks for that software and determine if and where the software is deployed.

The NSRL collects software from various sources and incorporates profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and private industry to review files on a computer by matching profiles in the RDS. This process helps alleviate much of the effort involved in determining which files on a computer are important forensics evidence.

Businesses and government agencies both use the NSRL RDS as part of their routine IT operations to ensure there are no malicious or unverified files on their systems.

Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)
NIST, working with multiple partners across the software industry, wrote a white paper that recommends a core set of high-level secure software development practices called a secure software development framework (SSDF) that can be integrated with any software development lifecycle. This paper facilitates communications about secure software development practices among business owners, software developers, project managers and leads and cybersecurity professionals within an organization.

Software Assurance Metrics And Tool Evaluation (SAMATE)
The NIST SAMATE project is dedicated to improving software assurance by developing methods to enable software tool evaluations, measuring the effectiveness of tools and techniques, and identifying gaps in tools and methods. The scope of the SAMATE project is broad, ranging from a periodic evaluation of static analysis tools to improving the understanding of software bugs to formal methods and AI-enabled bug finding.

Software Assurance Reference Dataset (SARD)
SARD provides users, researchers, and software security assurance tool developers with a set of known security flaws. This allows end users to evaluate tools and tool developers to test their methods. The dataset includes "wild" (production), "synthetic" (written to test or generated), and "academic" (from students) test cases. This database also contains real software application with known bugs and vulnerabilities. The dataset includes a wide variety of possible vulnerabilities and languages.

National Cybersecurity Center of Excellence (NCCoE)

Established in 2012, NIST's National Cybersecurity Center of Excellence (NCCoE)[2] is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges.

Through consortia under Cooperative Research and Development Agreements, including private sector collaborators—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. Working with communities of interest, the NCCoE produces practical cybersecurity solutions that benefit large and small businesses, and third-party service providers in diverse sectors.

The NCCoE has many published practice guides, on-going projects exploring solutions, and upcoming projects exploring new challenges and building communities of interest that all directly support many of the cybersecurity issues we have today. There are several projects focused on supply chain security that are currently underway at the NCCoE. One of these projects is aimed at identifying methods to help organizations verify that the internal components (chips) of purchased computing devices are genuine and have not been altered during the devices' lifecycle (from manufacturing to distribution, after sale from a retailer, and until the device is retired from service). Another project is working to demonstrate effective and efficient methods to patch software in a managed enterprise.

Conclusion

Our economy is increasingly global, complex, and interconnected. It is characterized by rapid advances in information technology. IT products and services need to provide sufficient levels

[2] https://www.nccoe.nist.gov/

of cybersecurity and resilience. The timely availability of international cybersecurity standards and guidance is a dynamic and critical component for the cybersecurity and resilience of all information and communications systems and supporting infrastructures.

The NIST's C-SCRM program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of information and information systems. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

NIST is proud of its role in establishing and improving the set of cybersecurity technical solutions, standards, guidelines, and best practices, and of the longstanding and robust collaborations we've established with our federal government partners, private sector collaborators, and international colleagues. Supply chain risk management is a complex issue that is not solely a cybersecurity problem, but an issue that needs to be addressed at an enterprise level. NIST is committed to applying its core values of excellence and persistence as we work with all of our stakeholders to continuously improve NIST standards, guidance, tools and other resources, and to identify new resources to help solve the critical issues facing our nation.

Thank you for the opportunity to present NIST's activities on C-SCRM and software assurance. I will be pleased to answer any questions you may have.

Matthew A Scholl

Matthew Scholl is the Chief of the Computer Security Division (CSD) in the Information Technology Laboratory (ITL) at the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). CSD, one of seven Divisions within ITL, has an annual budget of $32 million, nearly 100 federal employees, and an additional approximately 50 guest researchers from industry, universities, and foreign laboratories.

Mr. Scholl oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry.

He also co-leads NIST's participation with Cybersecurity National and International Standards Development Organizations (SDOs) and associated conformance testing programs.

Mr. Scholl has a Master's in Information Systems from the University of Maryland and a bachelor's degree from the University of Richmond.

He is a U.S. Army veteran and currently has more than 20 years of federal service.

Mr. PERLMUTTER. Bill, you need to unmute.

Chairman FOSTER. Did—who did that to me? OK. Next is Dr. Herr.

TESTIMONY OF DR. TREY HERR, DIRECTOR, CYBER STATECRAFT INITIATIVE, ATLANTIC COUNCIL

Dr. HERR. Chairman Foster, Ranking Member Obernolte, Chairwoman Stevens, and Ranking Member Waltz, and the Members and staff of the Subcommittees, thank you for the invitation to speak today. My name is Trey Herr, and I run the Cyber Statecraft Initiative at the Atlantic Council, a non-partisan think tank based here in D.C. For the past 2 years my team and I have been looking at the security of software supply chains and cataloguing a range of attacks against them. We're here in no small part because of the revelations about the Sunburst and SolarWinds campaign. The scale of this event, and its impact on the cybersecurity policies of a new administration, have received widespread appreciation, and this attention is duly warranted. But even in the crises of the past few months, there were remarkable echoes of the past decade. Software supply chain attacks are not new, and they're becoming more visible and more consequential by the day.

Over the past 10 years there have been more than 140 attacks or disclosures of vulnerabilities fit to be used in such an attack against software supply chains. Of these, at least 30 had been positively attributed to governments around the world. Within just a few months of the public discovery of the Sunburst SolarWinds campaign, cybersecurity vendors reported three different state-backed software supply chain attacks targeting governments and high-profile companies in South Korea, Mongolia, and Vietnam. Where the most recent crisis impacted hundreds of organizations, and perhaps tens of thousands of users, software supply chain attacks have been used to target millions of users at once.

Software has spread to every corner of the human experience. Our watches have internet connections. Combat aircraft come with more code than many operating systems, and embedded software controls the operation of everything from medical hardware to our brake pedals. With this software comes security flaws, and a long chain of updates from vendors and developers. This ongoing relationship between those that build code and those who use it creates a need for trust, trust that the update you're about apply is genuine and benign. Software supply chain attacks take advantage of and break this trust. The responsibility for the insecurity of these software supply chains lies at home more than with foreign adversaries. I'm encouraged by the proposals contained in the President's recent Executive order. We can demand more of our vendors, and of ourselves, while learning from the lessons of Sunburst, and a decade of software supply chain attacks.

In the final analysis it would be a mistake to equate software supply chain attacks to a new weapons system in an opponent's arsenal. These attacks are a manifestation of opportunity, pursuing targets, compromising weaknesses and the tools and code we depend on, and which we even take for granted. Trust in software supply chain security is not built, nor is it broken, in isolation. There are opportunities for meaningful progress, and this can play

an important role to better protect the code we have embedded in our daily lives with appropriate investment, and greater focus on cloud security, automatable guidance, and secure software deployment, not just development.

I commend the Committee for the time and effort taken to prepare today's hearing. Recent events show us it is an unambiguously important topic. With that, I look forward to your questions.

[The prepared statement of Dr. Herr follows:]

Testimony of

Dr. Trey Herr
Director, Cyber Statecraft Initiative
Atlantic Council

Before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Investigations and Oversight & Subcommittee on Research and Technology

"SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains"

May 25, 2021

Chairman Foster, Chairwoman Stevens, Ranking Members Obernolte and Waltz, and members and staff of the sub-committees – thank you for the invitation to speak today. We are here in no small part because of the revelations about the Sunburst/SolarWinds campaign. In this instance, the length of time the adversary remained in US networks, public and private, is staggering and suggests incredible amounts of information was likely stolen. The operation of the campaign – as much as is known to the public – appears to have required substantial lead time for reconnaissance against more than one hundred victim organizations. The scale of this event, and its impact on the cybersecurity policies of a new administration, have received widespread appreciation and it is duly warranted.

But even with this large and lengthy an operation, no reports have yet surfaced that the adversary exploited a hitherto unknown vulnerability or unprecedented means of attack. Against SolarWinds, the adversary undermined trust in the software supply chain in a manner observed repeatedly over the past decade. The trend line of these attacks is one that merits attention and no small move toward action.

Software Supply Chain Attacks

Since Ada Lovelace deployed the first computer program on an early mechanical device in the 1840s, software has spread to every corner of human experience. [1] Our watches now have Internet connections, combat aircraft come with more code than computer operating systems, and every organization from the Internal Revenue Service to an Etsy storefront relies on software to serve their customers. No longer confined merely to computers, embedded software now controls the operation of complex power generators, medical hardware, the behavior of automotive brake pedals, and planetary scale datasets. As one commentator put it, "software is eating the world."[2]

With software come security flaws and a long chain of updates from vendors and maintainers. This ongoing maintenance leaves software supply chains messy and in continuous flux, resulting in significant and underappreciated aggregated risk for organizations across the world. Unlike a physical system that is little modified once it has left the factory, software is subject to continual revision through updates and patches.

A software supply chain attack occurs when an attacker accesses and modifies software in the software development supply chain to compromise a target farther down on the chain by inserting their own malicious code. Modern software products contain a vast number of dependencies on other code, so tracking down which vulnerabilities compromise which products is a nontrivial organizational and technical feat. Software supply chain attacks take advantage of established channels of trust, between the user and a vendor or developer, to compromise their targets.

In the Sunburst case, intruders were able to access SolarWinds' build infrastructure, rather than

---

[1] This section and several portions of the following testimony are drawn from "Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain", Trey Herr, June Lee, Will Loomis, and Stewart Scott - https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/

[2] Marc Andreessen, "Why Software Is Eating the World," *Wall Street Journal*, August 20, 2011, https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.

just tacking malware onto a pending update. This difference between update and build is rather like choosing where to attach a bomb to a motorcycle. In this case, instead of adding their malware alongside the software just before being sent to customers, like attaching a sidecar with a bomb inside to a motorcycle, the intruders went further and compromised the company's build infrastructure and source code. The result was like secreting a bomb into the cylinders of the motorcycle's engine before it sold—far more deeply embedded in the resulting device, and thus harder to detect or remove.

In this – SolarWinds was only the most recent in a long line of software supply chain attacks. In the last 10 years, there have been more than 140 attacks, or disclosure of vulnerabilities which could be used in such attacks, on the software supply chain.[3] Of these, *at least* 36 were attacks on software updates, including 15 targeting source code or developer's computers of which nearly half of which were attributed to state actors including many targeting administrative or security tools like the SolarWinds Orion software. These attacks on software updates are important and they emerge as a clear, and unsettlingly consistent trend, in software supply chain attacks from the last decade.

There are several other notable trends including that state actors are behind a significant number of these attacks and both mobile application and open-source software have been successfully targeted as well, at times to great effect.

States have used software supply chain attacks to deliver highly impactful software supply chain attacks, thanks in part to recurring failures by vendors to secure the code-signing process for their products. And while concerns about the real-world ramifications of attacks on firmware, IoT devices, and industrial systems are warranted, these are far from novel threats. Stuxnet and other incidents have had physical impacts as early as 2012. Several of these incidents, like NotPetya and the Equifax data breach in 2017, impacted millions of users, showcasing the immense potential scale of software supply chain attacks and their strategic utility for states.

Since 2010, there have been *at least* 30 different state backed software supply chain attacks from states including Russia, China, North Korea, and Iran as well as India, Egypt, and Vietnam.[4] Within a few months of the public discovery of the Sunburst/SolarWinds campaign, there were reports of three other state backed software supply chain campaigns targeting foreign governments for espionage, with victims located in South Korea, Vietnam, and Mongolia.[5] Each of these targeted deeply privileged programs or widely used and mandated programs—usually at the seams between organizations.

Mobile applications remain a frequent vector for software supply chain attacks, with a quarter all publicly reported incidents impacting app stores since 2010.[6] Mobile application hubs and stores are a popular means of disseminating software supply chain attacks. The stores are a common

[3] The dataset associated with this figure and following breakdown of attack types is available online for perusal or download - https://www.atlanticcouncil.org/resources/breaking-trust-the-dataset/
[4] Ibid; Herr et. al "Breaking Trust"
[5] This section and several portions of the following discussion are drawn from "Broken Trust: Lessons from Sunburst", Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Emma Schroeder, and Tianjiu Zhou - https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/
[6] Herr et. al "Breaking Trust – The Dataset"

feature of the software ecosystem and are how many users interact with the software supply chain on a regular basis. Attackers can build their own apps, designed to appear legitimate, perhaps providing wallpapers, tutorial videos, or games. For instance, in 2017, the app Lovely Wallpaper hid malware under the guise of providing phone background images. The malware would gain device permissions and charge users' accounts for "premium" services they had not signed up for. Together with fifty other apps hiding the same payload, this attack infected as many as 4.2 million devices, and successors continued to infiltrate the associated app store long after the original offenders were removed. [7]

There is also publicly available evidence that attackers compromise the software used to build mobile software, allowing them to inject malware into legitimate applications as they are created. Compromising development tools used to build apps for those stores provides tremendous scale in a software supply chain attack. One example is the XcodeGhost malware, first detected early in the fall of 2015.[8] Xcode is a development environment used exclusively to create iOS and OS X apps. A version of Xcode found on Baidu Yunpan, a Chinese file-sharing service, came embedded with malicious logic to insert a backdoor in hundreds of applications impacting hundreds of millions of users.[9]

Open-source code was not at the heart of the Sunburst crisis, but it is a critically underdefended part of the software supply chain. Open-source software constitutes core infrastructure for major technology systems and critical software. Attacks and disclosures against open-source libraries have been increasingly frequent in recent years, though whether this is due to improved visibility and reporting, or attacker preferences, deserves further study. In February 2020, two accounts uploaded more than 700 packages to the official RubyGems repository and used typosquatting, naming malware in a format very similar to a legitimate software package, to achieve more than 100,000 downloads of their malware, which redirected Bitcoin payments to attacker-controlled wallets.[10] Many of these attacks remain viable against users for weeks or months after software is patches because of the frequency with which open-source projects patch and fail to notify users. Repositories and hubs can do more to help, providing easy to use tools for developers to notify users of changes and updates and shorten the time between when a vulnerability is fixed, and users notified.

Software supply chain insecurity remains a scourge on industry and the public sector despite billions of dollars in security investment over the last decade. Protecting these supply chains demands more persistent focus on the management of risks in software deployment, not just

---

[7] Check Point, "ExpensiveWall: A Dangerous 'Packed' Malware on Google Play That Will Hit Your Wallet," *Check Point Blog*, September 14, 2017, https://blog.checkpoint.com/2017/09/14/expensivewall-dangerous-packed-malware-google-play-will-hit-wallet/.

[8] Joseph Cox, "Hack Brief: Malware Sneaks into the Chinese iOS App Store," *WIRED*, September 18, 2015, https://www.wired.com/2015/09/hack-brief-malware-sneaks-chinese-ios-app-store/.

[9] FireEye Mobile Team, "Protecting Our Customers from XcodeGhost", *FireEye Blogs*, September 22, 2015, https://www.fireeye.com/blog/executive-perspective/2015/09/protecting_our_custo.html; Claud Xiao, "Malware XcodeGhost Infects 39 iOS Apps, Including WeChat, Affecting Hundreds of Millions of Users", *Unit 42*, September 18, 2015, https://unit42.paloaltonetworks.com/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/

[10] Catalin Cimpanu, "Clipboard hijacking malware found in 725 Ruby libraries", *ZDnet,* April 17, 2020, https://www.zdnet.com/article/clipboard-hijacking-malware-found-in-725-ruby-libraries/

development. NIST can play a more important role in improving the focus, and efficacy, of this risk management through the provision of technical tools and assistance to encourage the implementation of NIST standards and guidance and by building on existing programs of work in the public and private sectors.

Better Securing the Software Supply Chain

The secure development of software is important but addressing the pace and scale of software supply chain attacks demands we pay more, if not equal attention, to how that software is *deployed* and supported. Dozens of the software supply-chain attacks discovered in the last 10 years target weakly secured code signing certificates, update servers, and other tools for software deployment. NIST can first help by assembling all security controls that impact software deployment from its universe of guidance documents in one place, leading a multi-stakeholder process to work with industry in developing a software supply chain Lifecycle Security Overlay to NIST SP 800-53.[11] The Overlay offers an existing process to collect security controls relevant to a specific topic which would be faster than a new standalone special publication and would directly support the directive to create preliminary guidelines to enhance software supply chain security required by EO 14028 section (4)(c). This effort should wrap in controls the new supply-chain family in 800-53 rev. 5 and best practices collected in the Secure Software Development Framework (SSDF) which includes industry proposals and frameworks from SAFECode, OWASP, and others.[12] This work would build on NIST's expertise and strong network and follows on previous recommendations to anchor technical security obligations in standard-setting organizations. It could also capitalize on industry and non-profit led projects like the Linux Foundation's SigStore – an effort to provide free and more robust digital infrastructure to sign code and audit those signatures.[13]

In addition to any standard documentation and report formats, this overlay, and the associated preliminary guidance from EO 14028, should also be delivered as automated software tools or appropriate source material and references for the vendors of widely used developer tools to integrate these controls and an appropriate auditing framework into their products. At present, far too many cybersecurity regulations and risk management schemes are implemented in PDF and spreadsheets rather than the tools used to build and deploy software. This creates meaningful barriers for developers to implement these controls and users to audit them. Very little is to be gained from another standards document developers have to download in pdf form and make their own determination about how to implement.

NIST will need appropriate resources and support to develop software tools, and appropriately engage with industry, to implement these standards and guidance. This is a question of budget and billets as much as investment in time; NIST can become a more effective software development enterprise including following secure deployment practices like signing and maintaining code available on their website. This automation is particularly important for more rapid and "agile" development projects where software may go through multiple versions in a single day, each requiring these controls to be implemented and checked. GitHub's use of an automated tool called Dependabot to detect and flag vulnerabilities in open-source projects as

---

[11] Herr, et al., *Breaking Trust*.
[12] NIST, *Secure Software Development Framework*, https://csrc.nist.gov/Projects/ssdf
[13] Linux Foundation, *SigStore*, https://sigstore.dev/what_is_sigstore/

developers integrate them into their code is a good example of taking a best practice and practically implementing it.[14] Automation is the only feasible path to ensure security becomes a baked in component to such a software development and deployment pipeline.

One of the most striking lessons from the Sunburst/SolarWinds campaign, echoed in EO 14028, is the importance of securing cloud computing to the discussion of software supply chains. In developing the supply chain security guidance and preliminary guidelines required by EO 14028, NIST can offer mapping of software deployment controls to popular Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) offerings from commercial vendors.[15] NIST may well require additional resources for a greater volume of work on cloud security and cloud architectures as it could substantially expand upon existing efforts.

This focus on the cloud would support implementation in the private and public sectors. The federal government has an opportunity to enforce software security policies on agencies and departments and audit implementation of these policies in real time directly through the cloud services increasingly found in the .gov and .mil. Many of these policy-enforcement mechanisms and data-collection tools are already "baked in" to cloud services; the challenge is mostly in determining how to take advantage of them 'natively' with NIST standards and guidance. Addressing secure software deployment in cloud environments would help ensure this guidance is relevant for most IT environments outside the public sector, increasing the utility of this line of effort, and would provide deeper technical support for DHS efforts to develop a secure cloud governance framework and migration reference architectures per EO 14028 (3)(c)(ii) and (iii).

The move for NIST to be more involved in developing tools to implement their own standards and guidance, including in cloud services, raises an important question of shared responsibility between NIST and operational security partners, especially DHS' Cyber and Infrastructure Security Agency (CISA). NIST is best positioned to develop these control and map how they could be implemented in different kinds of software. NIST, in partnership with CISA, could also develop use-cases of popular combinations of software where these controls might interact or overlap. But it is CISA, and other cognizant operational security agencies, who should be working to develop specific templates and configuration guides for their customer agencies. NIST is not well positioned to become expert on the unique operating conditions and constraints of every agency. In sum, NIST's role should be expert on the controls, deeply familiar with these software products, and positioned to make recommendations on how they interact with major cloud services and cloud deployment models. CISA's role is to take that guidance and tell agencies how to set their dials and knobs – making specific recommendations on configuration and enforcing broader cybersecurity policies.

---

[14] Joe Uchill, "Microsoft's GitHub adds dependency review to new code submitted from programmers", *SC Magazine*, December 9, 2020, https://www.scmagazine.com/home/security-news/microsofts-github-adds-dependency-review-to-new-code-submitted-from-programmers/; Tammy Xu, "How to Keep Software Dependencies From Becoming Your Downfall", *BuiltIn*, February 18, 2021, https://builtin.com/software-engineering-perspectives/dependabot

[15] For more on what cloud computing is and how cloud services work, see Simon Handler, Lily Liu, and Trey Herr, "Dude, Where's My Cloud? A Guide for Wonks and Users", https://www.atlanticcouncil.org/in-depth-research-reports/report/dude-wheres-my-cloud-a-guide-for-wonks-and-users/

Lastly, while the aspirations of these efforts toward more secure software supply chains are necessarily focused on achieving the best possible outcomes, we must recognize that many organizations who seek to implement this guidance may not have the resources to do so effectively. Wendy Nather, of Duo Cisco, articulated the concept of the cyber poverty line to describe the threshold between organizations of equal intent and motivation to secure themselves but diverging resources and maturity. However, many high performing controls and extensive implementation guides emerge from NIST focused on software supply chain security over the next several years – there will be a population of users and some developers who are unable to effectively implement them.

There are two things NIST can do to address this. First, embrace an emphasis on automation. As much as automating controls and guidance to integrate with standard developer tools will enhance adoption of these best practices, it can also help lower the burden of implementation. Removing the need to translate from a pdf into homemade rules for an integrated development environment (IDE) or organization policy saves time, confusion, and potential mistakes. Second, NIST can work to model the environments and constraints of moderate to low resourced IT security organizations and recommend adaptations of existing guidance to fit. The situation is similar to that found in operational technology and industrial IT environments; resources like network bandwidth and computing power are constrained necessitating changes in how users collect and process data from these systems or apply patches. Such an effort to address the cyber poverty line for supply chain security guidance (and it could be applied to all existing supply chain risk management documentation) would help widen implementation of this work across the private sector and enhance the impact of NIST's expertise and efforts.

Conclusion

Trust in software supply chain security is not built, or broken, in isolation. It would be a mistake to equate software supply chain attacks to a new weapon system in an opponent's arsenal. They are manifestation of opportunity, attacking targets by compromising weaknesses in connected neighbors, vendors, and software dependencies. For the technology industry, the insecurity of the software supply chain is a crisis in waiting. For the national security establishment, it is a crisis realized.

There are opportunities for meaningful progress and NIST can play an important role to better protect the code we have embedded in our daily lives with appropriate investment and a greater focus on automatable guidance, cloud security, and software deployment. Change on this front will demand persistence, at least as much as that of the adversary, if not a measure more.

Thank you again for the opportunity to speak with you today. I look forward to your questions.

###

Dr. Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on cybersecurity and geopolitics including cloud computing, cyber effects on the battlefield, the security of the internet, supply chain policy, and growing a more capable cybersecurity policy workforce. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

Chairman FOSTER. Thank you, and next is Ms. Moussouris.

TESTIMONY OF MS. KATIE MOUSSOURIS,
FOUNDER AND CEO, LUTA SECURITY

Ms. MOUSSOURIS. Thank you. Chairman Foster, Ranking Member Obernolte, Chairwoman Stevens, Ranking Member Waltz, and distinguished Members of the Subcommittees, thank you for inviting me to testify today about how to improve software supply chain security. My name is Katie Moussouris. I'm the Founder and CEO of Luta Security, a company that works with governments and complex organizations to create mature, robust, and sustainable vulnerability disclosure and bug bounty programs. We base these programs on the international standard ISO 29147, Vulnerability Disclosure, ISO 30111, Vulnerability Handling Processes, and our Vulnerability Coordination Maturity Model. I'm the co-author and co-editor of these international standards. With more than 20 years of professional technical and strategic experience in technology and information security as a penetration tester at @stake, followed by creating Microsoft Vulnerability research, which handled supply chain vulnerability coordination, establishing Microsoft's first bug bounties and advising the U.S. Department of Defense, resulting in the launch of Hack-the-Pentagon. Additionally, I served as co-chair of the NTIA (National Telecommunications and Information Administration) multi-stakeholder vulnerability disclosure working group subcommittee of multi-party vulnerability coordination. It is an honor to appear before these Subcommittees to testify about the challenge that securing the software supply chain presents to our economy and to our national security.

While supply chain attacks have become more prevalent in the headlines during the past few years, these types of attacks have been occurring regularly since the dawn of major operating systems, which are then used to compromise many downstream targets. This problem is not new, and believing that it is can impede meaningful conversations regarding potential solutions. One of the main reasons why these problems haven't yet been solved is that the cybersecurity industry itself is still in its infancy, while the United States and the world have grown exponentially faster in our dependence and complexity of increasingly interconnected technology. Even large organizations with many highly skilled technical workers struggle with getting the right resources in place to simultaneously respond to incidents and investigate and fix single vendor vulnerabilities, let alone supply chain vulnerabilities in both open and closed source software.

In the global cybersecurity workforce shortage, estimated at over 3.1 million unfilled positions worldwide, over half a million of those unfilled cyber roles are in the United States. The United States participates in the software supply chain in many complex roles, as do our international partners and our adversaries. There are multiple ways that supply chain attacks can occur, and not all efforts to combat these various attacks result in the same return on investment (ROI). In our ongoing national effort to build up our cyber resilience, we must evaluate the efforts put forth with desired outcomes in mind to yield measurable increased security of the supply chain now.

To address the complexity in software supply chain security, my testimony today outlines the problem space, and offers proposed solutions and actions to measurably increase the cyber-resilience of the United States and our international partners. I believe that following the recommendations, building upon some of the most important work and best practices in the public and private sector, will increase our national security. No. 1, providing CISA with the authorities and resources to oversee cyber readiness for the civilian Federal Government, and as a resource to support privately owned critical infrastructure. No. 2, amending *FISMA* to require an annual, comprehensive Federal maturity assessment and gap analysis that will identify critical gaps in people, process, and technology. No. 3, conducting a CISA-led dynamic assessment of ROI for each proposed new requirement in the cybersecurity Executive order to determine the priority of each based on the investments required to make a dent in the problem. And four, raising Federal pay scales, especially in cybersecurity, to better compete with the private sector, and investing in cybersecurity recruitment and training for existing and aspiring workers.

In the early stages of building our cyber resilience, organizations focus first on incident response, which has been echoed in the cybersecurity Executive order's breach notification requirements, as well as CISA's request for more endpoint detection budget. Investing in better breach response is important, but the ROI for investment breach prevention is higher, yet lacks the urgency to drive near term action. While new requirements like SBOMs (software bill of materials) may make supply chain vulnerabilities faster to respond to in theory, producing or consuming an SBOM would've had no effect in stopping or detecting either the SolarWinds nor the CodeCov supply chain attacks. There are no tools that can produce this enriched vulnerability data that includes vetting actual exploitability at scale, forcing continued reliance on skilled cybersecurity workers to make that final determination of imminent risk and act upon it.

In conclusion, I appreciate this Committee's and CISA's leadership on cybersecurity and supply chain issues. The Federal Government must direct what resources we have, while also growing our capacity at scale. As part of expanding CISA's role and resources, CISA should apply a system dynamics approach that models the effects of changing variables in a complex system, focused on a targeted approach to enhance security outcomes. Thank you for this opportunity to testify before the Committee today on this critical issue. I look forward to answering any questions you may have for me.

[The prepared statement of Ms. Moussouris follows:]

Testimony of Katie Moussouris

Before the Committee on Science, Space, & Technology

Subcommittee on Investigations and Oversight & Subcommittee on Research and Technology

U.S. House of Representatives

On SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains

May 25, 2021

Washington, DC

Introduction

Chairman Foster, Ranking Member Obernolte, Chairwoman Stevens, Ranking Member Waltz, and distinguished members of the Subcommittees, thank you for inviting me to testify today about how to improve software supply chain security. My name is Katie Moussouris, I am the founder and CEO of Luta Security, a security company that works with governments and complex organizations to transform the way these organizations use people, processes, and technology to create mature, robust, and sustainable vulnerability disclosure and bug bounty programs. We base these programs on the industry international standards ISO/IEC 29147 Vulnerability disclosure[1], ISO/IEC 30111 Vulnerability handling processes[2], and our Vulnerability Coordination Maturity Model[3].

I am the co-author and co-editor of these international standards. I have more than 20 years of professional technical and strategic work in technology and information security, beginning as a penetration tester at @stake[4], followed by creating Microsoft Vulnerability Research, establishing Microsoft's first bug bounties, and advising the U.S. Department of Defense for several years, resulting in the launch of the Hack-the-Pentagon program. Additionally, I served as co-chair of the National Telecommunications and Information Administration's multi-stakeholder vulnerability disclosure working group subcommittee of multi-party vulnerability coordination[5]. I also served as one of two private industry official delegates of the U.S. technical experts working group to renegotiate the "intrusion software & intrusion software technology" provisions of the Wassenaar Arrangement[6], successfully helping clarify exemptions for vulnerability disclosure and incident response in export controls.[7] I am a cybersecurity fellow at New America and the National Security Institute, and I am also the founder of the Pay Equity Now Foundation[8].

1 https://www.iso.org/standard/72311.html

2 https://www.iso.org/standard/69725.html

3 https://www.lutasecurity.com/vcmm

4 https://en.wikipedia.org/wiki/@stake

5 https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-draft.pdf

6 https://langevin.house.gov/press-release/langevin-statement-wassenaar-arrangement-plenary-session

7 https://thehill.com/opinion/cybersecurity/365352-serious-progress-made-on-the-wassenaar-arrangement-for-global

8 https://www.payequitynowfoundation.org/

It is an honor to appear before these Subcommittees to testify about the challenges securing the software supply chain presents to our economy and our national security. While supply chain attacks have become more prevalent in the headlines during the past few years, these types of attacks have been occurring regularly since the dawn of major operating systems. Since the operating system (OS) sits fairly high upstream of most other technology, it has long been an effective target that is attacked, then used to compromise many downstream targets. This problem is not new and believing that it is can impede meaningful conversations regarding potential solutions.

The United States participates in the software supply chain in multiple complex roles, as do our international partners, and our adversaries. Taking on the challenge of securing the supply chain is not as simple as rolling out Executive Orders or even legislation but requires a nuanced approach that maximizes the investments in resources and capabilities we have, while measuring effectiveness and maturity, building new tools to scale solutions, and recruiting new talent to fill growing cyber security operational and strategic roles.

The COVID-19 pandemic and the move to remote work nearly overnight around the world drove more organizations to use technology to keep business operations going, often without increasing their cyber security budgets or personnel as they struggled with the economic downturn most businesses faced. Unfilled security jobs worldwide are over 3.1 million, with over half a million of those open roles in the United States[9]. This cyber workforce shortage has a compound effect when software supply chains are by definition interconnected, and only as strong as the weakest link upstream.

Our success in the desired outcome of improved cyber security, and greater cyber resilience, relies on our adaptability to threats and shifting tactics. Without a detailed understanding of our current capabilities, even our best intentions and efforts for following "best practices" and building new, world-leading capabilities will fall short of our adversaries' efforts more often than not. In the past year, "there was a 430% increase in upstream software supply chain attacks over the past year.[10]"

To address the complexity in software supply chain security, my testimony today will outline the problem space and offer proposed solutions and actions to measurably increase the cyber resilience of the United States and our international partners. I believe the following recommendations, building upon some of the most important work and best practices in the public and private sector, will increase our national security.

9 https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

10 https://www.sonatype.com/hubfs/Corporate/Software%20Supply%20Chain/2020/SON_SSSC-Report-2020_final_aug11.pdf

1. Providing the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. Department of Homeland Security with the authorities and resources to oversee cyber readiness for the civilian federal government, and as a resource for promoting best practices and cyber security incident response consultative support for privately-owned critical infrastructure;
2. Amending FISMA to require an annual, comprehensive federal civilian agency gap analysis and maturity assessment that will identify critical gaps in people, process, and technology and also support maturity-based metrics, which will measure improvements in cyber security and cyber resilience;
3. Conducting a CISA-led survey of ROI for each proposed new requirement in the Cybersecurity Executive Order[11] to determine the priority of each based on the investments required to make a dent in the problem through a system dynamics analysis; and
4. Raising federal pay scales across the board in all roles, especially in cyber security, to better compete with the private sector, and investing in cyber security recruitment and training for existing and aspiring workers who require additional skills to support the cyber mission.

The United States government is not alone in having to reckon with the vast technical debt built up in the global supply chain. If we are to improve our cyber resilience and reduce our risk profile, we have to focus the hard work and investments in effective inflection points across the ecosystem, especially in the context of supply chain security.

Understanding trends in supply chain attacks including SolarWinds

There are multiple ways that supply chain attacks can occur, and not all efforts to combat these various attacks result in the same return on investment. In our ongoing national effort to build up our cyber resilience, we must evaluate the efforts put forth with desired outcomes in mind, to avoid overinvesting at this critical time in complex good ideas that might yield dividends down the line, versus doing the simplest measures that yield measurable increased security of the supply chain now.

While SolarWinds focused security efforts on compliance, their software build process was compromised resulting in the widespread attacks of their customers. SolarWinds had weak passwords found that were set by interns that were part of a larger organizational control failure that on the whole contributed to their overall missed security steps that allowed the supply chain attack to be planted, once the adversary gained access to their build pipeline. Weak passwords weren't the definitive smoking gun of how the attackers got in, but with low hanging fruit footholds like weak passwords allowed, and not enough internal segmentation, or integrity checks in the build process, the systems ended up silently compromised for months.

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

The CodeCov[12] supply chain attack was similar, though so far it has garnered less attention in mainstream media. The attackers modified a CodeCov bash uploader to redirect credentials and other sensitive information, harvesting those downstream user's credentials and access tokens to further infiltrate the build processes of the downstream developers. It was insidious and the ramifications downstream are still not fully determined.

Smaller, ongoing supply chain attacks are usually overlooked until larger-scale attacks occur like the ones against CCleaner[13], and most recently, SolarWinds and CodeCov. Like most security problems, many experienced professionals seeing different angles of the problem envision different solutions for securing the software supply chain. One of the main reasons why these problems haven't yet been solved is that the cybersecurity industry itself is still in its infancy, while the United States and the world have grown exponentially faster in our dependence and complexity of increasingly interconnected technology.

During my 20 plus years as a cybersecurity professional, all the way back to my earliest modem-connectivity to the young Internet in the early 1990s, I have watched the scale of Internet defense grow at a slower pace than the emerging threats. Industry leading software manufacturing security best practices emerged by necessity, a wave of Internet worms regularly crippling early infrastructure, spawning the software giants to invest in their security response at first, followed by enhanced attack detection, and finally in incident prevention and resilience as they matured. This cybersecurity maturity has not had time to propagate to all software manufacturers, nor has it even taken root at some of the largest software builders, and it has no scalable support at some of the most heavily used open-source software deployed in systems worldwide.

As we have seen in the early software manufacturers who have matured in their software security capabilities, the downstream supply chain and the consumers of it, including the Federal government, must mature as well. In early stages of building our cyber resilience, we see organizations focus first on incident response, which has been echoed in the Cybersecurity Executive Order's breach notification requirements, as well as CISA's requests for more endpoint detection budget during recent Congressional hearings. Investing in better breach response is important, but the ROI for investment in breach prevention is higher yet lacks the urgency to drive near-term action.

One such maturation from pure security response into a broader supply chain vulnerability coordination focus was designed and implemented by me at Microsoft starting in 2008, when I created Microsoft Vulnerability Research (MSVR)[14] to look for vulnerabilities downstream in Microsoft's third-party software ecosystem and coordinate multi-party and supply chain issues in both hardware and software. Setting up this new multi-party and supply chain security capability was non-trivial, even for the largest software company in the world, investing in nearly half a billion dollars annually at the time in people, process, and technology that made up the organization formerly known as Trustworthy Computing.

---

12 https://blog.sonatype.com/what-you-need-to-know-about-the-codecov-incident-a-supply-chain-attack-gone-undetected-for-2-months

13 https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

14 https://www.microsoft.com/en-us/msrc/msvr

One of the first issues coordinated via MSVR was Dan Kaminsky's DNS vulnerability[15], which would have crippled the Internet. Another was a Microsoft Active Template Library (ATL) issue that affected all software compiled using that library downstream in the supply chain that also had to be coordinated in stages to enable protections to be rolled out to the most affected users at once. Yet another was a baseband chip family of issues that had to expand the coordination effort to most baseband chip manufacturers and standards bodies setting technical specifications.

One begins to appreciate the scale of the problem when even the largest organizations have only been tackling the issue of supply chain security head on for about a dozen years. While federal mandates can act as catalysts for positive change, unfunded mandates are less successful, and in this case, even well-funded new requirements will struggle to find skilled cyber workers to meet current and emerging needs.

Challenges to both the private and public sector in responding to supply chain attacks

We are, as a society, in a state of having built up interconnected cyber cities without enough cyber fire fighters, hydrants, or fire inspectors to ensure what we build next is safe. The infrastructure fragility caused by this chronic underinvestment in cyber security across both the federal and private sectors is at a crescendo now, not because supply chain attacks are new, but because they are increasing in frequency in parallel to the Internet resources upon which we increasingly depend.

Our federal and private sector capacity for responding to supply chain attacks and remediating underlying vulnerabilities is limited by gaps in people, process, and technology that change over time as new tools and processes are developed in the marketplace, and new workers are trained and gain experiences.

Cyber workforce challenges in both public and private sector

In an industry as young as cybersecurity, we do not have a good conduit for building a continuous pipeline of cybersecurity workers skilled at various levels to form a steady pipeline. The majority of security jobs are not entry level. Without providing entry-level jobs, mentoring programs, or training programs, we will never be able to effectively staff teams to prevent, detect, and remediate cyber attacks. The much-sought-after elite cyber workers that extremely well-funded organizations are seeking are cost-prohibitive for smaller private critical infrastructure organizations, as well as for federal, state, and local governments.

Even large organizations with many highly skilled technical workers struggle with getting the right resources in place to simultaneously respond to incidents and investigate and fix vulnerabilities. Security is not taught at most universities, and more successful coders come from diverse and informal backgrounds, compounding the issues of securing code, even if vulnerabilities are pointed out by skilled outsiders. The internal digestive system for vulnerabilities, as well as the muscle memory of an organization to handle its supply chain both upstream and downstream must be built over time.

---

15 https://channel9.msdn.com/Events/Blue-Hat-Security-Briefings/BlueHat-Security-Briefings-Fall-2008-Sessions-and-Interviews/v8--4

For example, while running two private bug bounty programs using outsourced support from both major bug bounty platform providers, Luta Security was called in to assist Zoom in the surge of new vulnerability report cases that came in when the pandemic created an exponential surge in popularity. Knowing about bugs is less than half the battle. We helped flatten the curve of Zoom's bug cases by 37 percent in less than 10 weeks, targeting and eliminating imminent zero-day risks for those cases. We also provided a vulnerability handling maturity gap analysis and roadmap for Zoom to use moving forward, as the company works toward achieving ISO 29147 and ISO 30111 compliance.[16]

To fill the gaps in the cyber workforce in the federal government, one issue to address is pay scale differences between the private and public sector, and another is to train new and existing federal workers. Raising federal pay scales across the board and especially in cyber security will allow for building out the more senior ranks of experts needed to protect national security. Investing in hiring for aptitude and training in key new technologies will address unfilled security roles over time as the hiring and training pipeline matures. This deliberate investment in the American workforce will also provide a vital conduit for providing economy-stimulating new skilled job opportunities for U.S. workers.

Government actions that could help address these challenges

There are several actions the federal government can take to begin addressing these challenges.

As we all know, NIST[17] does a great job with FIPS and special publications to provide smart guidance on security and other information-handling processes. The EO requires NIST to work to determine the implementation of many directives in collaboration with other agencies such as the Commerce Department. The process to gather relevant input to the proposed rules is on an aggressive time scale, which makes sense due to the urgency of the threats but can lead to implementations with unintended consequences. NIST can help by ensuring concerns with various proposed measures have been investigated in terms of expected impact in exchange for the effort.

In the recent SolarWinds attack, "SolarWinds saw signs of hackers invading their networks as early as January of 2019, about eight months earlier than the previously publicly disclosed timeline for the sweeping cyber-espionage campaign, and nearly two years before anyone discovered the breach.[18]" The United States must not only focus on breach response due to supply chain or other attacks, but also invest in identifying security vulnerabilities and coordinate fixes across the supply chain ideally before they are exploited. If we invest in response, detection, prevention, we will not be forced to be reactive only.

Many roles are needed at various technical skill levels to ensure comprehensive coverage of necessary security functions. Most of the requests for additional budget for cybersecurity focus on breach detection and incident response, rather than prevention activities and proactive vulnerability remediation via VDPs. While an "assume breach" security posture is recommended, focusing mostly on the post-breach actions leaves under investments in greater ROI preventative security activities.

16 https://www.lutasecurity.com/post/luta-security-highlights-for-zoom-bug-bounty-programs

17 https://www.nist.gov/

18 https://www.cyberscoop.com/SolarWinds-ceo-reveals-much-earlier-hack-timeline-regrets-company-blaming-intern/

Efforts supporting detection and response to breaches and vulnerabilities are shared resources inside an organization that are currently overstretched and covering numerous government directives at once.

These resources are overstretched even further due to the requirement for all civilian agencies to launch a Vulnerability Disclosure Program (VDP) to comply with CISA's Binding Operational Directive (BOD) 20-01[19]. The same internal personnel resources for VDPs are often needed to investigate and respond to these ongoing attacks. The federal government could address this overbooking of essential internal security personnel by investing in tools to identify vulnerabilities more frequently themselves, and enough skilled personnel to comprehensively investigate and fix incoming vulnerability reports.

Another important action this Committee and Congress could do is measure the maturity of the vulnerability response efforts of the federal agencies and their contractors now, and on at least an annual basis. Performing a comprehensive federal civilian agency gap analysis and maturity assessment will identify critical gaps in people, process, and technology and also support maturity-based metrics, which will measure improvements in cyber security and cyber resilience. These maturity measures could conceivably be part of the annual Federal Information Security Modernization Act[20] (FISMA) assessments. Since the cybersecurity maturity of any given organization changes over time with increased or decreased investments in tools, automation, and skilled key team members addressing an evolving threat landscape, performing maturity assessments should become part of the fabric of our cyber resilience strategy to deal with individual and supply chain vulnerabilities consistent with ISO standards.

The federal government must direct what resources we have while also growing our capacity at scale. As part of expanding CISA's role and resources, CISA should apply a system dynamics approach that models the effects of changing variables in a complex system, focusing on a targeted approach to enhance security outcomes. Some of these variables include the cybersecurity maturity of different links in the supply chain, the current availability of tools to assist in scaling efforts, and the readiness of a trained workforce able to meet different technical requirements as threats change. What we choose to invest in will change these variables in people, process, and technology, that in turn change the calculus for the entire system. Tools can close some gaps, as long as there are skilled operational workers to run them, and analysts are trained to interpret the results and act upon them strategically.

Since pushing on one lever in the system changes the calculus and behavior of the interconnected parts of the system, we can use a system dynamics approach to help inform ROI analysis over time. This will help the United States anticipate the changing needs in people, process, and technology to meet threats today and tomorrow, rather than the cycle of applying one-size-fits-all measures and chasing the threats of yesterday.

19 https://cyber.dhs.gov/bod/20-01/#fn:18

20 https://www.cisa.gov/federal-information-security-modernization-act

Strengths and limitations of federal actions protecting against and responding to supply chain attacks

The recent cybersecurity Executive Order provides requirements to address multiple cybersecurity problems at once, a bold and necessary step to catch up in our paying down of technical debt that has amassed like unread messages in the security inbox of the Internet. There are a few concerns and limitations to the proposed measures, and areas of concern where the devil lies in the details of implementation. Some recommendations in the EO may inadvertently introduce new risks by concentrating sensitive information into an attractive new aggregated target for adversaries if not properly managed.

Additionally, BOD 20-01 provides a welcome and much-needed forcing function to get federal agencies to respond to security vulnerability reports from the public, but resources and expertise to support those programs are often overstretched internally to handle breach investigations as well as first party and supply chain vulnerabilities and attacks.

Finally, there are important initiatives that over time will no doubt enhance the speed of responding to supply chain vulnerabilities and compromises, like the Software Bill of Materials (SBOM), but lack definition and implementation studies at this time. This makes them a premature requirement for the near term, possibly distracting from other efforts that could be implemented yielding a better security ROI in exchange for the effort.

A summary of challenging areas include the Cybersecurity Executive Order and BOD 20-01:

- Executive Order:
  - Centralized breach reporting for incidents under active investigation in progress will create an attractive target for adversaries wanting to know the state of their intrusion campaign efforts as investigations unfold. Determining who gets access to this information will be essential, unless the EO is amended to allow for after-action reporting once remediation and recovery actions are already taken.
  - Mandatory breach disclosure of three days for the most serious incidents might not be possible at that stage in the investigation, because they may not know yet they have a serious breach. Providing an exemption for later discoveries as the investigation unfolds may inadvertently reward organizations with slower investigative processes, while punishing organizations with faster and more sophisticated breach detection and investigation capabilities;
  - The SBOM requirement has yet to be defined and adopted even in some of the largest organizations, and like rolling out Multifactor Authentication (MFA) across the federal government and its suppliers, it will be a huge, industry-wide undertaking. Unlike the ambitious timelines for MFA adoption, SBOM does not have a well-understood model for the people, process, and technology needed for a successful rollout. CISA and NTIA should perform studies to measure the beneficial security outcomes that producing and consuming SBOMs require.

- BOD 20-01:
  - Impacts federal agencies level of preparedness - Since the SolarWinds and Microsoft Exchange investigations have the federal government scrambling to deal with its aftermath, it is unclear what steps, if any, federal agencies have taken to systematically assess their ability to carry out their cyber investigation and response duties on multiple fronts at once.
  - Same personnel, multiple functions - That could easily sow greater confusion, distracting key internal cyber incident first responders and creating patching backlogs that could be exploited by the very adversaries that launched SolarWinds and the Microsoft Exchange attacks.
  - Delayed metrics, increased risk - Leaving assessment of the gaps in people, process, and tools assessment until the metrics reporting deadline as stipulated in the BOD will leave critical areas understaffed and outgunned while our adversaries continue to operate undetected for months if not longer. The required metrics in the BOD do not include cybersecurity workforce statistics. These delayed and missing metrics increase the risk to national security.

As mentioned above, SBOM is a worthy initiative that will ideally improve supply chain remediation and response. At the same time, the inclusion of SBOM in the EO now is of concern due to many unanswered questions not yet resolved in a scalable way. The concept certainly bears merit in a commonsense way - knowing what other software is included in a product can speed the response in a supply chain vulnerability or incident response scenario. However, producing or consuming an SBOM would have no effect in stopping or detecting either the SolarWinds nor the CodeCov supply chain attacks. The public comment period for defining the minimum SBOM requirements will leave even more questions about the level of effort required for each organization attempting to comply with that section of the EO, depending on the depth of information that is determined to comprise the minimum SBOM.

An ingredient list of software alone is not useful to determine risk quickly without additional analysis. Neither is the addition of vulnerability data, which would at a minimum include what known vulnerabilities affected each software ingredient. This is because from a technical standpoint, a bug in a software ingredient may not be exploitable in all products that contain that software ingredient. Exploitability would be determined in what code paths are taken via the product, and what other countermeasures may be in place in the overall product that obviate or mitigate the underlying software supply chain vulnerability.

There are no tools that can produce this enriched vulnerability data that includes vetting actual exploitability at scale. This ends up in the same resource crunch situation relying on skilled cybersecurity workers to make that final determination of risk and act upon it.

"Although mounting security problems in healthcare and their root causes have clarified that SBOMs might solve several problems, implementation has been slow and there are few data available from the published peer-reviewed literature. Complicating this issue is a lack of out-of-the-box solutions and industry-wide standards, such that organizations have developed homegrown proprietary solutions to improve interoperability and security of their systems. As one example, the Mayo Clinic now requires prospective vendors of medical devices to submit a complete description of all components of their products, including software architecture, as part of its procurement process. This is a rare instance of such information being publicly available for a healthcare entity, however.[21]"

The SBOM working group has not addressed these open questions or developed consensus around standard minimum information. Further, the group has had mostly industry participants with huge existing investments in internal specialized security teams - the security and incident responder 1 percent. We have no broad field data on how less mature organizations will fare in this new requirement versus investing in other fundamental security efforts.

With significant effort and investment across the ecosystem, an SBOM will help speed up supply chain security response. Given the current state of maturity of both the SBOM project and the United States' cybersecurity capabilities, timely and actionable information to address supply chain risks using SBOMs would be a costly and enormous effort. An SBOM requiring too little information at a minimum would force additional skilled security analysis in order to determine risk. With limited cybersecurity workers, performing this data enrichment step could displace vital security work that might have a greater ROI towards the desired secure supply chain outcomes. More real-world data is needed to determine the people and skill requirements to facilitate SBOM production and consumption. With this additional study, I believe SBOM will become an invaluable part of managing software and hardware supply chain security.

Conclusion

I appreciate this Committee's and CISA's leadership on cybersecurity and supply chain issues. The urgency of action must be balanced with an analysis of the right action at the right time. I believe that the system dynamics approach to assessing relative ROI of various efforts to improve supply chain security is the "work smarter" approach to paying down our accumulated technical debt that contributes to our national security.

In the private sector, among those defending against becoming the vector for the next supply chain attack, investment in internal resource segmentation, access controls, and build integrity processes would have helped prevent or detect SolarWinds and CodeCov at the source of the compromises. Those efforts have industry-proven risk reduction, whereas forward-thinking measures like SBOM hold great promise, but are not yet proven in reducing supply chain attacks.

21 https://www.nature.com/articles/s41746-021-00403-w

What we really need to pay down the technical debt in securing the software supply chain is an understanding of our gaps in people, process, technology to effectively enhance our software supply chain to be resilient and secure. By amending FISMA to measure our maturity and capabilities, now and on an annual basis, we can more efficiently allocate resources, investments, and improve agencies' preparedness for attacks.

We can take on bold new initiatives, such as those outlined in the EO and other regulations, to start making significant improvements in supply chain security and our national cyber resilience. Our success in these security programs depends on our focus on high ROI activities.

Overlapping internal security roles are currently overstretched in both the federal government and contractors, in keeping with the entire industry's cyber workforce shortage. Supporting multiple new and existing security initiatives will require new recruitment, training, and funding for additional personnel and tools to meet current and future supply chain threats.

Thank you for this opportunity to testify before the Committee today on this critical issue.

I look forward to answering any questions you may have for me.

Katie Moussouris
Founder & CEO, Luta Security

As a computer hacker with more than 20 years of professional cybersecurity experience, Katie has a unique and unparalleled perspective on security research, vulnerability disclosure, and bug bounties. Currently, Katie serves as the founder and CEO of Luta Security. She is also an advisor for several governments and large organizations around the world.

During her tenure with Microsoft, her work included industry-leading initiatives such as Microsoft Vulnerability Research and the company's first bug bounty program. Katie is also the co-author and co-editor of ISO 29147 (vulnerability disclosure) and ISO 30111 (vulnerability handling processes). Working with the Department of Defense, Katie led the launch of the U.S. government's first bug bounty program, "Hack the Pentagon." She also worked with the State Department to help renegotiate the Wassenaar Arrangement, specifically changing the export control language to include technical exemptions for vulnerability disclosure and incident response.

Katie is a cybersecurity fellow at New America and the National Security Institute. She is also the founder of the Pay Equity Now (PEN) Foundation, and through the PEN Foundation, Katie established the Anuncia Donecia Songsong Manglona Lab for Gender and Economic Equity at Penn State Law in University Park. Additionally, she served as a visiting scholar with the MIT Sloan School, a Harvard Belfer affiliate, and an advisor to the Center for Democracy and Technology. In 2018, Katie was featured in two Forbes lists: The World's Top 50 Women in Tech and America's Top 50 Women in Tech.

Chairman FOSTER. Thank you. And next is Mr. D'Souza.

TESTIMONY OF MR. VIJAY D'SOUZA, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

Mr. D'SOUZA. Hello, Chairs Foster and Stevens, Ranking Members Obernolte and Waltz, and Members of the Subcommittees. Thank you for inviting me to testify at today's hearing on SolarWinds and IT supply chain issues. My testimony is based on GAO's ongoing look at the SolarWinds cybersecurity incident, and GAO's December 2020 report on IT supply chain risk management at Federal agencies.

The SolarWinds cybersecurity incident was arguably one of the most severe and sophisticated cyberattacks on the Federal Government, but much remains unknown publicly about the full impact. The attackers, now known to be affiliated with the Russian Foreign Intelligence Service, were able to take advantage of weaknesses in the SolarWinds company security practices to insert malicious content in updates that SolarWinds supplied to its customers, including Federal agencies. Thus, the attackers were able to take advantage of what we generally consider good cybersecurity practice, patching and updating your software regularly.

The government has taken a number of steps in response to SolarWinds. Beginning in December 2020, DHS and CISA issued an emergency directive, and later several additional tools and pieces of guidance on how Federal agencies and other organizations should respond to the attack. The most recent guidance was actually just issued a few days ago, and more remains to be done. A unified coordination group including CISA, the FBI (Federal Bureau of Investigation), NSA (National Security Agency), and ODNI (Office of the Director of National Intelligence) was also created to coordinate the government's intelligence gathering and response activities. This group was recently disbanded, and has shifted its focus to identifying lessons learned from the incident. GAO currently has work underway compiling what is known about the impact of SolarWinds on the Federal Government, and what lessons have been learned. We recently issued a blog post on this issue, and plan to issue a public report later this year.

Although SolarWinds was both an unpleasant and unprecedented discovery, unfortunately, we can't be surprised that something like this occurred. In December 2020, just as the attack was announced by CISA, GAO released a public version of our report looking at how well Federal agencies were keeping an eye on their IT supply chains. The bottom line, most agencies were not following even foundational practices in this area. We identified seven practices that should be followed agency wide. These include establishing executive oversight, developing a strategy, and developing a way to document and identify risks. For the 23 agencies we examined, none had implemented all the practices, and 14 hadn't implemented any of the practices. Given what we now know about the threats we face, this is concerning.

Agencies told us they hadn't implemented many of these practices because they were awaiting additional guidance, most specifically from the Federal Acquisition Security Council, or FASC. And

it's true today that FASC hasn't issued detailed guidance that agencies may need to fully implement a supply chain risk management program, but it's important to not let the perfect be the enemy of the good in this case. NIST has had guidance in this area since 2015, and OMB has directed agencies to begin thinking about this issue since at least 2016. The foundational practices we focused on include basic issues, such as identifying who is in charge in establishing an overall strategy and process. While, as with all issues technology related, how you do this will change over time, SolarWinds demonstrates that it's important to get started on supply chain security right away.

To be fair, it's important to note that there are a lot of Federal activities underway looking at IT supply chain security. NIST is currently revising its existing guidance, and hopes to reissue it in 2022 to incorporate best practices from Federal and private organizations, and to integrate with other NIST guidance. In addition, CISA has a task force underway that is trying to address some of the underlying issues in this area. For example, how do we encourage private companies to share information, and how do we certify and vet Federal suppliers? We issued a more detailed sensitive report in October of last year that our December report was based on. In the October report we made 145 recommendations to specific agencies to implement the foundational practices that I discussed. We have received updates from six agencies on their progress, but to date none of the agencies have fully implemented our recommendations.

It's not going to be easy to address IT supply chain issues, and what we do is going to change as we continue to learn more about the threats in this area, but if we want to be prepared for the next SolarWinds type incident, it's important for Federal agencies to immediately begin addressing this issue, and for Congress to continue its oversight through activities such as today's hearing. This concludes my statement. I'm happy to answer any questions you may have.

[The prepared statement of Mr. D'Souza follows:]

United States Government Accountability Office
Testimony
Before the Subcommittees on Investigations and Oversight and Research and Technology, Committee on Science, Space and Technology, House of Representatives

For Release on Delivery
Expected at 2:00 p.m ET,
Tuesday, May 25, 2021

CYBERSECURITY

Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks

Statement of Vijay A. D'Souza, Director,
Information Technology and Cybersecurity

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-594T

GAO@100 Highlights

Highlights of GAO-21-594T, a testimony before the Subcommittees on Investigations and Oversight and Research and Technology, Committee on Science, Space and Technology, House of Representatives

Why GAO Did This Study

Federal agencies rely extensively on ICT products and services (e.g., computing systems, software, and networks) to carry out their operations. However, agencies face numerous ICT supply chain risks, including threats posed by malicious actors who may exploit vulnerabilities in the supply chain and, thus, compromise the confidentiality, integrity, or availability of an organization's systems and the information they contain. Recent events involving a software supply chain compromise of SolarWinds Orion, a network management software suite, and the shutdown of a major U.S. fuel pipeline due to a cyberattack highlight the significance of these threats.

GAO was asked to testify on federal agencies' efforts to manage ICT supply chain risks. Specifically, GAO (1) describes the federal government's actions in response to the compromise of SolarWinds and (2) summarizes its prior report on the extent to which federal agencies implemented foundational ICT supply chain risk management practices. To do so, GAO reviewed its previously published reports and related information. GAO has ongoing work examining federal agencies' responses to SolarWinds and plans to issue a report on this in Fall 2021.

What GAO Recommends

In a sensitive version of its December 2020 report, GAO made 145 recommendations to 23 federal agencies to fully implement selected foundational practices in their organization-wide approaches to ICT SCRM.

View GAO-21-594T. For more information, contact Vijay D'Souza (202) 512-6240 or dsouzav@gao.gov.

May 25, 2021

CYBERSECURITY

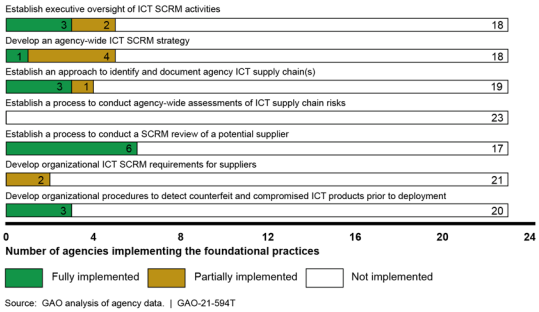
Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks

What GAO Found

Federal agencies continue to face software supply chain threats. In December 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued an emergency directive requiring agencies to take action regarding a threat actor that had been observed leveraging a software supply chain compromise of a widely used enterprise network management software suite—SolarWinds Orion. Subsequently, the National Security Council staff formed a Cyber Unified Coordination Group to coordinate the government response to the cyberattack. The Group took a number of steps, including gathering intelligence and developing tools and guidance, to help organizations identify and remove the threat.

During the same month that the SolarWinds compromise was discovered, GAO reported that none of 23 civilian agencies had fully implemented selected foundational practices for managing information and communication technology (ICT) supply chain risks—known as supply chain risk management (SCRM) (see figure).

Twenty-three Civilian Agencies' Implementation of Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) Practices



Source: GAO analysis of agency data. | GAO-21-594T

GAO stressed that, as a result of not fully implementing the foundational practices, the agencies were at a greater risk that malicious actors could exploit vulnerabilities in the ICT supply chain, causing disruptions to mission operations, harm to individuals, or theft of intellectual property. Accordingly, GAO recommended that each of the 23 agencies fully implement these foundational practices. In May 2021, GAO received updates from six of the 23 agencies regarding actions taken or planned to address its recommendations. However, none of the agencies had fully implemented the recommendations. Until they do so, agencies will be limited in their ability to effectively address supply chain risks across their organizations.

Chairs Foster and Stevens, Ranking Members Obernolte and Waltz, and Members of the Subcommittees:

I am pleased to participate in today's hearing on the federal government's information and communications technology (ICT) supply chain risk management (SCRM) and recent cybersecurity incidents. The risks to information technology (IT) systems supporting the federal government and the nation's critical infrastructure are increasing, including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks.

We have designated information security as a government-wide high-risk area since 1997.[1] We expanded this high-risk area in 2003 to include the protection of critical cyber infrastructure. In September 2018, we reported that the federal government needed to take 10 specific actions to address the four major cybersecurity challenges that the federal government and other entities face: (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.[2] Since September 2018, we and others have made numerous recommendations to federal agencies and the Congress related to the 10 specific actions—including mitigating global supply chain risks—needed to address the four major cybersecurity challenges.

Federal agencies rely extensively on ICT products and services (e.g., computing systems, software, and networks) to carry out their operations. However, agencies face numerous ICT supply chain risks, including threats posed by malicious actors who may exploit vulnerabilities in the

[1]See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 2, 2021) and *High Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 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.

[2]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

supply chain and, thus, compromise the confidentiality, integrity, or availability of an organization's systems and the information they contain.

In September 2019, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) reported that federal agencies then faced approximately 180 different ICT supply chain-related threats. Recent events involving a software supply chain compromise of SolarWinds Orion, a network management software suite, and the shutdown of a major U.S. fuel pipeline due to a cyberattack highlight the persistence and significance of these threats.[3]

To address threats such as these, it is essential that agencies apply SCRM—that is, the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT products and service supply chains. Doing so is vital to agencies being effectively positioned to make risk-based decisions about how best to secure their systems.

In response to your request, my testimony today (1) describes the federal government's actions in response to the compromise of SolarWinds and (2) summarizes our prior report on the extent to which federal agencies have implemented foundational ICT SCRM practices. To prepare this statement, we reviewed our previously issued reports on major cybersecurity challenges and federal agencies' efforts to manage supply chain risks, as well as other information we have published that explains the compromise of SolarWinds and describes the federal government's efforts to coordinate and respond to the incident.[4] In addition, this statement includes updates on progress that agencies have made in implementing the recommendations made in our December 2020 supply chain report. Detailed information on the objectives, scope, and methodology of our work contributing to this statement can be found in the issued reports.

[3]GAO, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, (Washington, D.C.: Apr. 22, 2021) and *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic),* (Washington, D.C.: May 18, 2021).

[4]GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-164SU (Washington, D.C.: Oct. 27, 2020); GAO-21-171; *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) and *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, (Washington, D.C.: Apr. 22, 2021).

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The exploitation of ICT products and services through the supply chain is an emerging threat. ICT supply chain-related threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services. Moreover, these threats can appear at each phase of the system development life cycle, when an agency initiates, develops, implements, maintains, and disposes of an information system. As a result, the compromise of an agency's ICT supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.

According to the Office of the Director of National Intelligence (ODNI), numerous supply chain attacks have occurred over the last several years. In response to one such recent attack, CISA issued an emergency directive and alert in December 2020 related to a cyberattack campaign that exploited software supply chain weaknesses in the SolarWinds Orion network management software.[5] Specifically, an advanced persistent threat actor used weaknesses in the software's supply chain to conduct a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations.

To carry out the attack, the threat actor inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a version of that software product. According to CISA, 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. SolarWinds estimated that nearly 18,000 of its customers received a compromised software update. CISA further explained that the advanced

[5]CISA, *Mitigate SolarWinds Orion Code Compromise*, Emergency Directive 21-01 (Dec. 13, 2020); and *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, Alert AA20-352A (Dec. 17, 2020).

persistent threat actor had demonstrated complex intrusion techniques and that removing this threat actor from compromised IT networks would be highly complex and challenging.

Over the past several years, Congress and federal agencies have taken a number of steps aimed at mitigating ICT supply chain risks. For example:

- In December 2018, the Federal Acquisition Supply Chain Security Act of 2018 established the Federal Acquisition Security Council (FASC).[6] The FASC is a cross-agency council responsible for providing direction and guidance to executive agencies to reduce their ICT supply chain risks. According to officials in the Office of Management and Budget's (OMB) Office of the Chief Information Officer, the council finalized a strategic plan in June 2020 for addressing supply chain risks that is intended to, among other things, establish requirements for sharing relevant information about supply chain risks with all federal agencies.
- The Department of Homeland Security, through CISA, established the ICT SCRM Task Force in December 2018 as a public-private partnership to identify and develop strategies to enhance global ICT supply chain security. The task force has been extended until July 2021 to allow it to, among other things, collaborate on other ongoing public-private engagement efforts around supply chain, and support the FASC.
- The John S. McCain National Defense Authorization Act for Fiscal Year 2019 included a provision that prohibits executive branch agencies from, among other things, obtaining telecommunications equipment—or contracting with entities that use equipment—produced by Huawei Technologies Company, ZTE Corporation, or

[6]Federal Acquisition Supply Chain Security Act of 2018—Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act), Pub. L. No. 115-390, Title II, § 202(a), 132 Stat. 5173, 5178 (2018) (codified at 41 U.S.C. § 1322). The law also establishes requirements specifically for the heads of executive agencies. 41 U.S.C. § 1326.

any of their subsidiaries or affiliates.[7] In May 2019, the Department of Commerce (Commerce) added Huawei and certain non-U.S. affiliates to the Entity List[8] (with additional affiliates added in August 2019 and August 2020) as entities who may have engaged in activities that are contrary to U.S. national security or foreign policy interests and are subject to specific license requirements for the export, reexport, and/or transfer (in-country) of specified items.

- Also in May 2019, the President issued an executive order prohibiting transactions involving ICT and services provided by foreign adversaries or their agents, and which pose an undue risk to critical infrastructure or to U.S. national security.[9]
- In 2020, the Federal Communications Commission (FCC) published a final rule in response to ongoing concerns about the integrity of the communications supply chain.[10] The rule prohibits the use of money from the Universal Service Fund to purchase or obtain equipment or services from any communications equipment or service provider identified by the FCC's Public Safety and Homeland Security Bureau as posing a national security risk to communications networks or the communications supply chain, such as Huawei Technologies Company and ZTE Corporation.[11]

[7]The John S. McCain National Defense Authorization Act for Fiscal Year 2019 prohibits executive branch agencies from procuring, obtaining, extending, or renewing a contract to procure or obtain any equipment, system, or service that uses "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system. Pub. L. No. 115-232, § 889(a)(1)(A), 132 Stat. 1636, 1917 (2018). Executive branch agencies are also prohibited from entering, renewing, or extending contracts with entities that use equipment containing "covered telecommunications equipment or services." *Id.*, at § 889(a)(1)(B). The act defines "covered telecommunications equipment or services" to include telecommunications equipment produced by Huawei Technologies Company (Huawei), ZTE Corporation, or any of their subsidiaries or affiliates. *Id.*, at § 889(f)(3)(A).

[8]The Entity List can be found at Supplement No. 4 to Part 744 of the Export Administration Regulations.

[9]The White House, *Securing the Information and Communications Technology and Services Supply Chain*, Executive Order 13873 (Washington, D.C.: May 15, 2019).

[10]See 47 C.F.R. § 54.9 (2020).

[11]To support broadband deployment in unserved areas, FCC provides billions through the Universal Service Fund's high-cost program to telecommunications carriers that offer broadband and voice services in areas that are costly to serve. These areas are typically rural or remote and increase carriers' infrastructure costs due to challenges, such as difficult terrain and longer distances between consumers. These areas also often have fewer consumers overall, further limiting carriers' abilities to offset infrastructure costs with end-user revenue.

- The President signed into law the Secure and Trusted Communications Networks Act of 2019 in March 2020, which prohibits the use of certain federal funds to obtain or maintain communications equipment or services from a company that, as determined by the FCC, poses an unacceptable risk to U.S. national security or the security of U.S. persons.[12]
- In February 2021, the President issued an executive order requiring the Secretaries of Commerce and Homeland Security to submit a report by February 2022 on supply chains for critical sectors of the ICT industrial base, including the industrial base for the development of software, data, and associated services.[13]
- In May 2021, CISA announced the publication of an ICT SCRM toolkit to assist organizations with information on how to secure ICT and related supply chains.

Despite these measures, we have previously reported that federal agencies have not effectively managed supply chain risks (which we further discuss later in this statement).[14] Similarly, we have previously reported on supply chain ICT risks to our nation's critical infrastructure sectors. For example:

- In June 2019, we reported that more than 2.7 million miles of pipeline that transports and distributes the natural gas, oil, and other hazardous liquids that U.S. citizens and businesses depend on, increasingly rely on sophisticated networked computerized systems and electronic data, which may be vulnerable to cyberattack or intrusion if not adequately protected.[15] In December 2018, we reported on weaknesses in the Transportation Security Administration's (TSA) management of its pipeline security efforts, including that the quantity of TSA's reviews of corporate and critical facilities security had varied considerably. So far, TSA has fully addressed 7 of our 10 recommendations for improving their oversight of pipeline security. However, 3 recommendations related to pipeline

[12]Pub. L. No. 116-124, §§ 2-3, 134 Stat. 158-159 (2020).

[13]The White House, *America's Supply Chains*, Executive Order 14017 (Washington, D.C.: Feb. 24, 2021).

[14]GAO-21-171.

[15]GAO, *Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment*, GAO-19-426 (Washington, D.C.: June 5, 2019).

security workforce and risk management have yet to be fully addressed.[16]

- In August 2019,[17] we reported that the Federal Energy Regulatory Commission (FERC)[18] had approved a new standard in October 2018 to bolster SCRM protections for the nation's bulk power system.[19] However, we found that this and other FERC-approved cybersecurity standards only partially addressed NIST's guidance for improving critical infrastructure cybersecurity. In particular, the standards fully addressed associated subcategories for establishing SCRM processes, security measures in contracts with suppliers and third-party partners, and evaluations of suppliers and third-party partners to ensure they meet their contractual obligations. However, the standards did not address subcategories for response and recovery planning and testing with suppliers and third-party providers, and for using the SCRM process to identify, prioritize, and assess suppliers and third-party partners.
- In October 2020, we reported that vulnerabilities can be introduced to avionics systems at multiple points within an insecure supply chain.[20] To date, extensive cybersecurity controls have been implemented and there have not been any reports of successful cyberattacks on an airplane's avionics system. However, the increasing connections between airplanes and other systems, combined with the evolving cyber threat landscape, could lead to increasing risks for future flight safety.

[16]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).

[17]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[18]FERC is the regulator for the interstate transmission of electricity with responsibility to review and approve standards for the reliable operation of the bulk power system.

[19]The term "bulk power system" refers to (1) facilities and control systems necessary for operating the interconnected electric transmission network and (2) the output from certain generation facilities needed for reliability. FERC oversees the North American Electric Reliability Corporation, the federally designated U.S. electric reliability organization responsible for conducting reliability assessments and developing and enforcing mandatory standards to provide for reliable operation of the bulk power system.

[20]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).

- In November 2020, we reported that the global reach of the 5G supply chain, as well as the technological complexity of the components of 5G technologies, presented the risk that components from suppliers whose quality and security could not be fully guaranteed may be used in 5G networks.[21] According to an April 2019 Defense Innovation Board report, a compromised 5G supply chain could pose a serious threat to national security by introducing vulnerabilities into networks and systems.[22]

In addition to our findings, the Cyberspace Solarium Commission[23] has also made recommendations related to the challenge of mitigating supply chain risks.[24] For example, the Commission has recommended that:

- Congress direct the U.S. government to develop and implement an ICT industrial base strategy to ensure more trusted supply chains.
- Congress appropriate consistent funding and task the executive branch to develop and implement research and development priorities in emerging technologies.
- Congress and the executive branch identify and budget the funds necessary to achieve the goals of the Cyber Moonshot Initiative.[25]
- The Supply Chain and Counterintelligence Risk Management Task Force within ODNI explore additional avenues to expand its support to critical infrastructure.
- The executive branch strengthen the capacity of the Committee on Foreign Investment in the United States.

[21]GAO, *5G Wireless: Capabilities and Challenges for an Evolving Network*, GAO-21-26SP (Washington, D.C.: November 24, 2020).

[22]Defense Innovation Board, *The 5G Ecosystem: Risks & Opportunities for DOD* (Washington, D.C.: April 2019).

[23]John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140 (2018) established the Cyberspace Solarium Commission, a federal commission made up of members of Congress and appointees, as well as officials from the Office of the Director of National Intelligence, the Department of Homeland Security, the Department of Defense, and the Federal Bureau of Investigation.

[24]U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

[25]In 2018, the President's National Security Telecommunications Advisory Committee called for a "moonshot" initiative to address the action needed to address the "progressively worsening cybersecurity threat environment" facing our public safety, economic prosperity, and national security. The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on a Cybersecurity Moonshot* (Nov. 14, 2018).

Recent events have illustrated that the nation's critical infrastructure continues to face growing and increasingly sophisticated cyber threats, as demonstrated by the SolarWinds incident, as well as the ransomware attack that led to a shutdown of a major U.S. fuel pipeline in early May 2021.[26]

Federal Agencies Have Taken Actions to Respond to the Recent Compromise of Widely Used Network Management Software

In response to the recent compromise of a widely used network management software—SolarWinds Orion—several federal agencies have taken action. Specifically, in December 2020, CISA issued an emergency directive requiring agencies to take action and an alert explaining that an advanced persistent threat actor, later determined to be the Russian Foreign Intelligence Service, had been observed leveraging, among other techniques, a software supply chain compromise of the SolarWinds software.[27] As emphasized in the directive, this threat posed a grave risk to federal, state, local, tribal, and territorial governments, as well as critical infrastructure entities and other private sector organizations.

Also in December 2020, the National Security Council (NSC) staff formed a Cyber Unified Coordination Group (UCG), in accordance with Presidential Policy Directive-41, to coordinate the government response to the cyberattack. The UCG is composed of the Federal Bureau of Investigation (FBI), CISA, and ODNI, with support from the National Security Agency (NSA).

In response to the incident, the UCG was tasked with, and took, a number of steps to help organizations identify and remove the threat actor. These steps included gathering intelligence and developing tools and guidance. Specifically, the FBI identified the scale and scope of the incident and engaged with affected entities. In addition, NSA and CISA released cybersecurity advisories that detailed adversary techniques and provided mitigation actions for system owners.

[26]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.

[27]CISA, Emergency Directive 21-01 and Alert AA20-352A.

The UCG also undertook a number of other efforts. For example:

- The UCG reported in January 2021, that fewer than 10 U.S. government agencies were compromised for the primary purpose of espionage.
- In March 2021, CISA released the CISA Hunt and Incident Response Program, a software tool that helps network defenders find indicators of compromise associated with malicious activity for on-premises systems.
- In April 2021, CISA, the FBI, and NSA jointly confirmed that the Russian Foreign Intelligence Service was responsible for the SolarWinds incident. In addition, to aid organizations in conducting their own investigations and security their networks, the Department of Homeland Security, including CISA, and the FBI released an advisory providing information on the Russian Foreign Intelligence Service's cyber tools, targets, techniques, and capabilities.
- Also in April 2021, the NSC stated that lessons learned from this incident will be identified and used to improve future federal government responses to significant cyber incidents.[28]

Subsequent to these actions, in April 2021, the Deputy National Security Advisor for Cyber and Emerging Technology announced the deactivation of the Cyber UCG for the SolarWinds incident. According to the Deputy National Security Advisor, the group was deactivated after the UCG completed its initial surge efforts.

In addition to the actions taken by the UCG, in April 2021, the President issued Executive Order 14024. The executive order declared a national emergency to address the threat of harmful foreign activities of the Government of the Russian Federation, including engaging in and facilitating malicious cyber-enabled activities against the United States and its allies and partners.[29]

Also, in May 2021, the President issued Executive Order 14028 that was prompted, in part, by the compromise of the SolarWinds software supply chain. Among other things, the executive order directed the Secretary of Homeland Security, in consultation with the Attorney General, to establish

[28]https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/19/statement-by-deputy-national-security-advisor-for-cyber-and-emerging-technology-on-solarwinds-and-microsoft-exchange-incidents/ (accessed Apr. 20, 2021).

[29]The White House, *Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation*, Executive Order 14024 (Washington, D.C.: Apr. 15, 2021).

a Cyber Safety Review Board to review and assess the threat activity, vulnerabilities, and mitigation activities of, and agency responses to, significant cyber incidents.[30]

The Board's initial review is to be focused on the compromise of SolarWinds and is to include recommendations to the Secretary of Homeland Security for improving cybersecurity and incident response practices. To address software supply chain security, the executive order directed, among other things, the Director of the National Institute of Standards and Technology's (NIST) to publish guidelines that include criteria to evaluate the security practices of developers and suppliers of critical software and guidance identifying practices that enhance the security of the software supply chain.[31]

We have ongoing work examining federal agencies' responses to SolarWinds and any lessons that they have identified from the compromise. We plan to issue a report detailing our findings later this Fall 2021.

Few Federal Agencies Implemented Foundational Practices for Managing ICT Supply Chain Risks

The recent compromise of SolarWinds highlights the significance of threats to the ICT supply chain. In December 2020, we reported on the 23 civilian agencies'[32] implementation of foundational practices for managing ICT supply chain risks.[33] In that report, we identified and selected the

[30]The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[31]The executive order defines critical software as software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources).

[32]The 23 civilian 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. We did not include the Department of Defense because our scope was the civilian agencies.

[33]GAO-21-171.

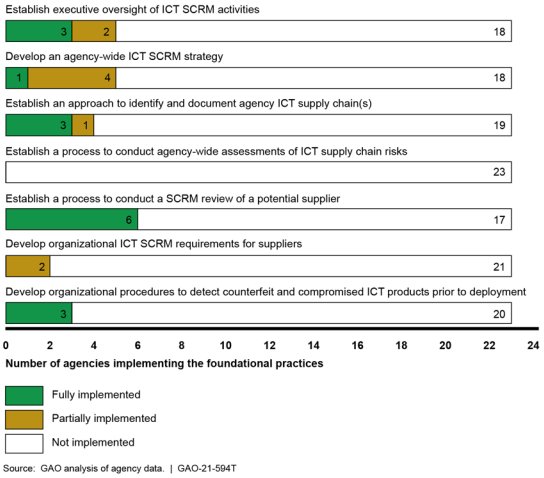
seven practices from NIST's guidance that are considered foundational for an organization-wide approach to ICT SCRM.[34] These selected foundational practices are:

- establishing executive oversight of ICT activities, including designating responsibility for leading agency-wide SCRM activities;
- developing an agency-wide ICT SCRM strategy for providing the organizational context in which risk-based decisions will be made;
- establishing an approach to identify and document agency ICT supply chain(s);
- establishing a process to conduct agency-wide assessments of ICT supply chain risks that identify, aggregate, and prioritize ICT supply chain risks that are present across the organization;
- establishing a process to conduct a SCRM review of a potential supplier that may include reviews of the processes used by suppliers to design, develop, test, implement, verify, deliver, and support ICT products and services;
- developing organizational ICT SCRM requirements for suppliers to ensure that suppliers are adequately addressing risks associated with ICT products and services; and
- developing organizational procedures to detect counterfeit and compromised ICT products prior to their deployment.

However, as we discussed in our report, none of the 23 agencies had fully implemented all of the supply chain risk management practices. Further, 14 of the 23 agencies had not implemented any of the practices. Figure 1 summarizes the extent of the agencies' implementation of the practices.

[34]See NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, v. 1.1 (Apr. 16, 2018); *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP 800-161 (Gaithersburg, Md.: Apr. 2015); *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37, Rev. 2 (Gaithersburg, Md.: Dec. 2018); and *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: Mar. 2011).

Figure 1: Extent to Which 23 Civilian Agencies Implemented Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) Practices



Source: GAO analysis of agency data. | GAO-21-594T

As a result of not fully implementing these selected foundational practices, the agencies are at a greater risk that malicious actors could exploit vulnerabilities in the ICT supply chain, causing disruptions to mission operations, harm to individuals, or theft of intellectual property. For example, without establishing executive oversight of SCRM activities, agencies are limited in their ability to make risk decisions across the organization about how to most effectively secure their ICT product and service supply chains. Moreover, agencies lack the ability to understand and manage risk and reduce the likelihood that adverse events will occur without reasonable visibility and traceability into supply chains.

Officials from the 23 agencies cited various factors that had limited their implementation of the selected foundational practices for managing supply chain risks. The most commonly cited factor was the lack of

federal SCRM guidance. For example, 11 agencies reported that they were waiting for federal guidance to be issued from the FASC before implementing one or more of the selected foundational practices. At the time that our report was issued, according to OMB officials, the council expected to complete this effort by December 2020. As of May 2021, we have not yet received further information from OMB regarding the council's progress on this effort.

Nevertheless, while the additional direction and guidance from the council could further assist agencies with the implementation of the selected foundational practices, federal agencies currently have guidance they can already use to assist with managing their ICT supply chain risks. Specifically, NIST issued ICT SCRM-specific guidance in 2015[35] and OMB has required agencies to implement ICT SCRM since 2016.[36]

NIST is currently updating its guidance, with a final version expected by April 2022. According to NIST, the revised guidance, among other things, is expected to capture leading cyber SCRM practices from government and industry and integrate related SCRM concepts and processes from other NIST publications.

In a sensitive report issued in October 2020, we made 145 recommendations to the 23 agencies to fully implement selected foundational practices in their organization-wide approaches to ICT SCRM.[37] Of the 23 agencies, 17 agreed with all of the recommendations made to them; two agencies agreed with most, but not all of the recommendations; one agency disagreed with all of the recommendations; two agencies neither agreed nor disagreed with the recommendations, but stated they would address them; and one agency had no comments. We believe that all of the recommendations are warranted.

In May 2021, we received updates from six of the 23 agencies regarding actions taken or planned to address our recommendations. We are currently evaluating evidence provided by these six agencies to determine the extent to which implementation of recommendations has occurred. However, to date, none of the agencies have yet fully

[35]NIST SP 800-161.

[36]OMB, Managing Information as a Strategic Resource, Circular No. A-130 (July 28, 2016).

[37]GAO-21-164SU.

addressed recommendations to implement foundational practices in their organization-wide approach to ICT SCRM. We intend to continue monitoring agencies' progress in implementing them.

In summary, as our work has emphasized, the need for agencies to make risk-based ICT supply chain decisions about how to secure their systems is urgent. Recent events, such as the compromise of SolarWinds Orion, highlight the importance of implementing SCRM to protect against threats posed by malicious actors. In the absence of foundational risk management practices, malicious actors may continue to exploit vulnerabilities in the ICT supply chain, causing further disruption to mission operations, harm to individuals, or theft of intellectual property.

Chairs Foster and Stevens, Ranking Members Obernolte and Waltz, and Members of the Subcommittees, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Vijay A. D'Souza, Director of Information Technology and Cybersecurity, at (202) 512-6240 or dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Edward R. Alexander, Jr. (Assistant Director), Josh Leiling (Assistant Director), Season Burris (Analyst-in-Charge), Linda Erickson, Rebecca Eyler, Keith Kim, Katherine Noble, Niti Tandon, and Scott Pettis. Other staff who made key contributions to the reports cited in the testimony were Anna Bennett, Kiana Beshir, Donald Baca, Christopher Businsky, Donna Epler, John deFerrari, Jennifer Franks, Carol Harris, Kaelin Kuhn, Hoyt Lacy, Catherine Maloney, Nick Marinos, Carlo Mozo, Sukhjoot Singh, Angela Watson, and Eric Winter.

Vijay D'Souza a Director of Information Technology and Cybersecurity at the US Government Accountability Office (GAO) where he leads a diverse set of evaluations of government cybersecurity and IT issues. Current areas of work include ransomware, the SolarWinds breach, use of the NIST Cybersecurity Framework and IT modernization efforts at USDA. Vijay also leads GAO's Center for Enhanced Cybersecurity, which provides advanced technical support for GAO's cybersecurity audits. He previously led GAO's data analytics activities and worked for GAO's Health Care Team. Vijay has been at GAO since 2001. Prior to GAO, he worked in the international development area, and before that as a developer of technology training. Mr. D'Souza has an M.B.A from the University of California Berkeley and a B.S. in Engineering from the University of Maryland, College Park.

Chairman FOSTER. Thank you. And, at this point, we will now begin our first round of questions. The Chair will recognize himself for five minutes.

Mr. D'Souza, if we could step back for a moment and consider the Federal response to SolarWinds? Could you please briefly go over the timeline of how the Federal agencies responded? You know, when was the Federal Government first made aware of the breach, how did the directions to address the breach roll out, and in general did the system work as designed, and did the—all the Federal agencies act quickly to remediate the breach?

Mr. D'SOUZA. Thank you. As I mentioned, the first public announcement from DHS was in December, although it is our understanding they may have, you know, had some earlier information about the incident. The agencies were directed to respond to that, and certainly by April our understanding is it had been largely addressed. However, the details are—we're still looking into the details. Part of what we're doing in our ongoing work is trying to look at the detailed information that was provided to Congress and to CISA, and try to compile it to see kind of how it lines up.

Chairman FOSTER. Yeah. Did—so what is the procedure when the first alert comes in through classified channels, and then people realize this will have a big—as—a big effect on the commercial world? Is there a well-defined protocol for deciding when the commercial world should be apprised of the threat?

Mr. D'SOUZA. So your question is when the government should let the private sector entities know about issues?

Chairman FOSTER. Right. Yeah. Is that—is there a well-defined procedure for that that operates regularly?

Mr. D'SOUZA. I think—so I think there are procedures, but I don't—I think well—you know, I think there's area for improvement. I think part of what this has established is the need for better information sharing. Part of what you touched on is, you know, the Executive order that the administration recently released, directs DHS to do more to kind of specify the triggers in this area. There definitely are tools and processes in place. For example, there was some legislation passed a few years ago directly related to cyber information sharing. But, you know, our experience has been, when we talked to the private sector, you know, they definitely identified positive steps that the Federal Government has taken with regard to information sharing, but also a lot of room for improvement.

Chairman FOSTER. Um-hum. Is there—would the rest of the panelists like to chime in on that issue? Any observations on, you know, whether the system was badly designed, or worked as it should, or what the—or are we going to have to undergo a fundamental redesign to get a better result?

Mr. D'SOUZA. If I could add one point, is—I think the processes are in place, but I think it's the trust building. I think, you know, there's a lot of—there tends to be a lot of nervousness from the private sector about sharing information with the government. I'm not sure so much about the other way, although one of the issues the government has is sharing classified information, figuring out how to sort of declassify the information, share it publicly. So these

issues have been identified, but we're definitely not where we need to be in this area.

Chairman FOSTER. Um-hum. And one of the decisions that the government, and probably every player in industry has to do, is the make versus buy decision. And, you know, if we're—you know, we do a lot in Congress to encourage the government to contract with a large number of small businesses, all right? That is sort of the exact opposite of what you'd want to do for cybersecurity reasons. And how should we think about and handle that, you know, that tension? Any observation, or—some of you have experience with some of the large players in industry, where it's my understanding they just do a lot of stuff in house in part to avoid cybersecurity threats that they cannot control.

Dr. HERR. It's a good question, asking about firm size and vendors, but I think it speaks to two issues. One is capability and maturity, but the other is innovation, and to some degree the downside of a large vendor is the risk of a monoculture, and the risk of some homogeneity in the way that that vendor approaches security in the way it manages the assumptions, or the threat model, that it has for its products. So I don't think it's necessarily a clean cut to say bigger is better. It can offer some efficiencies and some scale, and you will find, in some cases, at a number of these vendors' security teams that no other company could afford to maintain, and talent that you're not going to find in very many places on the planet, but that said, a mix—a composition of small and large I think is important.

Mr. SCHOLL. I also—I'm sorry.

Ms. MOUSSOURIS. Go ahead, Matthew.

Mr. SCHOLL. When you look at the build versus buy decision, it's not necessarily just the point issue of acquiring, especially in software, a piece of software, but it's a full range of life cycle costs that come with keeping and maintaining a piece of software over time. And often in those cases you will find industry has the persistence, to some extent, to be able to maintain and update, especially software now that is so dynamic in its nature in a way that sometimes the government is not able.

Ms. MOUSSOURIS. And I'd like to add to that answer, in terms of build versus buy, in some cases we have to participate according to technical specifications, so even if we were to build technology ourselves, there still may be vulnerabilities inherent in the technical specification. That is one of the reasons why the United States, its partners, and also the adversaries that we have in cyberspace, participate in international standard setting and specification setting. But there are going to be implementation issues if an underlying technical specification contains vulnerabilities. That is one of the common scenarios that requires multi-party vulnerability coordination across the supply chain.

Chairman FOSTER. Thank you, and I'll now recognize the Ranking Member, Mr. Obernolte, for five minutes of questions.

Mr. OBERNOLTE. Thank you, Mr. Chairman, and thank you to our panelists. It's been a fascinating hearing. My first question is for Mr. Scholl at NIST.

So one of the things that stood out to me, from reading the GAO report was that these organizations that had not implemented the

best practices, when questioned about why they had not implemented them, the No. 1 answer was a lack of Federal guidance, which I think is probably going to be a source of frustration for you. Hopefully the Executive order will help with that, because it directs NIST to either identify existing standards and best practices, or develop new standards and best practices to combat this problem. Do you have a preliminary feel for which of those two options NIST is going to take? Are there existing standards that you'll be able to identify, or are you going to have to write your own?

Mr. SCHOLL. Thank you for the question, and it's an excellent question. We too are encouraged by the Executive order and its ability to shine a focus on this issue not just for the Federal agencies, but for NIST in our work as well. Our preliminary look at fulfilling the requirements within the Executive order will be to identify existing guidance, or even specifics within existing guidance, that we can call out and consolidate for use by the agencies. So, first and foremost, we want to identify and cite work that exists rather than create new work. After we have done that, we will work with both our industry and our agency partners to see if there are any critical gap areas in that existing work, and then that will form the nucleus for any new created items that we'll have to make. The timelines are short in getting out our initial deliverables, and so that is going to be our approach.

Mr. OBERNOLTE. Well, thank you, that makes sense. And follow-on question, since you brought it up, obviously the timelines in the Executive order are very ambitious. Do you think that they are realistic, and does NIST have the resources that you need to meet them?

Mr. SCHOLL. NIST is certainly committed to meeting all of the objectives that NIST is assigned within the Executive order, and we are on track and working toward achieving all of those objectives. So currently NIST believes wholeheartedly that we will accomplish the objectives assigned to us, and even though the timelines for initial deliverables may be short, NIST is also committed to applying a sense of persistence to this activity over a much longer term. So the initial deliverable may be short, but we also plan on staying persistent on these issues over a much longer period of time as well.

Mr. OBERNOLTE. Well, great. Thank you. Well, we're certainly looking forward to reviewing what you've come up with. Then a question for Dr. Herr. So we've been talking about guidance here, but obviously guidance is meaningless without implementation. So what can be done to make the guidance that's being developed more implementable by Federal agencies?

Dr. HERR. It's a great question, sir. I think part of the challenge that we've seen is that much of the standards process for software development for security, for deployment, is still rooted in PDFs and spreadsheets, I think as you mentioned in your opening statement, and that is a—it presents an implementation challenge for any developer to then take that, interpret it, and try to write it into their own tools, and build their own organic processes and policies.

So I think the biggest thing, and we've seen calls for this from a number of folks in the community, is automation, right?

Implementable guidance that can be pulled into common developer tools, into integrated development environments, and made an automated rule. And there's two sort of big drivers for this, or reasons for this. One is that ease of implementation, but the second is to keep pace with software development. So not just developers of varying levels of maturity and scale. Not everybody is a large software vendor. Many of these security concerns are coming from open source projects, small, not well resourced academic outfits, places where we want to see good security practice, but we're not necessarily going to expect a million dollar, full time security team. But the second is to keep pace with software development, where we may see five, 10, 15 versions of a single product in one day, and so there is no process, no PDF-based audit framework, that is going to allow someone to come along behind and check every box for every one of those versions. So I think automation really has to be the watch word. And, to the extent possible, where NIST is appropriately resourced to provide guidance to developers, and to those that own these development tools, on exactly how to implement that in those programs.

Mr. OBERNOLTE. I completely agree with you. And then lastly here, not a question as much as a comment on, Dr. Herr, your response to Chairman Foster's previous question, you said that you thought that a mix of large and small companies is vital to the supply chain, and I completely agree, but I'd also like to highlight some other advantages of having more companies in the supply chain is maintaining diversity in the supply chain so that we don't have a single point of failure that affects the rest of the chain. And so I think it's vital that we have lots of companies in the supply chain, and—both small and large companies, particularly small companies, because in addition to diversity, that also creates competition, and drives down our governmental costs. I think we're stuck with this idea that we're going to have a lot of companies out there, and that some of them are going to be small, and therefore are going to be less sophisticated about implementing these best practices. But I want to thank you very much, and I'll yield back, Mr. Chairman.

Chairman FOSTER. Thank you. And we will now recognize Representative Stevens for five minutes.

Ms. STEVENS. Thank you so much. Mr. Scholl, how long have you been working at NIST?

Mr. SCHOLL. I've been at NIST for 15 years, ma'am.

Ms. STEVENS. OK, great. And I know you're—you also served your country previously as well as a veteran, and we want to thank you for that. And how big is your shop in your area with the chief information, or chief—you know, cybersecurity efforts? How many people are working with you?

Mr. SCHOLL. My Federal staff is at 94 headcount, and I am augmented with post-doctoral fellows, guest researchers, foreign guest researchers, and summer undergraduate research fellows as well. But Federal——

Ms. STEVENS. Great.

Mr. SCHOLL [continuing]. Staff is 94.

Ms. STEVENS. Great, great. And do you mind just reminding us your total budget? Is it 32?

Mr. SCHOLL. Yes, ma'am.

Ms. STEVENS. OK. $32 million? And I know my colleague on the other side of the aisle asked you a nice question about your ability to meet the Executive order, and it—very much appreciated your response. And I'm not a fan, by the way, of—you know, I think NIST is a great example of an agency that does a lot with a little. I'm not a fan of bloating, and, you know, just unnecessarily, you know, pumping up dollars in agencies that, like yours, can do a lot with a little, but I do think identifying, you know, that pinpoint of where we could use additional resources could be helpful. I'm just also wondering, could you—do you have any—you say you have 94 people, and you're working with different researchers and the post-docs—we love hearing from them when they come to testify—throughout NIST, but how's retention back?

Mr. SCHOLL. Retention is outstanding at NIST.

Ms. STEVENS. Great.

Mr. SCHOLL. A fair amount of my workforce actually could retire any day, and they have no intention to do so. There's a strong commitment to mission. People feel very energetic and energized by the purpose, and it's an outstanding set of staff that I'm actually privileged to lead.

Ms. STEVENS. Well, that's what we like to say, Mr. Scholl, NIST is the best kept secret in government, and so I'm glad to hear that your workforce has a high retention and a high charge to the mission, and we want to continue to support you in all those ways.

Katie, your company and background is just absolutely amazing, and I'm drooling hearing your testimony, and reading about your contribution to ISO standards, and the implementation of those. Have you worked with NIST in any specific ways?

Ms. MOUSSOURIS. I have been invited to work with NIST, presented at various meetings, and I'm in the process of potentially joining one of the advisory boards for NIST, so Matthew and I have met a few times before.

Ms. STEVENS. Wonderful. Yeah, you and Matthew have to spend some time together, because—yeah, we're—I think what we're getting at in this hearing is pinpointing the nexus between where we can identify our software supply chain opportunities with our Federal Government. You know, Dr. Foster touched on this as well with the standards, and, you know, in many respects I guess we'll have to come back to you, because I'd be interested in any feedback that you have to pay about, you know, why people aren't leveraging certain programs, you know, is there enough outreach? And it's not programs, but, you know, when we were brief on NIST's cybersecurity capabilities it's like, does everyone really know about this? How are we connecting—and, you know, we've got our NIST MEP centers as well that are located around the country. Can you just remind me where you're located too, Katie, if you don't mind sharing for the record?

Ms. MOUSSOURIS. I am in the sunny Seattle area in the Pacific Northwest.

Ms. STEVENS. Right. So—yeah, and so, you know, you're also bolstered by a strong ecosystem out there, but you could imagine that—and I don't know if you've encountered any partners, or people who are different geographies who haven't been able to connect

into some of the resources out there in our Federal Government who maybe aren't as co-located by—like entities such as yours.

Ms. MOUSSOURIS. Well, I can say that, by comparison of the scale of what Microsoft, one major software vendor, invested in overall cybersecurity, its budget at the time that I was last there close to half a billion dollars in cybersecurity, with more than 400 dedicated technical resources and others in support of the cybersecurity mission of just one company. So I think that, you know, when we look at—that's an outlier, obviously, in its investment and its capabilities, but we do have to look at this in terms of a long tailed spectrum of even very large organizations similar in, you know, overall size of company to Microsoft not having those types of investments in place over many years because they weren't forced to do so, like the operating systems were starting, you know, over 20 years ago.

Ms. STEVENS. Well, great. Well, with that, thank you so much to all of our witnesses, and I'll yield back, Mr. Chair.

Chairman FOSTER. Thank you, and we will now recognize the Ranking Member of the Full Committee, Mr. Lucas, for five minutes.

Mr. LUCAS. Thank you, Mr. Chairman. This has been a very fascinating hearing so far. I'd like to turn to Mr. Scholl. This Committee's one of three congressional Federal agencies who are required to be notified within 7 days of a major cyber incident under the *Federal Information Security Modernization Act of 2014*, or *FISMA*, as I prefer to call it. After the SolarWinds incident, only a handful of Federal agencies that were breached complied with *FISMA* notification requirement, and they did not consider the breach to be a major incident. These reports are a major source of transparency and oversight for Congress and the American people. Can you explain the process for how Federal agencies determine what constitutes a major incident under *FISMA*?

Mr. SCHOLL. I certainly will do my best, sir, and if need be, I can follow up. It is my understanding that specific guidance on definitions of major incidents come through policy from the Office of Management and Budget to the agencies. This is further clarified and specified by CISA, whereupon an agency then identifies an issue first, then categorize it as reportable or not reportable under that OMB policy guidance, and then initially conducts the first reports back to CISA and OMB. This is my understanding.

Often first analysis and initial forensics of an issue may be incomplete or inaccurate, so I believe agencies are encouraged to err to the side of reporting just to be safe, but that lack of sometimes initial information does make the clarity of reportable versus nonreportable incident difficult, at least upon initial report.

Mr. LUCAS. You see why that causes us great concern. Would anybody else on the panel like to touch on this subject about the recommendations about how to improve reporting and transparency under *FISMA*?

Mr. D'SOUZA. Sure, if I could. A major incident is basically an incident that's likely to result in demonstrable harm to the U.S. interest, so, I mean, I think just from—sort of from instinct SolarWinds would meet that criteria, but we do know that several agencies working at the same criteria came up with, you know, dif-

ferent determinations. So I think part of what we're doing in our work, for example, is to compare the decisionmaking by the different agencies. I do think a more consistent interpretation of the guidance is probably something that's going to be important.

Ms. MOUSSOURIS. I would also like to add that some of the resources internally to investigate some of these issues are the same resources that have to, you know, implement security best practices, as well as performing these investigations, as well as investigating potential vulnerability reports that ideally have not been exploited yet. We have an overstretch of internal cybersecurity resources across the private sector as well with those unfilled job roles. The problem is exacerbated across the Federal Government.

Mr. LUCAS. Anyone else? Mr. D'Souza, is there presently an oversight mechanism by which Federal agencies that fail to implement requisite standards and best practices under ICT SCRAM can be held accountable? And if so, can you briefly describe that process?

Mr. D'SOUZA. We think that there's a weakness in this area. There are a number of processes that Federal agencies have to follow for oversight generally in IT security. There's the annual *FISMA* reporting. DHS has authority in this area as well through its binding operational directives. However, the specific issue of supply chain risk management is really the FASC, the Federal—the organization I mentioned earlier. That is going to have sort of the enforcement ability here. And they have not done a lot in this area. They had issued a strategic plan, and they issued an interim rule, but more needs to be done there. The agency inspector generals (IGs), which do the annual *FISMA* evaluations, they did add one metric related to supply chain security to their latest evaluation guidance, but that was just added after SolarWinds, so, you know, clearly we need to probably add more to that area going forward, and then both the IGs and OMB are going to need to incorporate that into their annual reporting. This is going to take, you know, several years to really change the culture, and really make sure agencies are dedicating the resources they need to do, but they could do it through the existing oversight mechanisms.

Mr. LUCAS. Clearly, Mr. Chairman, this is an area we need to keep track of, and with that I yield back. Thank you, Mr. Chairman.

Chairman FOSTER. Thank you. And we'll now recognize the gentleman from Colorado, Mr. Perlmutter, for five minutes. Mr. Perlmutter? You're being recognized for five minutes of questions. And you must unmute.

Mr. PERLMUTTER. Sorry.

Chairman FOSTER. Yes, sir.

Mr. PERLMUTTER. I'm multitasking here. I've got a——

Chairman FOSTER. I know it was a last minute——

Mr. PERLMUTTER [continuing]. Couple things going.

Chairman FOSTER [continuing]. Change of order.

Mr. PERLMUTTER. I——

Chairman FOSTER. Right.

Mr. PERLMUTTER. Let's see. Can you hear me?

Chairman FOSTER. Yes.

Mr. PERLMUTTER. All right, good. Sorry. So I just have a few questions. And, first, Dr. Scholl, where is your office?

Mr. SCHOLL. I am located in Gaithersburg, Maryland.

Mr. PERLMUTTER. OK. And is that where most of your staff is?

Mr. SCHOLL. Correct.

Mr. PERLMUTTER. OK. We've been working with NIST for several years, and I've got several of my Financial Services Committee colleagues on here, a bill called the *Data Breach Insurance*, where we've tried to use the NIST protocols for, you know, to get small businesses, not so much because of Federal hacking, but because of hacking that a small business might have that then affects their lender, or their bank, which then spreads every place. And we've been trying to use both insurance and tax incentives, to couple those with the NIST protocols. How do you find your protocols that you guys established back in 2014/2015 being accepted by small business generally? Is it—do you see it happening or not?

Mr. SCHOLL. We see it happening across a wide range of both small businesses, as well as levels of use and adoption. We have a couple of different mechanisms to do that. We have a dedicated small business corner, where we look to tailoring and adapting our work to small businesses. Chairwoman Stevens had mentioned the MEP Centers as well, the Manufacturing Extension Partnership Centers that NIST has around the country, which we also use to tailor and amplify NIST cybersecurity products out to small businesses through the MEP Centers as well. So we have a couple of different mechanisms that we use to try to both tailor our guidance so it's appropriate for a small business, as well as reach them.

Mr. PERLMUTTER. OK. Thanks. I mean, I guess from the Financial Services standpoint, we're just trying to—you know, the banks say, well, the vendor caused this hack, and vice versa, and who's going to pay for it? So we're going to continue to press forward in providing incentives and promoting that protocol. But my next question is for Ms. Moussouris and Dr. Herr, because you both said something that was a little bit troubling to me, and they involve sort of—I guess I'll start with you Dr. Herr. There was an effort a number of years ago at the Federal level to have a single portal for all the departments, all the agencies, everything goes through there, and it used some kind of—and, Mr. D'Souza you may recall this too—something called EINSTEIN, or—I can't remember what the heck it was, to try to, you know, be a first guard against hacking. But there has always been a desire to try to have sort of separate silos so that everything didn't get hacked at once. I mean, what's your opinion on something like that? Do you understand what I'm asking?

Dr. HERR. Yes, sir, and I think the question you're asking is one that's been discussed at length over the last five to 10 years in cybersecurity. It's the debate between a walled, you know, garden, effectively, right, a single perimeter that you defend with your life, and acknowledging that that perimeter is not going to save you from the enemy, and figuring out how to adapt to that.

So EINSTEIN, as I understand it, is a multi-generational set of systems intending to detect and mitigate attacks on Federal networks as rapidly as possible in time potentially to also eject them automatically. The challenge is, I think, to the question that you're asking, is that trying to take a network and isolate it from the outside world to keep it pristine is what we've seen in many cases fail

against both rudimentary and sophisticated attacks, and that, in SolarWinds and Sunburst, I think what we're seeing really good evidence of is the need to embrace the concept that's known as assumed breach, to look at your network, to assume that it's been compromised, and to try to minimize the harm that any one device or any one user can do to you as they're moving through those networks. So I think EINSTEIN, you know, is a pathway toward that, hopefully.

There's been some discussion about the notion of zero trust, as you saw in the Executive order to a great extent. Zero trust is a useful concept. It's a design philosophy. There's a lot of maturation still required there to take that and actually implement it into policy, but I—hopefully I think that gets to the question you're asking.

Mr. PERLMUTTER. Thank you. And, Ms. Moussouris, do you have a thought about that?

Ms. MOUSSOURIS. Yes. EINSTEIN, you know, has limitations, much like many other, you know, cybersecurity tools, in that it is limited to look for what is already known and identified. In the SolarWinds incident, for example, that wouldn't have been detectable using EINSTEIN, or truly any other off the shelf tools, and that's evidenced in the fact that one of the top companies for investigating internal compromises, FireEye, even itself failed to detect that compromise for a few months while the attackers were working using the SolarWind software that they had compromised.

To your point about network segmentation internally, we do want organizations to move away from the model of hard, crunchy outside, soft, chewy center, so that is an apt, you know, an apt observation of what needs to go into place. I think the Executive order further stipulates that multi-factor authentication needs to be applied and rolled out across Federal Government systems, especially at access points to critical assets. That endeavor in the Executive order, while bold and necessary, is going to be a huge, heavy lift, so that is something to be aware of, that parts of the solution, including that example of rolling out multi-factor authentication to tightly access control, or monitor the access control, of various assets in the Federal Government, that is going to require a very, very heavy lift.

Mr. PERLMUTTER. Thank you. My time is way over, and I thank the Chair and Ranking Members for allowing me, and I yield back.

Chairman FOSTER. Thank you. And we'll now recognize Mr. Gonzalez for five minutes.

Mr. GONZALEZ. Thank you, Mr. Chairman, and thank you to our witnesses and panel for their testimony today to discuss the importance of our cybersecurity infrastructure. SolarWinds exposed multiple government and private sector vulnerabilities. The witness testimonies today have illuminated some improvements that I think we can make. I want to talk briefly about public/private partnerships, and data and information sharing with respect to how we solve this going forward.

I was speaking with one of my friends yesterday who works in the industry, the cybersecurity industry, and his comment to me was, we share information across portfolio companies, this gentleman happens to work in private equity, with respect to cybersecurity and cyber threats, but there's not a great coordi-

nating mechanism, either at the Federal level or in private industry and we can do it with our companies, but broadly there's less information sharing. So I guess, Ms. Moussouris, from the industry perspective, I want to get your insight on this notion of cyber threat sharing across agencies and industry. Do you think there needs to be further collaboration, and do you think one of the existing public/private partnerships on cybersecurity is the best way to foster this collaboration? Just help me understand, from your perspective, what we might gain from this sort of thing.

Ms. MOUSSOURIS. Well, I think information sharing with the private industry is very much gated upon the perceived or actual liability for those private organizations, so that is something that has been brought up numerous times, not just in this hearing, as something that would need to be addressed to provide sufficient legal cover for organizations that are seeking to share, private organizations.

I do think that, you know, some of our issues here are information sharing when there has been a breach versus before the breach, which is the vulnerability coordination type of information sharing. So when you are coordinating a vulnerability that affects a supply chain, ideally you're doing so ahead of a breach, so that is a different kind of information sharing that poses its own risks, in terms of, you know, investigations in progress up and down the supply chain, remediation plans in progress and being coordinated up and down the supply chain. The risks to that information sharing being accessed by an attacker is something that is of concern, especially with some of the Executive order breach notification requirements that are in place, because some of the deadlines would be occurring sort of mid-investigation of a potential vulnerability that could lead to a supply chain attack or a breach.

Mr. GONZALEZ. And how——

Ms. MOUSSOURIS. Does that sort of answer your question?

Mr. GONZALEZ. Yeah, it does. How would you recommend we mitigate that risk, if at all? I mean, what ideas do you have on that?

Ms. MOUSSOURIS. Well, you know, some of this has to be built out, in terms of capability. It is why I'm recommending maturity assessments for capabilities not just in regular cybersecurity practices, but also in the specialized internal practices that are required for multi-party vulnerability coordination. Microsoft itself, with its significant investment in cybersecurity, has only been tackling this problem head-on of supply chain vulnerability coordination with other entities since about 2008. When I created Microsoft Vulnerability Research to help coordinate Dan Kaminsky's DNS (Domain Name System) vulnerability was one of the first issues that we coordinated industry-wide, and including our government partners.

Mr. GONZALEZ. Thank you. And in your testimony you mentioned some improvements that could be made to the software bill of materials. Can you elaborate on some of the concerns with creating machine-readable inventory that is uniform?

Ms. MOUSSOURIS. I have no issues with creating machine-readable inventory that is uniform. The concerns that I have around implementing SBOM is that, one, you know, it may yield dividends to us, in terms of speeding up vulnerability coordination across the

supply chain in time. However, that working group has been at it for about 3 years, has not come up with a standard definition of what a minimum SBOM would entail, and that is part of NIST's big heavy lift to do as part of this Executive order, is defining what a minimum SBOM would be. An ingredient list alone does not give you actionable information, nor does a mapping to which CVEs (Common Vulnerabilities and Exposures), which vulnerabilities, apply to those ingredients. You actually need additional technical information, including the exploitability of a particular sub-vulnerability that may be included in the product package. So those are a summary of my concerns in that area.

Mr. GONZALEZ. Well, thank you, Mr. Chairman, and I yield back.

Chairman FOSTER. Thank you. And we'll now recognize Mr. Beyer for five minutes.

Mr. BEYER. Dr. Foster, thank you very, very much. This is really fascinating, I'm very grateful. Mr. D'Souza, how do you live with the frustration? Let me just point out that five months ago GAO recommended 23 agencies adopt these seven procedures. That's—seven times 23, that's 161 opportunities to succeed. 16 of them did it, so you've got a 10 percent completion ratio. As I read it, 14 did nothing. They complained about lack of guidance, and yet there was SCRM guidance from NIST in 2015, from OMB in 2016. You put out 145 recommendations in October 2020. As somebody who was never late with a paper, or unprepared for a test, even if I didn't do well on the test, how do you—well, is there any consequence for our public leaders who just don't do their job?

Mr. D'SOUZA. I think—as I was commenting earlier, I think enhanced reporting and oversight here is really going to be key to making changes. Agencies always face, you know, more than they—more things to do than they have time for, so they have to make a decision about what are they going to devote the most time to. If the status of their supply chain security programs is routinely reported on, and measured by Congress, and measured by OMB, and there's more transparency around these issues, I think that they will make progress in these areas. I think that's basically the thing that has to happen.

Mr. BEYER. Well, this slides right into a question for Ms. Moussouris. Luta Security, you had four very good suggestions, but the last was that Federal pay scales across the board, especially in cybersecurity, have to be able to compete with the private sector. I represent Northern Virginia, where every contractor I've talked to, every business I've talked to, says they can't find the sophisticated people that they need. How are we—do you see any plausible political way of paying Federal employees enough money to compete with the private sector? Like even a third of what they could make in the private sector?

Ms. MOUSSOURIS. Well, I think that, especially those of us with offensive security skills that can hack into everything, money is not our deciding driver of what we choose to do with our talents. Mission is also very important. But even with such an important mission, and an honor to contribute to national security, I think there does need to be, you know, a—an effort to uplift the cybersecurity salaries in the Federal Government.

But another part of that suggestion No. 4 in my testimony was actually hiring and training either existing employees in the Federal Government who desire to move into cybersecurity, but also providing a better national pipeline for hiring talent. Most of the cybersecurity job openings that you see are for senior and very experienced people. We do not have a great pipeline for entry level cybersecurity positions, which may help with some of the talent shortage, and some of the budgetary concerns.

Mr. BEYER. And it sounds like the talent shortage and the budgetary concerns feed back into what Mr. D'Souza has to work with, when, if you have people that don't have enough time, they're overwhelmed by the challenges that they have and may not have the training either.

As long as we're talking consequence, maybe, Ms. Moussouris, one more thought. When any of these supply chains things happen, or when they shut down Colonial Pipeline, and we see the consequence ripple through the economy, and, you know, with not much imagination, ripple through the fatality rates, you know, it hit the hospitals, it hits pharmacies, it—what should the consequences be? And I'm reminded of—in the Old West, when you stole a horse, you got hung, because it was life or death in that situation. It's life or death for so many people right now, and yet you never hear about anybody going to jail for violating cybersecurity. What you typically hear is they get hired.

Ms. MOUSSOURIS. Was there a question in there for me?

Mr. BEYER. I guess I'm asking you to lay out the criminal penalties for hacking, so——

Ms. MOUSSOURIS. You know, the Colonial Pipeline issue, as you are aware, sir, was orchestrated by non-Americans. They were a Russian cybercrime group, so I do think that, you know, some additional pressure from this administration on not harboring cybercrime groups, or turning a blind eye toward their activities internationally, will go a long way. But in terms of domestic cybercrime—or domestic origin cybercrime, I do think that there's a lot of opportunity for reform in existing cybersecurity anti-hacking laws. There's been a lot of ambiguity and a chilling effect on good cybersecurity researchers who happen to be able to perform very bad activities against critical infrastructure, and only recently have vulnerability disclosure programs been in place in the Federal Government level, but certainly hasn't trickled down to all of critical infrastructure in terms of allowing the public to notify if they see something, say something in cybersecurity.

So I do think that we need to take a look at ways to redirect young talent in cybersecurity domestically, especially if they got into a little bit of trouble when they were young. I think that is a potential huge source of cybersecurity talent eventually.

Mr. BEYER. Thank you.

Chairman FOSTER. Thank you. And we will now recognize Mr. Casten for five minutes.

Mr. CASTEN. Thank you, Mr. Chairman, and thank you to our panelists. The—I want to start with my own experience, that I'm hoping is not too stale. Before I came to Congress I ran a company that we built and operated utility operations inside industrials, which is to say that we managed huge campuses that had a ton

of dumb equipment, valves, traps, meters, lots of PLC- (programmable logic controller-) based systems. And we were sort of keenly aware that they didn't dispatch in the most efficient possible way, but when we tried to bring in an overarching system control to manage it, we never got comfortable that we could maintain, I think as you described, Ms. Moussouris, a—that hard, crunchy exterior. But we knew we had the creamy interior, if we let them in.

And, you know, to take it maybe in less metaphorical language, we couldn't find the software to solve the problem, and so we're then backing up to saying, well, can we implement the processes that would allow this? And as a mid-sized company, we just couldn't get comfortable that we could have the human resources, the process RAM (random-access memory) to manage it. So my first question for you, Ms. Moussouris, is there's a whole set of these solutions that are technical in nature, software patches, standards, what have you. There's a whole other set of solutions that are process in nature. When you are advising companies in the private sector, is there a single answer to that or—for a given problem, or does it depend on the size of the organization?

Ms. MOUSSOURIS. It depends on a number of factors. That's why we conduct maturity assessments, because an organization can be at a different maturity level for different areas of cybersecurity at a given time. Usually cybersecurity efforts are somewhere between the basement of compliance and the ceiling of whatever, you know, best practice trends were successfully marketed to the CISO (chief information security officer) of that organization. Whether or not those practices in between are effective at securing an organization, you know, it depends. And I've seen very large organizations struggle with maturity in vulnerability disclosure and coordination, for example, even when they are doing well in other areas of cybersecurity, so there are specializations and maturity changes over time. A recent study said that there were no magic bullets, no definitive correlations between certain best practices in cybersecurity and security outcomes.

Mr. CASTEN. OK. So the—my district is a lot of small suburban towns, and I get—I've recently been getting the question from a lot of the, you know, small municipal water utilities, who are saying that they're grappling with this issue. They've got, you know, diverse assets, and are starting to get concerned that they're not going to be able to get the cyber insurance they need to protect their assets because there's no credible way that they can provide that scope of maturity that you describe. Are there good models out there for organizations banding together to provide some kind of an umbrella security, right? Or does that create a security vulnerability of its own? So, you know, should I be recommending to all these municipals to say, you know, everybody pitch in your 20 percent to hire a, you know, a cybersecurity unit, or does that create more problems that we have to be mitigating——

Ms. MOUSSOURIS. Well, there may be some problems, you know, with having enough resources if you are relying on a single or very few shared resources, in terms of a shared cybersecurity team across some different organizations. But you also run into a—you know, a—sort of a single point of failure if that centralized security team is compromised in and of itself. And certainly all major orga-

nizations have been compromised at one point or another, and the adversaries do tend to go for, you know, highly valuable information systems, accounts, and leverage additional attacks from there. So aggregation may have some efficiencies gained, but it also may present an attack surface and a further overtasking of those resources.

Mr. CASTEN. Well, you've maybe perfectly teed up my final question for Dr. Herr, which is, I'm going to confess, wildly outside the jurisdiction of this Committee. My roommate in college senior year, his dad was a New York City beat cop for a long time, and he joked with me at one point that he had no idea why criminals ever committed anything but white collar crime, because the risk/reward for white collar crime was so much better than everything else. And the—and I share that story because if our enemies wanted to attack and take Rhode Island from us, there are a whole lot of rules around kinetic warfare. But if they wanted to steal all the data from J.P. Morgan, it's probably a lot more valuable, and there's a lot fewer rules. So, you know, we can put all these standards in place, but I'm curious, Dr. Herr, do we need something like a Geneva Convention for cyber warfare that we have for kinetic warfare?

Dr. HERR. I appreciate the question, sir, and as a native of Massachusetts, I suspect Rhode Island would be a tough fight. You know, I think the question that you ask about a broader geopolitical response is a good one. I think the Geneva Convention is a very bad model for what we talk about here for two reasons. One, the consequence scale of the events we're talking about on a daily basis do not come anywhere near close to—you know, to match the horrors of chemical warfare and nuclear conflict. The second, though, is that that sort of broad, you know, as much of the globe as possible kind of multi-stakeholder collaboration gets us to a point of very low accomplishment, right? We have as many people bought into a very small standard, a very little bit of progress, as possible, and I think, unfortunately, the cyber norms process has demonstrated that over the last decade.

Instead, I would suggest that our thought process for this is, rather than a negotiated settlement or a set of rules, how do we get more competitive? How do we—as we think about this not as trying to prevent a catastrophe, but more like improving our batting average, how do we get up to the plate and start taking more walks? How do we start hitting just a few more singles each time? And if that's about protecting some of these lower hanging fruit—some of these targets, or if that's just competing against many of these adversaries more effectively, I think that gets us to a place where we're able to keep J.P. Morgan and Rhode Island safely at home at night, where they need to be, and avoid any sort of catastrophe down the line.

Mr. CASTEN. Thank you so much, and I yield back.

Chairman FOSTER. Thank you, and we will now recognize Representative Ross for five minutes.

Ms. ROSS. Thank you so much, Mr. Chairman, and thank you also to Chairwoman Stevens, for holding this very crucial and timely meeting. I'm from North Carolina, so I want to let you know I represent the Research Triangle area of North Carolina, and we have a lot of tech companies there, including SASS, Red Hat,

Pendo, and the companies have a talent pipeline that comes through our colleges and universities. And, to Ms. Moussouris's issue of building this pipeline, we have a Secure Computing Institute at NC State University that has become a focal point for cybersecurity research, and at our community college, at Wake Tech Community College, we have a—it's been designated a National Center of Academic Excellence in Cyber Defense Education. So I think we need a field trip to my district. I just—I'm pitching that to the whole Committee.

And while I recognize that ransomware isn't the topic of this hearing, the Colonial Pipeline has come up several times, and, because it affected my district so acutely, I just wanted to ask in particular, Dr. Herr and Ms. Moussouris, had the requirements articulated in the May 12 Executive order been adopted by private industry, do you think the cyber attack on the Colonial Pipeline would've unfolded the way that it did?

Dr. HERR. I think there's no way to give a definitive answer, unfortunately, because much of the order, which is, I think, aspirational and positive in the direction that it's heading, is still to be decided, and it sets up processes and policy to be defined. But in—to your question, the focus on IT security, and on the security of software, certainly couldn't have hurt in the context of what Colonial faced.

Ms. MOUSSOURIS. I would say that the Colonial Pipeline attack allegedly occurred because of a phishing—a successful phishing attempt that was an administrator clicking on a link that they shouldn't have. Internal network segmentation, asset management requiring robust multi-factor authentication, may indeed have helped slow down the ransomware attack, however, ransomware is opportunistic. It is just a—you know, it's an opportunistic monetization of vulnerabilities that exist, so whether they are partly due to human error is one thing, but certainly network segmentation and multi-factor authentication tagged to specific assets may have helped mitigate it. It might not have completely eliminated the possibility of that attack taking place.

Ms. ROSS. OK. Thank you both. And, Mr. Scholl, your testimony talks about the National Cybersecurity Center of Excellence, which is a public/private partnership that works to address business cybersecurity challenges. And I wanted to know, has the private sector shown any interest in the NIST standards and best practices, and what can we do to get them more on board? Because they just keep—can't, you know, wait for something bad to happen, or say it costs too much. What can we do to make them more robust participants?

Mr. SCHOLL. So—yeah, thank you for the question.

Mr. BAIRD. I'm moving, so I have turned my video off.

Mr. SCHOLL. The private sector has shown great interest in NIST's work, in our—in the guidance that we've developed. This initially was seen in 2015, when we created the cybersecurity framework under a previous Executive order, which had outstanding participation from the private sector in its development. It—the cybersecurity framework, and all of NIST's work, is voluntary for use outside of the U.S. Government, so NIST is not a regulatory agency, nor do we wish to be one, but we find, because

of that, participation and use of our work on a voluntary basis does seem to be rather robust. As far as furthering that participation through other mechanisms, I'm actually not sure what would be good leverage in order to have that from the private sector.

Ms. ROSS. OK. Well, maybe we should explore that. If anybody has any ideas for good leverage—yes, Ms. Moussouris?

Ms. MOUSSOURIS. I think that, you know, adding Federal procurement guidelines, and leveraging the NIST framework, and requiring that companies that want to do business with the Federal Government comply with some of these NIST guidelines and standards is a good step in that direction.

Ms. ROSS. Thank you very much, and thank you, Mr. Chairman. I yield back.

Chairman FOSTER. And now, without objection, we will attempt to recognize Representative Baird, despite his having video problems right now. If his—the audio is working, I'm—Jim, are you available here?

Mr. BAIRD. I'm here. I'm here. Thank you.

Chairman FOSTER. OK. You're recognized for five minutes.

Mr. BAIRD. Thank you, sir, and good afternoon. And I really appreciate Chairwoman Stevens and Ranking Member Waltz of the Research and Technology Subcommittee, and Chairman Foster, I appreciate your efforts, and Ranking Member Obernolte, of the Investigations and Oversight Subcommittee for holding this important hearing over the SolarWinds incident.

So I guess my first question goes to Dr. Herr. In your testimony you point out that since 2010 there have been at least 30 different state-backed software supply chain attacks on the United States from states including Russia, China, North Korea, Iran, as well as others. So the United States is increasingly being targeted with cyber attacks as the nation-states are focusing on using cyber capabilities for malicious intent. As the scale of our cybersecurity posture is growing at a slower pace than emerging threats, how can the United States shore up our cybersecurity in order to protect our networks from our foreign adversaries?

Dr. HERR. Yes, sir, and I would point out only that those 30 attacks impacted a variety of countries, although the U.S. was certainly a leading part of that whole. I think there's a whole host of answers, and we could hold a number of hearings on the topic, but I'll give you two. The first is better combining the activities of our offensively focused organizations with those focused on defense.

The—part of the challenge that we face is where defense is rooted entirely on audits and compliance, it lacks the focus on where adversaries are attempting to push their own tactics, and their techniques, and their technologies. And so one of the failings that we recognized, and are reporting on Sunburst, is an inability for defenders to recognize software systems which were relatively small and innocuous, but incredibly value to—incredibly valuable to attackers, based on where they were placed on the network, or the permissions that they were granted. And so I think informing defenders with what offensive agencies—on a more regular basis, and trying to push that offensive mindset as defenders are choosing where to invest and prioritize, I think, is important.

But the second, and it's been mentioned a number of times today, is that, as we seek to improve our defensive posture, we have to push to automate as many of these activities as possible. There's a really good piece of work that's been done, I think it was—the term was coined by Wendy Nather of Cisco in 2011, the notion of the cyber poverty line. The majority of the organizations operating the technology that we care about, the potential targets of the next decade, don't have the resources or the internal maturity to operate at a high level of sophistication to make many of their own choices and judgments. They have the ability to plug things in, and hope for the best. And so what they plug in, and how they monitor it, has to be as capable as possible out of the box, and supported from as many directions as possible.

So I would come back and suggest to you that while we do have reasonable threats in these high consequence attacks, and have a lot of conversations to be had about what the U.S. is doing with allies outside of its borders, that at home a key part of our focus should be trying to resource and support, with technology that's as usable as possible, those folks that are most likely to be the target of these events.

Mr. BAIRD. Thank you. Dr. Foster, do I have any time left? I've got one more question for——

Chairman FOSTER. You have 1 minute and 45 seconds, and——

Mr. BAIRD. There we go, one minute——

Chairman FOSTER. 20 seconds——

Mr. BAIRD. 45——

Chairman FOSTER [continuing]. After that.

Mr. BAIRD. OK. So I have a joint question for Dr. Herr and Ms. Moussouris, and that is in the months since the SolarWinds incident it's become clear just how sophisticated this hack was, and, with some estimating, the operation involved over 1,000 engineers. States like Russia and China they can deploy the manpower to carry out an operation like this. So what actions need to be taken to ensure that the United States is capable of defending our networks at this scale? Dr. Herr, you want to start?

Dr. HERR. Sure. I'll say only that that 1,000 engineers number has come under significant, and I think fairly accurate, criticism. While there were likely a large number of people, perhaps more than 1,000, involved in processing all of the intelligence gathered in this operation, the number involved in actually building and maintaining the tools that targeted these U.S. Government agencies and private sector organizations was likely substantially smaller. What that suggests, though, is that manpower is not a good measure of impact, and I think we've seen that repeatedly in——

Mr. BAIRD. OK. Ms. Moussouris?

Ms. MOUSSOURIS. Absolutely agreed. The 1,000 engineers number, I believe, you know, was produced by Microsoft, and by their head lawyer, so I do not—I don't think that they're—that that number is realistic, in terms of what we're up against in that particular attack. I do think that our, you know, our numbers of people who can perform some of the most sophisticated attacks worldwide is actually a fairly small number. I can provide references after this hearing on the record for some of the labor market numbers that I and colleagues at MIT and Harvard had studied the

vulnerability economy and exploit market, and estimated some of those numbers worldwide.

So we are, you know, in the United States, obviously needing to create more of those elite cyber warriors to have the ability to create those types of attacks ourselves, but the number of them tends to be fairly small worldwide because the target gets harder and more sophisticated. The latest operating systems, the latest phone operating systems, get hardened further and further, and that enhances the technical needs and the bar to meet to carry out attacks of that sophistication level.

Mr. BAIRD. Thank you very much for those responses. I wish I had time to question the other witnesses, but I'm sure I'm out of time, so thank you, Dr. Foster, and I yield back.

Chairman FOSTER. Thank you. And—now, before bringing this hearing to a close, I want to thank our witnesses for testifying before the Committee. The record will remain open for two weeks for additional statements from the Members, and any additional questions the Committee may ask of the witnesses, and the hearing is now adjourned.

[Whereupon, at 3:45 p.m., the Subcommittee was adjourned.]

Appendix

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Trey Herr

Questions for the Record: Response from Dr. Trey Herr, Atlantic Council[1]

House Committee on Science, Space, and Technology Subcommittee on Investigations & Oversight Subcommittee on Research and Technology

"SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains."

Question 1. *How much of a risk to government networks is the governance and maintenance of commonly used open source software? What policy changes can help reduce the likelihood of, and what you call in your report calls the "blast radius" of security flaws in open source software? Is this an area where a significant government investment with dedicated full time personnel could make a difference?*

The security risks presented by the use of open source software (OSS) to government networks stem from the prevalence of OSS dependencies—a 2021 report sampled 1,546 codebases and found that 98 percent contained open source code.[2] Most proprietary code is, to some degree, dependent on, and at risk from, open source.

OSS is subject to many of the vulnerabilities as proprietary code, but it is often less visible, used as part of other software or depended on for a critical but opaque. The open, often distributed, and sometimes volunteer nature of open-source projects means OSS may come with less support and consistent maintenance than other proprietary software. This flexibility and ease with which important new software projects are created is part of what gives OSS tremendous, and responsive, innovative capacity.

OSS projects vary wildly in maturity, some are little more than small community projects like the 'ntpd' library (which synchronizes the system time of day in internet connected servers) while others are highly evolved endeavors with some commercial dimensions like the Ubuntu operating system. Many open-source projects lack centralized support and most do not have full time security personnel. In addition, the websites and online platforms where much OSS code is developed and stored, called repositories, may not follow best practices in notifying users of patches and updates.[3]

The widespread (and often nonobvious) reliance on open-source code, combined with its under-resourced security, can lead to highly impactful flaws, such as the Apache Struts vulnerability behind the Equifax breach and the widely reported Heartbleed vulnerability in OpenSSL.[4] The challenges in keeping up open-source security are known to the community—OSS projects are often understaffed and rely on volunteer service. The OpenSSL codebase, at half a million lines

---

[1] With assistance from Stewart Scott, Atlantic Council

[2] Synopsys, "2021 Open Source Security and Risk Analysis Report", *Synopsys*, April 13th, 2021, https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

[3] Trey Herr, William Loomis, June Lee, and Stewart Scott, *Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain, Atlantic Council*, July 27, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain.

[4] Timothy B. Lee, "The Heartbleed Bug, explained", *Vox*, May 14th, 2015, https://www.vox.com/2014/6/19/18076318/heartbleed

of code, was audited and reviewed by just one fulltime developer, prior to the discovery of Heartbleed, with voluntary and inconsistent support from others.[5]

OSS risk would be reduced with full time US Government cybersecurity personnel with budget and remit to focus exclusively on improving OSS supply chain and development security across this varied ecosystem. These personnel could help vendors of software designated what NIST defines as "EO-critical" outside the government and high-value asset program owners inside identify common OSS dependencies, encourage collaboration between the United States and allies in supporting the security of open-source projects identified as critical, and work with industry and regulators to target new security investments and requirements. Identifying these OSS dependencies would help map their potential blast radius if compromised, allowing for more targeted risk management efforts. Creating full time OSS security or risk management roles inside of the US Government, likely in multiple venues for example a small research and evangelism group at NIST supporting an operational security team at DHS CISA and a strategy role in the office of the National Cyber Director, would help improve the security of OSS and, critically, provide support for OSS projects to better utilize existing donations and volunteer time from industry.

These personnel should be supported with adequate financial resources to fund baseline security improvements in OSS identified as critical and better support common OSS community security efforts, on the order of $20 to $30 million dollars annually. Speaking to the Atlantic Council, two senior leaders at a major OSS governance and security non-profit stated plainly that their organization faces challenges from constrained resources and manpower, particularly for software development—many of their best programmers are hired away for exorbitant salaries at marquee software corporations, as are other developers at other open-source organizations. Funds appropriated by Congress for improvements in OSS security should be administered by an Executive branch entity, potentially DHS CISA in conjunction with NIST, and provided as both rolling application and as needed 'spot' grant funding to OSS projects. This administering organization should work with the Office of the National Cyber Director to obtain matching industry commitments and help magnify the public investment.

Open-source code was not at the heart of the Sunburst/SolarWinds crisis, but it is a critically underdefended attack vector in the software supply chain. Software supply-chain attacks since Sunburst show plainly that zeroing in on proprietary code simply because it was the vector in this case could court disaster.[6] Open-source software constitutes core infrastructure for major technology systems and critical software pipelines. For the federal government, risk in widely used internet services and common line of business applications stemming from OSS vulnerabilities is OSS risk to government networks and systems.

---

[5] Jose Pagliery, "Your Internet security relies on a few volunteers", *CNN*, April 18th, 2014, https://money.cnn.com/2014/04/18/technology/security/heartbleed-volunteers/index.html

[6] Dan Goodin, "New Type of Supply-chain Attack Hit Apple, Microsoft and 33 Other Companies", Ars Technica, February 16, 2021, https://arstechnica.com/information-technology/2021/02/supply-chain-attack-that-fooled-apple-and-microsoft-is-attracting-copycats/.

Question 2. *What additional tools or guidance can help improve the security of cloud solutions and multi-factor authentication adopted by the Federal government?*

The underlying security promise of cloud migration for federal government is the ability to, at scale, shift many of the burdens of cybersecurity away from unequally resourced organization and concentrate them with far better resourced cloud service providers with significant security and engineering talent. The ability for Sunburst/SolarWinds attackers to move laterally through systems built and operated by some of the largest of these vendors, including silently bypassing multi-factor authentication (MFA) systems, illustrates the challenges of successfully realizing these benefits and risk of such concentration without corresponding oversight.[7]

We suggest three lines of effort to improve the security of cloud solutions, along with MFA, sold to the US Government. First, NIST should be authorized and appropriately resourced to provide guidance on best practices and advise on standards relating to the secure design, adoption, and deployment of cloud services. Focusing too much on deployment and individual product security, where much of existing regulatory effort including the FedRAMP program, is concentrated risks architectural flaws deeper in provider's infrastructure and technology base. As efforts from the White House and elsewhere begin to more closely evaluate the security of cloud infrastructure, NIST should be empowered to support these engagements and resourced to do so effectively. Designing and operating cloud infrastructure remains a scarce knowledge base, held largely in proprietary industry silos. This can be addressed but it will take time and appropriate resources.

Second, supply chain security best practices, standards, and policies – especially those for EO-critical software – should be applied to appropriate cloud services. Exempting cloud computing from the laudable progress being made through the Software Bill of Materials effort and the NIST led development of software supply chain security policies would set the stage for frustration and high-consequence failures in the years to come, as cloud computing becomes the dominant form of widely used information technology. Cloud computing services are software, often complex and rather opaque chains of software. These services present as significant a portion of software supply chain risk as could be identified in any single software category.

Third, NIST and its partners must ensure the standards and guidance they release dealing with cloud computing and software supply chain security are automatable in common developer tools and software. The most significant barrier to adoption of best practices and security standards in cybersecurity is the challenge a user faces to interpret and apply these guidance documents. Where the target audience for a standard or best practice is a developer, the information contained in a PDF must also be available as part of a software tool or, better yet, made to integrate with existing widely used developer software. This relentless emphasis on automation will help drive adoption in vendors both large and small and help users overcome context specific roadblocks to certain best practices such as in National Security Systems.

---

[7] Trey Herr, William Loomis, Emma Schroeder, Stewart Scott, Simon Handler, and Tianjiu Zuo, "Broken Trust: Lessons from Sunburst", *Atlantic Council*, March 29th, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/

○