RESOURCING DHS'S CYBERSECURITY AND INNOVATION MISSIONS: A REVIEW OF THE FISCAL YEAR 2021 BUDGET REQUEST FOR THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY AND THE SCIENCE AND TECHNOLOGY DIRECTORATE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

MARCH 11, 2020

Serial No. 116–68

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

42–345 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida

MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, Texas

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

CEDRIC L. RICHMOND, Louisiana, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KATHLEEN M. RICE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
BENNIE G. THOMPSON, Mississippi *(ex officio)*

JOHN KATKO, New York, *Ranking Member*
MARK WALKER, North Carolina
MARK GREEN, Tennessee
JOHN JOYCE, Pennsylvania
MIKE ROGERS, Alabama *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
SARAH MOXLEY, *Minority Subcommittee Staff Director*

CONTENTS

RESOURCING DHS'S CYBERSECURITY AND INNOVATION MISSIONS: A REVIEW OF THE FISCAL YEAR 2021 BUDGET REQUEST FOR THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY AND THE SCIENCE AND TECHNOLOGY DIRECTORATE

Wednesday, March 11, 2020

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 11:05 a.m., in room 310, Cannon House Office Building, Hon. Cedric L. Richmond [Chairman of the subcommittee] presiding.

Present: Representatives Richmond, Thompson, Jackson Lee, Langevin, Rice, Underwood, Slotkin; Katko, Rogers, Walker, Green, and Joyce.

Mr. RICHMOND. Good morning. I would like to thank Director Krebs and Acting Deputy Under Secretary Hentz to discuss the fiscal year 2021 budget priorities for the Cybersecurity and Infrastructure Security Agency, CISA, and the Science and Technology Directorate, S&T.

Before I begin I would like to commend my colleague, Congressman Jim Langevin, for his work on the Cyberspace Solarium Commission.

The Solarium Commission's final report will be formally released hours from now, and I look forward to working with you and Chairman Thompson to codify important recommendations aimed at empowering CISA and better securing our elections.

I understand Director Krebs was very engaged in the cyberspace solarium. Toward that end, I will be interested in knowing if the fiscal year 2021 budget request from CISA is sufficient to implement the recommendations aimed at increasing CISA's capacity and, if not, what additional resources will be necessary.

At the outset I want to debunk the myth that the Federal agencies can do more with less. I support eliminating waste and increasing efficiency, but the fact is that with more you can do more.

Technology is evolving and creating opportunities for our adversaries to hack critical infrastructure, disrupt our elections, and hold State and local government networks hostage. CISA must be

equipped to be an effective Federal partner and S&T must be positioned to develop and identify technology to strengthen our defenses.

The President's fiscal year 2021 budget fails to do either of those important components. Last year committee Democrats led a bipartisan letter to appropriators seeking additional funding for CISA's cybersecurity mission. Together we succeeded in increasing CISA's cyber budget by $350 million, accelerating efforts to secure Federal networks, and ramping up CISA's threat analysis and response capabilities for private-sector critical infrastructure owners and operators and State and local governments.

Despite bipartisan support for an increase in CISA's cybersecurity budget, the President's budget cuts it by over $150 million. I don't understand how a cut of that magnitude makes communities trying to defend themselves against ransomware attacks, Federal networks, or critical lifeline services, from power to communications, any more secure.

Director Krebs, you know your mission. I want to know what resources you need to do it.

I would also like to express my concern about the administration's decision to eliminate the CFATS program. To the best of my knowledge, there is no intelligence that suggests that the security risk to chemical facilities has diminished. There is no evidence that a voluntary security framework will yield the same security results as a regulatory program. You can be certain that members of this committee will not allow CFATS to expire.

I am also concerned about the administration's continued efforts to cut S&T. Last fall this committee held a hearing exploring the security threats posed by emerging technologies. Despite ample evidence that U.S. investment in research and development is lacking, this budget cuts research and development for cybersecurity, as well as important university programs and centers of excellence. We cannot afford to continue to defer investments in R&D, and I will work hard to restore funding.

Before I close, I want to make clear my expectation that Members of this committee will receive accurate, candid intelligence about threats to our elections. Last month the intelligence community's assessment of whether the Russian Government's influence activities were intended to advance the President's re-election appeared to change overnight, because the President did not like the intelligence. As Members of Congress, we must have the information necessary to understand the threat and ensure you have budget and resources you need to defend against sophisticated cyber threats.

With that, I thank the witnesses for being here, and I yield back the balance of my time.

[The statement of Chairman Richmond follows:]

STATEMENT OF CHAIRMAN CEDRIC L. RICHMOND

MARCH 11, 2020

The Solarium Commission's final report will be formally released hours from now, and I look forward to working with you and Chairman Thompson to codify important recommendations aimed at empowering CISA and better securing our elections. I understand Director Krebs was very engaged in the Cyberspace Solarium.

Toward that end, I will be interested in knowing if the fiscal year 2021 budget request for CISA is sufficient to implement the recommendations aimed at increasing CISA's capacity and, if not, what additional resources will be necessary. At the outset, I want to debunk the myth that Federal agencies can do more with less. I support eliminating waste and increasing efficiency, but the fact is that with more you can do more.

Technology is evolving and creating opportunities for our adversaries to hack critical infrastructure, disrupt our elections, and hold State and local government networks hostage. CISA must be equipped to be an effective Federal partner and S&T must be positioned to develop and identify technology to strengthen our defenses. The President's fiscal year 2021 budget does fails both of these important components.

Last year, Committee Democrats led a bipartisan letter to appropriators seeking additional funding for CISA's cybersecurity mission. Together, we succeeded in increasing CISA's cyber budget by $350 million, accelerating efforts to secure Federal networks and ramping up CISA's threat analysis and response capabilities for private-sector critical infrastructure owners and operators and State and local governments.

Despite bipartisan support for increasing CISA's cybersecurity budget, the President's budget cuts it by about over $150 million. I don't understand how a cut of that magnitude makes communities trying to defend themselves against ransomware attacks, Federal networks, or critical lifeline services—from power to communications—any more secure.

Director Krebs, you know your mission. I want to know what resources you need to do it. I would also like to express my concern about the administration's decision to eliminate the CFATS program.

To the best of my knowledge, there is no intelligence that suggests that the security risks to chemical facilities has diminished. There is no evidence that a voluntary security framework will yield the same security results as a regulatory program.

You can be certain the Members of this committee will not allow CFATS to expire. I am also concerned about the administration's continued efforts to cut S&T.

Last fall, this committee held a hearing exploring the security threats posed by emerging technologies. Despite ample evidence that U.S. investment in research and development is lacking, this budget cuts R&D for cybersecurity as well as important University Programs and Centers of Excellence. We cannot afford to continue to defer investments in R&D, and I will work hard to restore funding.

Before I close, I want to make clear my expectation that Members of this committee will receive accurate, candid intelligence about threats to our elections. Last month, the intelligence community's assessment of whether the Russian government's influence activities were intended to advance the President's re-election appeared to change overnight because the President did not like the intelligence.

As Members of Congress, we must have the information necessary to understand the threat and ensure you have budget and resources you need to defend against sophisticated cyber threats.

Mr. RICHMOND. I would recognize the Ranking Member of the committee, Mr. Katko, for 5 minutes.

Mr. KATKO. Thank you, Mr. Chairman.

Thank you, Mr. Krebs, for being here. Thank you also for participating yesterday in the election security briefing. It was very helpful and informative and, as always, your input was well received.

I want to echo the sentiments of my colleague, the Chairman, about the cyber solarium and the work that has been done on it. I know you were an integral part of that, and I know Mr. Langevin has, as well. I look forward to a bipartisan effort implementing as many, if not all, of his policies into law and—on the Homeland side. Working closely with both sides now to get that done is, I think, critical.

Our Nation faces digital and physical threats daily that have the potential to disrupt, damage, and destroy their targets. These threats will only grow in magnitude, frequency, and sophistication in years ahead, as you well know, as cyber adversaries, particularly

nation-state actors, seek political, economic, and National security advantages.

The Federal Government works with public and private-sector partners to prevent and deter current threats, but also to plan for the future. The Cybersecurity Infrastructure Security Agency Act, or CISA, was tasked by Congress in 2018 to serve as the Nation's risk advisor, providing for the timely sharing of information, analysis, and assessment, and facilitating resilience building and mitigation in the .gov domain, State and local governments, and the private sector across industries.

Today we will take a closer look at CISA's plans and how they intend to carry out and achieve their mission. I must say I agree with Ms.—the chair. Cutting CISA's budget is not a really good idea at all. In fact, the opposite is true. We need to expand your resources so you can better handle the emerging threats.

CISA is responsible for securing the civilian Federal networks, monitoring emerging threats across sectors 24/7/365, securing our Nation's chemical facilities, advising State and local governments on election security, partnering with the public and private sector to protect soft targets in crowded places, and identifying and addressing risks to our National critical functions.

During the past year CISA completed its transition to a standalone agency subject to DHS oversight. I am very interested in hearing how strengthening CISA's authorities could further clarify civilian cybersecurity risk management authorities, and CISA's role as a convener of public-private partnerships.

As we have spoken in private, and in my office, and elsewhere, I am very interested in you telling us what else you need, and you know we will respond if you tell us what you need. I encourage you not to be shy about it, Mr. Krebs.

I look forward to hearing about CISA's plans to continue its progress securing our supply chain and tackling risk to our National critical functions and election infrastructure.

Finally, I invite you to share insights on CISA's work with State and local governments to secure the 2020 elections from the hindsight of Super Tuesday and other election primaries.

We will also hear from the Directorate of Science and Technology, or S&T, about how they plan to execute their mission in the year ahead. S&T, through partnerships with the Federal Government, academia, and industry, develops innovative solutions to aid the Department of Homeland Security in achieving its mission more effectively, efficiently, and affordably.

I look forward to hearing from both of our witnesses and my colleagues to see how we can work together—and the keyword is "together"—to ensure DHS is capable of protecting our Nation from digital and physical threats. This is the inherently bipartisan effort we are all involved in, and we should proceed in that manner.

With that I yield back.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

Thank you, Mr. Chairman, for holding this hearing, and thank you to our distinguished witnesses for being here today.

Our Nation faces digital and physical threats daily that have the potential to disrupt, damage, and destroy their targets. These threats will only grow in magnitude,

frequency, and sophistication in the years ahead as cyber adversaries particularly nation-state actors seek political, economic, and National security advantages.

The Federal Government works with public and private-sector partners to prevent and deter current threats, but also to plan for the future.

The Cybersecurity and Infrastructure Security Agency Act, or CISA, was tasked by Congress in 2018 to serve as the Nation's risk advisor, providing for the timely sharing of information, analysis, and assessment, and facilitating resilience building and mitigation in the .gov domain, State and local governments, and the private sector across industries.

Today we will take a closer look at CISA's plans and how they intend to carry out and achieve their mission.

CISA is responsible for: Securing the civilian Federal networks; monitoring emerging threats across sectors 24/7/365; securing our Nation's chemical facilities, advising State and local governments on election security; partnering with the public and private sector to protect soft targets and crowded places; and identifying and addressing risks to our National critical functions.

During the past year CISA completed its transition to a stand-alone agency subject to DHS oversight. I am interested in hearing how strengthening CISA's authorities could further clarify civilian cybersecurity risk management authorities and CISA's role as a convener of public-private partnerships.

I look forward to hearing about CISA's plans to continue its progress securing our supply chain and tackling risks to our National critical functions and election infrastructure.

Finally, I invite Director Krebs to share his insights on CISA's work with State and local governments to secure 2020 elections from the hindsight of Super Tuesday and other election primaries.

Today we also will hear from the Science & Technology Directorate, or S&T, about how they plan to execute their mission in the year ahead.

S&T, through partnerships within the Federal Government, academia, and industry, develops innovative solutions to aid the Department of Homeland Security in achieving its mission more effectively, efficiently, and affordably.

I look forward to hearing from both our witnesses and my colleagues to see how we can work together to ensure DHS is capable of protecting our Nation from digital and physical threats.

Mr. RICHMOND. The gentleman from New York yields back. I now recognize the Ranking Member of the full committee to give an opening statement.

Mr. Rogers.

Mr. ROGERS. Thank you, Mr. Chairman, and thank you for holding this important hearing. I want to thank the witnesses for being here, and taking the time to prepare for these hearings. I know it takes a lot of time, and that you have got other things to do, but we appreciate it. It is very helpful to us.

Today's threats can be cyber, or physical, or man-made, or natural. They can emerge from nation-states, criminal organizations, or terrorists. Just in the last 2 months we have dealt with cyber threats from Russia and Iran, ransomware attacks and disinformation campaigns on social media. These are the threats we know about. Many more may be lurking on the networks.

Unless we do something about it, these threats will only grow. CISA is the agency Congress created to do something about this. CISA's work is critical. That is why I was disappointed to see this year's budget request for the agency. I am very concerned that any cuts like this would undermine CISA's ability to successfully carry out its mission.

But I do take comfort in knowing, from my 18 years here, that the President only proposes budgets; we write budgets. I can tell you these cuts are not going to take place.

I look forward to hearing from Director Krebs on how he intends to mitigate the growing cybersecurity threats with a smaller budget, if that were to happen.

I also look forward to hearing from S&T on the important work it is doing to develop new technologies to defend our homeland.

[The statement of Ranking Member Rogers follows:]

STATEMENT OF RANKING MEMBER MIKE ROGERS

MARCH 11, 2020

Thank you, Mr. Chairman, for holding this hearing, and to our witnesses for being here today.

Today's threats can be cyber or physical, manmade or natural. They can emerge from nation-states, criminal organizations, and terrorists.

Just in the last 2 months, we've dealt with cyber threats from Russia and Iran, ransomware attacks, and disinformation campaigns on social media.

These are the threats we know about. Many more may be lurking on our networks.

Unless we do something about it, these threats will only grow.

CISA is the agency Congress created to do something about it.

CISA's work is critical.

That's why I was disappointed to see this year's budget request for the agency.

I'm very concerned these cuts will undermine CISA's ability to successfully carry out its critical mission.

I look forward to hearing from Director Krebs on how he intends to mitigate growing cybersecurity threats with a smaller budget.

I also look forward to hearing from S&T on the important works it's doing to develop new technologies to defend our homeland.

Mr. ROGERS. With that, Mr. Chairman, I yield back, and thank you.

Mr. RICHMOND. The gentleman yields back.

Other Members are reminded that statements may be submitted for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

MARCH 11, 2020

Around this time last year, this subcommittee held a hearing to discuss the fiscal year 2020 budget request.

At the time, Acting Secretary McAleenan had just replaced Secretary Nielson amid a flurry of leadership changes throughout the Department of Homeland Security.

Today you report to Acting Secretary Chad Wolf, the fifth person to serve as Secretary during this administration and the third to serve as Secretary since CISA became an operational component in November 2018. I have raised concerns about the lack of consistent leadership at the Department in the past, but I think it is particularly relevant in conversations about the future of CISA and S&T.

Both CISA and S&T play critical roles in defending the homeland. CISA is charged with coordinating the Federal efforts to defend critical infrastructure against physical and cyber attacks and protecting the .gov. S&T is responsible for putting cutting-edge technologies into the hands of DHS's boots on the ground to enable the workforce to do their jobs better and safer.

Despite their critical missions, neither of these agencies are without their challenges. CISA has been an operational component for less than 2 years.

As foreign adversaries increasingly rely on cyber tools to undermine our democratic institutions, surveil critical infrastructure networks, and hold State and local government networks hostage, Congress and the public have demanded more of CISA. But Trump administration has never provided Congress with a candid assessment of how much funding is necessary for CISA to accommodate the increased demands for its services. The White House has been without a White House cybersecurity coordinator for nearly 2 years, leaving Federal agencies to coordinate cybersecurity activities amongst themselves.

Although CISA's leadership has been steady and widely respected both within the Federal Government and among the private-sector stakeholder community, a strong, only a strong, Senate-confirmed Secretary can effectively advocate for CISA's budget need and policy positions at the White House.

In the absence of strong DHS leadership, the White House proposes to gut CISA's budget by over $250 million, cutting funding for cybersecurity activities and eliminating the Chemical Facility Anti-Terrorism Standards Program (CFATS).

As a Member of Congress with a number of chemical facilities in my Congressional District and a long-time advocate for ensuring chemical facilities across the Nation are not weaponized by terrorists, I was particularly troubled to learn the administration supports eliminating the program.

I believe that if DHS had a permanent Secretary in place, the White House would not have proposed eliminating the program. Accordingly, on Monday, I introduced legislation to extend the CFATS program for 18 months, and I expect CISA to support that effort. I would also note that the lack of consistent leadership at DHS has similarly undermined S&T's mission.

The Science and Technology Directorate has been victim of too many "course corrections" to count and has struggled to solidify its position as the research and development hub among DHS's components.

Moreover, its budget is most frequently raided to pay for the President's political promises or to cut spending in order to comply to budget caps. The President's fiscal year 2021 budget request is no different—reducing cyber R&D and cutting University Programs in half.

We cannot continue to defer investments in R&D for homeland security technologies. A permanent Secretary would understand that. I will not ask either of you to explain how these proposed cuts will make us safer because they will not. Instead, I hope that you will be frank with Congress about the resources you need to do your jobs.

Mr. RICHMOND. Let me welcome our panel of witnesses.

First I would like to welcome Chris Krebs, the director of the DHS Cybersecurity and Infrastructure Security Agency, back to testify before this panel.

Director Krebs has been at the helm of DHS's cybersecurity activity since 2017, and he has been an integral player in shaping and developing the Department's election security capabilities.

Next we have Mr. Andre Hentz. He is the acting deputy under secretary for science and technology. Deputy Under Secretary Hentz has been with S&T since 2014, and in his current role since 2017.

Without objection, the witnesses' full statements will be inserted into the record.

I now ask each witness to summarize his or her statement for 5 minutes, beginning with Dr. Krebs—Director Krebs, I am sorry.

Mr. KREBS. I will take doctor.

Mr. RICHMOND. I made you a doctor overnight.

[Laughter.]

STATEMENT OF CHRISTOPHER C. KREBS, DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KREBS. Chairman Richmond, Ranking Member Rogers, Ranking Member Katko, and Members of the subcommittee.

Happy Cyberspace Solarium Report Rollout Day. Congressman Langevin, thanks for all your efforts there, and thank you for recognizing the significance and importance of CISA in the broader National cybersecurity efforts. So thank you for that. Thank you for today's opportunity to address the Cybersecurity and Infrastructure Security Agency's—CISA's—fiscal year 2021 budget.

The 2021 budget provides meaningful investment in CISA's ability to lead the National effort to safeguard and secure critical infrastructure from cyber and physical threats. To accomplish this mission, we must work with our partners where they are, not where

we are. Accordingly, this budget invests an additional field-based personnel that are located outside the D.C. Beltway, where our partners are found.

My statement focuses on each of our priorities: Protection of Federal networks; election infrastructure security; securing operational technology; supply chain risk management; and soft target security.

First, with Federal cybersecurity, across the Federal Government our ability to defend networks has improved. The budget will help CISA establish a cybersecurity shared services offering that will centralize, standardize, and deliver best-in-class cybersecurity capabilities to Federal agencies. Through this effort CISA will develop service standards, evaluate individual offerings, and oversee a marketplace of qualified cybersecurity services for Federal customers.

We must also invest in our people. CISA is leading a Government-wide training program for all Federal cybersecurity professionals. This includes a rotational program, training program, and re-skilling academy. Training cybersecurity professionals is a crucial part of closing the gap on workforce demands for CISA and across our Government.

But perhaps the most high-profile threat today is attempts by nation-state actors to interfere in our elections. Over the last several years, as you heard yesterday, we have been—become close partners with the election community, and we are focusing on broadening the reach and depth of assistance, emphasizing the criticality of election audit ability, prioritizing the need to patch vulnerabilities in election systems, and developing locality-specific cybersecurity profiles that officials can use to manage risk.

Also, we are focusing on operational technologies or control systems, those components that operate our critical infrastructure. The increasing integration and connectivity of those technologies has vastly increased the potential impact of cyber threats. Included in this year's budget is funding to expand our control system security efforts, including sensing analytics and partner training platforms.

We are also investing in our efforts to understand and manage supply chain security risks. CISA's Supply Chain Risk Management Task Force has brought together 20 Federal agencies and 20 of the largest companies in information communications sectors to reach consensus on how to best manage risk. We are not using—rather, we are using this forum to understand what is working and what is not, sharing best practices and crowd-sourcing solutions to close out supply chain risk management gaps.

At CISA we also recognize that far too often our Nation is confronted with violent attacks on places such as entertainment venues, places of worship, and schools. Funding in this budget to support CISA's school safety initiatives, including stewardship of the Federal School Safety Clearinghouse, a one-stop shop for local officials to find resources that help provide children with a safe learning environment.

Before closing, research and development is critical to CISA's mission. CISA and S&T are committed to effective coordination. We are partnering to advance threat-driven cyber analytics and devel-

opment of a cyber risk framework. This project is an important first step in the larger plan to enhance analytics in conjunction with big data and machine learning.

In closing, I would like to briefly touch on my keys to success for CISA in 2020. Those keys to success are threefold: First, we must continue focusing on our strengths; second, we must seek strategic alignment with our interagency partners, not compete with them; and third, we must be a customer-centric organization.

So what are our strengths? Convening, bringing a broad range of partners together to tackle tough challenges, sharing actionable information, and collectively identifying best practices for areas like Federal and State and local cybersecurity and soft target security.

Who must we align with? Our partners in the intelligence community and law enforcement, the Department of Defense, and elsewhere in the civilian government. This is crucial, if we are going to be successful, for instance, in election security, as well as control systems.

Last, if we are not intensely focused on our customers, we are doing it wrong. We must continue to push—to support out across this great Nation and help infrastructure partners big and small. Ransomware is the perfect example of how we must become a customer-centric organization.

So with that, thank you for the opportunity to be here today. Thank you for your prior investments at CISA. I look forward to discussing this year's budget, and I look forward to your questions.

[The prepared statement of Mr. Krebs follows:]

PREPARED STATEMENT OF CHRISTOPHER C. KREBS

MARCH 11, 2020

Good afternoon Chairman Richmond, Ranking Member Katko, and distinguished Members of the subcommittee, thank you for the opportunity to testify regarding the fiscal year 2021 President's budget for the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The fiscal year 2021 President's budget of $1.78 billion for CISA reflects our commitment to safeguard our homeland, our values, and our way of life.

CISA strengthens the cybersecurity of Federal networks and increases the security and resilience of our Nation's critical infrastructure. Safeguarding and securing critical infrastructure is a core DHS mission. The fiscal year 2021 President's budget recognizes the criticality of this mission and ensures the men and women of CISA have the resources they need to achieve it.

CISA's defends the homeland against the threats of today, while working with partners across all levels of government and the private sector to secure against the evolving risks of tomorrow—"Defend Today, Secure Tomorrow."

As the Nation's risk advisor, CISA is a hub of efforts to build National resilience against a growing and interconnected array of threats; organizing risk management efforts around securing the National Critical Functions that underpin National security, economic growth, and public health and safety; and ensuring Government continuity of operations. CISA marshals its wide-ranging domain expertise and central coordination role to guide partners in navigating hazards ranging from extreme weather and terrorism to violent crime and malicious cyber activity. We identify high-impact, long-term solutions to mobilize a collective defense of the Nation's critical infrastructure.

The fiscal year 2021 President's budget for CISA has been reorganized under new budget lines to fully reflect the operational vision for CISA. The CISA Act of 2018 reorganized the National Protection and Programs Directorate into an operational component, and the budget should reflect the new organization. For instance, management and operational watch activities that were previously spread across multiple budget lines are now merged into a single funding line that will serve as a nexus of cyber, physical, and communications integration. The new funding lines also combine all regional field operations, including Protective Security Advisors and

Cybersecurity Advisors, into a single report channel. This enhances the ability of CISA to engage with critical infrastructure partners outside the beltway, where they are located. If adopted, this new structure will streamline authority, increase transparency, and better enable CISA to execute the funding.

CISA PRIORITIES

Nefarious actors want to disrupt our way of life. Many are inciting chaos, instability, and violence. At the same time, the pace of innovation, our hyper connectivity, and our digital dependence has opened cracks in our defenses, creating new vectors through which our enemies and adversaries can strike us. This is a volatile combination, resulting in a world where threats are more numerous, more widely distributed, highly networked, increasingly adaptive, and incredibly difficult to root out.

CISA is strengthening our digital defense as cybersecurity threats grow in scope and severity. The fiscal year 2021 President's budget continues investments in Federal network protection, proactive cyber protection, infrastructure security, reliable emergency communications for first responders, and supply chain risk management.

CISA, our Government partners, and the private sector, are all engaging in a more strategic and unified approach toward improving our Nation's defensive posture against malicious cyber activity. In May 2018, DHS published the Department-wide *DHS Cybersecurity Strategy,* outlining a strategic framework to execute our cybersecurity responsibilities during the next 5 years. Both the Strategy and *Presidential Policy Directive 21—Critical Infrastructure Security and Resilience* emphasize an integrated approach to managing risk.

CISA ensures the timely sharing of information, analysis, and assessments to build resilience and mitigate risk from cyber and physical threats to infrastructure. CISA's partners include intergovernmental partners, the private sector, and the public. Our approach is fundamentally one of partnerships and empowerment, and it is prioritized by our comprehensive understanding of the risk environment and the corresponding needs of our stakeholders. We help organizations manage their risk better.

The fiscal year 2021 President's budget includes $1.1 billion for cybersecurity initiatives at CISA to detect, analyze, mitigate, and respond to cybersecurity threats. We share cybersecurity risk mitigation information with Government and non-Government partners. By issuing guidance or directives to Federal agencies, providing tools and services to all partners, and leading or assisting the implementation of cross-Government cybersecurity initiatives, we are protecting Government and critical infrastructure networks.

Within the cybersecurity initiatives funding amount, the fiscal year 2021 President's budget includes $660 million for cybersecurity technology and services, including Continuous Diagnostics and Mitigation (CDM) and National Cybersecurity Protection System (NCPS) programs. These programs provide the technological foundation to secure and defend the Federal Government's information technology against advanced cyber threats.

NCPS is an integrated system-of-systems that delivers intrusion detection and prevention, analytics, and information-sharing capabilities. NCPS primarily protects traffic flowing into and out of Federal networks. One of its key technologies is the EINSTEIN intrusion detection and prevention sensor set. This technology provides the Federal Government with an early warning system, improves situational awareness of intrusion threats, and near-real time detection and prevention of malicious cyber activity. Funding included in the budget will allow NCPS to begin transitioning capabilities to use commercial and Government cloud services to the greatest extent possible. The funding will also support newly-developed information sharing and intrusion prevention capabilities into the operational environment.

CDM provides Federal network defenders with a common set of capabilities and tools they can use to identify cybersecurity risks within their networks, prioritize based on potential impact, and mitigate the most significant risks first. The program provides Federal agencies with a risk-based and cost-effective approach to mitigating cyber risks inside their networks. The fiscal year 2021 President's budget includes funding to continue deployment and operation of necessary tools and services for all phases of the CDM program. Funding will cover completion of activities to strengthen management of information technology assets including for cloud and mobile-based assets and protection of data on networks that carry highly-sensitive and critical information. By pooling requirements across the Federal space, CISA is able to provide agencies with flexible and cost-effective options to mitigate cybersecurity risks and secure their networks.

Funding for cybersecurity initiatives also includes $408 million for cybersecurity operations. Within this category, approximately $264 million is dedicated to threat hunting and vulnerability management operations. Threat hunting activity identify, analyze, and address significant cyber threats across all domains through detection activities, countermeasures development, as well as hunt and incident response services. Vulnerability management capabilities include assessments and technical services, such as vulnerability scanning and testing, penetration testing, phishing assessments, and red teaming on operational technology that includes the industrial control systems which operate our Nation's critical infrastructure, as well as recommended remediation and mitigation techniques that improve the cybersecurity posture of our Nation's critical infrastructure.

The budget includes funding to support CyberSentry. This voluntary program is designed to detect malicious activity on private-sector critical infrastructure networks, including operational technology, such as industrial control systems. The pilot will utilize network sensor systems to detect threats; collect threat data; increase the speed of information sharing; and produce real-time, effective, actionable information to the companies vulnerable to malicious attacks.

Funding is also included to support cybersecurity capacity building. Capacity building is delivering tools and services to stakeholders to strengthen cyber defenses and coordinating policy and governance efforts to carry out CISA's statutory responsibility to administer the implementation of cybersecurity policies and practices across the Federal Government. The budget provides funding for a cybersecurity shared services office that will centralize, standardize, and deliver best-in-class cybersecurity capabilities to Federal agencies. Through this effort, CISA will develop service standards, evaluate individual offerings, and oversee a marketplace of qualified cybersecurity services to Federal customers.

Through this budget, CISA will lead a Government-wide cybersecurity training program for all Federal cybersecurity professionals, including an interagency cyber rotational program, a cybersecurity training program, and a cyber-reskilling academy. Training cybersecurity professionals will be a crucial part of closing the gap on workforce demands for CISA and across Government. This effort also includes funding for CISA to continue hosting the annual President's Cup Challenge, a cyber competition to test the skills of the Federal cyber workforce.

The fiscal year 2021 President's budget request also includes funding for State and local Government cybersecurity and infrastructure assistance prioritized for election security. These resources are institutionalizing and maturing CISA's election security risk-reduction efforts, allowing the agency to continue providing vulnerability management services such as cyber hygiene scans, and on-site or remote risk and vulnerability assessments, organizational cybersecurity assessments, proactive adversary hunt operations; and enhanced threat information sharing with State and local election officials.

For infrastructure security, the fiscal year 2021 President's budget includes $96 million for protecting critical infrastructure from physical threats through informed security decision making by owners and operators of critical infrastructure. Activities include conducting vulnerability and consequence assessments, facilitating exercises, and providing training and technical assistance Nation-wide. The program leads and coordinates National efforts on critical infrastructure security and resilience by developing strong and trusted partnerships across the Government and private sector. This includes reducing the risk of a successful attack on soft targets and crowded places, from emerging threats such as unmanned aircraft systems. Funding supports CISA's school safety initiatives, including stewardship of the Federal School Safety Clearinghouse, the expansion of existing school security activities, and the development of additional resources and materials for safety to provide children with a safe and secure learning environment.

This year's budget eliminated funding for the Chemical Facilities Anti-Terrorism Standards program while simultaneously increasing funding significantly for the Protective Security Advisors program. This will allow CISA to provide voluntary support for chemical facilities without the unnecessary burden of regulatory requirements, placing the chemical sector on par with all the other critical infrastructure sectors for which CISA has oversight.

The fiscal year 2012 President's budget includes $158 million for emergency communications to ensure real-time information sharing among first responders during all threats and hazards. CISA enhances public safety interoperable communications at all levels of Government across the country through training, coordination, tools, and guidance. We lead the development of the National Emergency Communications Plan to maximize the use of all communications capabilities available to emergency responders—voice, video, and data—and ensures the security of data and information exchange. CISA supports funding, sustainment, and grant programs to advance

communications interoperability, such as developing annual SAFECOM Grant Guidance in partnership with Public Safety stakeholders, and partnering with FEMA Grants Program Directorate to serve as communications subject-matter experts for FEMA-administered grants. We assist emergency responders and relevant Government officials with communicating over commercial networks during natural disasters, acts of terrorism, and other man-made disasters through funding, sustainment, and grant programs to support communications interoperability and builds capacity with Federal, State, local, Tribal, and territorial stakeholders by providing technical assistance, training, resources, and guidance. The program also provides priority telecommunications services over commercial networks to enable National security and emergency preparedness personnel to communicate during telecommunications congestion scenarios across the Nation.

The President's budget includes $167 for the Integrated Operations Division. This division is charged with coordinating CISA's front line, externally facing activities in order to provide seamless support and an expedited response to critical needs. These funds include $82 million to support 373 protective security advisors and cybersecurity advisors located across the country. Protective Security Advisors conduct proactive engagement and outreach with Government at all levels and critical infrastructure. Additionally, cybersecurity advisors expand the DHS cyber field presence across the country. These resources better enable CISA to reach critical infrastructure partners and other stakeholders where they live outside the beltway.

The fiscal year 2021 President's budget fully funds CISA's risk management activities, including $91.5 million for the National Risk Management Center (NRMC). The NRMC is a planning, analysis, and collaboration center working to identify and address the most significant risks to our Nation's critical infrastructure. The NRMC also houses the National Infrastructure Simulation and Analysis Center (NISAC), which provides homeland security decision makers with timely, relevant, high-quality analysis of cyber and physical risks to critical infrastructure across all sectors during steady state and crisis action operations. Increased funding will support election security, securing 5G telecommunications, and supply chain risk analysis.

The new Stakeholder Engagement and Requirements program is funded at $38 million. This funding will support the coordination and stewardship of the full range of CISA stakeholder relationships; the operation and maintenance of the CISA stakeholder relationships; the operation and maintenance of the CISA stakeholder relationship management system; the implementation of the National Infrastructure Protection Plan voluntary partnership framework; the management and oversight of National infrastructure leadership councils; and the effective coordination among the National critical infrastructure stakeholder community in furtherance of shared goals and objectives.

The President's budget asks for $24 million within the Science and Technology Directorate (S&T) to continue research and development efforts in support of CISA's cybersecurity mission. CISA and S&T have made tremendous strides in collaborating to advance joint priorities. In fiscal year 2019, CISA and S&T awarded a project to create a 'pipeline' for low technology readiness-level efforts to mature and transition into CISA. Workstreams in this pipeline are advancing threat-driven cyber analytics and development of a cyber risk framework. This project is an important first step in the larger plan for CISA and S&T to enhance analytics in conjunction with big data and machine learning. Subsequent efforts in fiscal year 2020 and beyond are planned to leverage hyperscale cloud platforms and significantly advance the data and analytics capabilities of CISA.

Finally, Congress provided a substantial investment last year to consolidate CISA in a new state-of-the-art headquarters facility at DHS's St. Elizabeth's Campus. CISA currently must operate from 8 different leased locations spread across the National Capital Region, in facilities not capable of fully supporting CISA operational demands, which contributes to administrative inefficiencies. The fiscal year 2021 President's budget provides $459 million to the General Services Administration for the continued consolidation of DHS facilities at the St. Elizabeth's Campus. Included in this amount are funds for both additional DHS component building construction and also campus infrastructure enhancements, such as additional parking, that are critical to the success of CISA's future relocation to the campus.

CONCLUSION

In the face of increasingly sophisticated threats, CISA employees stand on the front lines of the Federal Government's efforts to defend our Nation's Federal networks and critical infrastructure. The threat environment is complex and dynamic with interdependencies that add to the challenge. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation.

CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies.

I recognize and appreciate this committee's strong support and diligence as it works to resource CISA in order to fulfill our mission. Your support over the past few years has helped bring additional Federal departments and agencies into NCPS more quickly, speed deployment of CDM tools and capabilities, and build out our election security efforts. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient homeland while also being faithful stewards of the American taxpayer's dollars.

Thank you for the opportunity to appear before the subcommittee today, and I look forward to your questions.

Mr. RICHMOND. Thank you, Director.

I now recognize Acting Deputy Under Secretary Hentz to summarize his statement for 5 minutes.

STATEMENT OF ANDRE HENTZ, ACTING DEPUTY UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HENTZ. Good afternoon, Chairman Richmond, Ranking Member Katko, Ranking Member Rogers, and distinguished Members of the subcommittee. Thank you for inviting me here today to testify on the President's budget for fiscal year 2021, which includes a request for $643 million for the Science and Technology Directorate within the Department of Homeland Security.

S&T's research develops activities which support a broad range of DHS missions, including domain threat awareness, delivery of mitigation strategies, and creating novel technologies and approaches for the components, first responders, and other partners across the Homeland Security enterprise.

Our customers put their lives on the line every day to keep our Nation safe. Having the correct tools, techniques, and/or technologies can be vital to the operational safety and success.

Research and development must enable efficient, effective, and secure operations across all DHS security missions by applying timely, scientific, engineering, and innovation solutions. This is how S&T delivers results. Technology innovation cycles are rapidly changing, and the nature of the threats we see are dynamic.

It is important to note, however, that S&T represents less than one-half of 1 percent of the entire Federal R&D budget. Let me repeat that: S&T represents less than one-half of 1 percent of the entire Federal research and development budget, and we strive every day to get as much value out of those funds as possible.

Under my leadership, with Mr. Bryan, S&T has strengthened our relationship with our customers by providing impactful solutions to those on the front line. We continue to solidify and strengthen S&T's core capabilities and provide deliberative approaches to program execution that ensures timely delivery and solid returns on investment for our Nation's taxpayers.

The fiscal year 2021 request includes $5 million for quantum information sciences, including artificial intelligence. S&T is beginning to focus on machine learning, with the goal of mitigating risk to potential misuse of artificial intelligence, and identifying opportunities and applications for the use of trustworthy artificial intelligence, while providing privacy protection and developing new governance and policy frameworks for artificial intelligence and machine learning.

The fiscal year 2021 budget request provides $14.3 million for S&T's Probabilistic Analysis for National Threats, Hazards, and Risk program, known as PANTHR. PANTHR aligns S&T's chemical and biological hazard awareness and characterization activities to provide timely, accurate, and defensible decision support tools and knowledge to stakeholders. Working with the Countering Weapons of Mass Destruction Directorate, PANTHR is leveraging S&T's National Biodefense Analysis and Countermeasures Center to address pertinent scientific questions and DHS operational concerns regarding the surface stability and decontamination of COVID–19. Funding in 2021 would allow PANTHR to develop additional assessment capabilities to address growing infrastructure concerns such as the bio-economy, and fill other critical gaps regarding weapons of mass destruction risks to the homeland.

The administration is also focusing on targeted violence and terrorism prevention, and S&T's 2021 requests includes $7 million for research to inform policy, strategy, tactics, techniques, and procedures in this area. S&T is actively working to support technology integration and techniques to reduce the likelihood of mass violence and improve the ability to prevent and respond to a mass violent event.

The fiscal year 2021 budget request supports S&T's Office of University Programs in two vital efforts, our centers of excellence and working with minority-serving institutions. Centers of excellence that receive funding in fiscal year 2021 will conduct research and development that aligns with the administration's priorities to strengthen border security, cybersecurity, infrastructure protection, and prioritize transnational criminal investigations.

Finally, the 2021 budget requests at $18.9 million in a procurement, construction, and investment account for S&T to begin to address the decontamination and closure of the Plum Island Animal Disease Center. S&T is committed to our mission to deliver effective, innovative insights, methods, and solutions for critical needs of DHS components, first responders, and our operational partners in the Homeland Security space.

Chairman Richmond, Ranking Member Katko, Ranking Member Rogers, and Members of the committee, thank you again for the opportunity to appear before you today, and for your continued support of S&T. I look forward to answering your questions.

[The prepared statement of Mr. Bryan, as presented by Mr. Hentz, follows:]

PREPARED STATEMENT OF WILLIAM BRYAN

MARCH 11, 2020

Good afternoon Chairman Richmond, Ranking Member Katko, and distinguished Members of the subcommittee. Thank you for inviting me here today to testify on the President's budget request for fiscal year 2021, which includes a request of $643.7 million for the Science and Technology Directorate (S&T) within the U.S. Department of Homeland Security (DHS).

S&T's research and development (R&D) activities support a broad range of DHS missions, including domain threat awareness, delivering mitigation strategies, and creating novel technology and approaches for the components, first responders, and other partners across the homeland security enterprise. Our customers put their lives on the line every day to keep our Nation safe, and having the correct tools, techniques, and/or technologies can be vital to the operators' safety and success.

We must enable efficient, effective, and secure operations across all homeland security missions by applying timely scientific, engineering, and innovative solutions through research, design, test and evaluation, and acquisition support. This is how S&T delivers results. Technology innovation cycles are rapidly changing and the nature of the threats we see is dynamic. This combination presents a significant challenge to traditional R&D approaches as well as meeting component requirements and needs in a fiscally constrained R&D environment. S&T is less than 1 percent of the entire Federal R&D budget—and we strive every day to get as much value out of those funds as possible.

Therefore, it is my responsibility to ensure an efficient, effective, and nimble organization is in place to address R&D needs of Homeland Security front-line operators, particularly the DHS operational components and first responders, today and into the future. Either through the identification of existing technologies or the timely development of new technology, S&T can provide them with the tools they need to safely and effectively protect the homeland and the American people. Under my leadership S&T has strengthened our relationships with our customers, the DHS operational components and first responders, to provide impactful solutions to those on the front line. We continue to solidify and strengthen S&T's core capabilities and provide a deliberative approach to program execution that ensures timely delivery and solid return on investment for our Nation's taxpayers.

S&T has become more agile and responsive, ready to move quickly in response to changes in the threat environment, and makes use of existing technologies, when available, that can be adapted and leveraged to expedite the development of vital capabilities. S&T has significantly enhanced its ability to transfer capabilities to where they are most needed by working closely with operators, component partners, and industry to deliver effective solutions. The revitalized S&T has strengthened its relationships with DHS components, first responders, and other customers, and results in a more integrated approach to innovation, requirements gathering, and problem solving. At a strategic level, S&T has created a capability to identify, prioritize, and report on emerging technology risks facing the United States. Together with DHS Policy, S&T will identify and assess emerging technologies most likely to significantly improve operations and/or threaten the DHS mission over the next 2–5 years. Results will support senior DHS executives as they prioritize the list of technologies and shape the DHS investment portfolio to address risk.

A strong cross-Department cybersecurity R&D program is critical for DHS. The Cyber Security & Infrastructure Security Agency (CISA) and S&T have made tremendous strides in resetting the relationship, directing R&D resources into mission support of CISA requirements. CISA and S&T have established repeatable processes to identify capability gaps, prioritize needs, and execute on RD&I needs. The fiscal year 2021 cybersecurity R&D budget request is for $24 million and places all cyber R&D funding with S&T.

S&T is currently partnered with the National Institutes of Artificial Intelligence (AI) with the goal of mitigating risks to misuse of AI, identifying opportunities and applications of AI within the homeland security mission space, improving privacy protection, and developing new governance and policy frameworks for artificial intelligence and machine learning. S&T is working with its operational DHS component partners to assess opportunities for leveraging Automated Machine Learning (AutoML) and related data preparation tools as a means of accelerating understanding and use of this technology within the DHS enterprise. In fiscal year 2021, S&T will examine and characterize the state of artificial intelligence research relative to future homeland security mission applications. Research activities will focus on the development of core capabilities that enable trustworthy artificial intelligence to improve core automation capabilities that are secure, private, and trusted for critical homeland security applications.

The fiscal year 2021 budget request provides $14.4 million for S&T's Probabilistic Analysis for National Threats Hazards and Risks (PANTHR) program that aligns S&T's chemical and biological hazard awareness and characterization activities to provide timely accurate and defensible decision support tools and knowledge to stakeholders. PANTHR is currently supporting the Countering Weapons of Mass Destruction Office (CWMD) to address the on-going Coronavirus outbreak by providing consolidated up-to-date information regarding the virus to DHS components. PANTHR is currently leveraging the capabilities of one of the DHS laboratories, the National Biodefense Analysis and Countermeasure Center (NBACC), which is addressing pertinent scientific questions and DHS operational concerns regarding Coronavirus surface stability and decontamination. PANTHR funding in fiscal year 2021 would further support the expansion of these National capabilities to address current and emerging chemical and biological concerns. Additionally, the fiscal year 2021 request would allow PANTHR to develop additional assessment capabilities to

address growing infrastructure concerns, such as the bio-economy, and fill other critical technical hazard data gaps regarding WMD risks to the Homeland.

S&T is requesting $35.9 million in the fiscal year 2021 budget to directly address Customs and Border Protection (CBP), the U.S. Coast Guard (USCG), the U.S. Secret Service (USSS), and the Federal Protective Service (FPS) requirements for Countering Unmanned Aircraft System (CUAS) requirements. In close coordination with our operational customers, S&T is responsible for the initial CUAS deployment architecture, technology selection, system integration, system test, training and cyber compliance. The fiscal year 2021 S&T CUAS investment will focus on mission interoperability with the Department of Defense and Department of Justice in the National Capital Region, improved CUAS capabilities for DHS components, and addressing future threats. UAS threats to critical infrastructure and security activities will likely increase in the near future as the number of UAS introduced into the National airspace continues to increase. However, currently the use of technical means to detect, track, and disrupt malicious UAS operations remains limited.

S&T is dedicated to developing or adopting innovative tools for DHS components, and the fiscal year 2021 budget request supports that effort. For example, the S&T Opioid Detection project continues to integrate advanced technologies, including narcotics anomaly detection algorithms and chemical sensing technologies, into CBP international mail facilities, and to evolve efforts directed at detecting synthetic opioids in additional operational environments in response to changing trafficking dynamics. Increased funding will also further improve the understanding of supply chain logistics and intelligence to aid in targeting, investigations, and ultimately, disruption of international smuggling. The administration is also focusing on Targeted Violence and Terrorism Prevention, and S&T is a vital partner using research to inform policy, strategy, tactics, techniques, and procedures. S&T is actively working to support technology integration and techniques to reduce the likelihood of mass violence and improve the ability to prevent and respond to a mass violence event.

The fiscal year 2021 request continues support for S&T's Silicon Valley Innovation Program (SVIP) at $10 million, which leverages innovative commercial capabilities from across the country through non-traditional Government contractors to rapidly deliver technology to fulfill DHS component-defined requirements. This program fosters rapid development and delivers tested technology into the field in a much shorter time frame than is possible under traditional vehicles. S&T's SVIP collaborates with DHS operational components to provide solutions that enhance overall situational awareness, detection, tracking, interdiction, and apprehension.

To date, S&T's SVIP has awarded $18 million in funding and processed over 485 applications across 14 topic areas. S&T has worked with 49 small start-up companies from 15 different States and leveraged over $500 million in private-sector investment that aligns on-going private-sector activity with DHS operational component requirements. SVIP has successfully transitioned 3 technologies into CBP operational environments including a new generation of radar to support U.S. Border Patrol operations. This radar technology was incorporated into 58 Border Patrol towers on the Southwest Border and a similar amount are planned for transition in 2020.

The fiscal year 2021 budget request adds a Procurement, Construction, and Improvements account to address the decontamination and closure of the Plum Island Animal Disease Center. S&T is on time and on budget to complete the construction of the National Bio and Agro-Defense Facility (NBAF). This state-of-the-art facility will be transferred to the U.S. Department of Agriculture upon completion of construction and will be the Nation's only Bio Safety Level 4 laboratory that is capable of studying large animal diseases in livestock, such as African Swine Fever and Foot and Mouth Disease. After NBAF is completed, the Plum Island facility will require decontamination. The $18.9 million of the fiscal year 2021 request will begin decontamination activities and stand up the program office to manage this multi-year effort.

The fiscal year 2021 budget request supports S&T's Office of University Programs in two vital efforts, our Centers of Excellence (COE) and working with Minority Serving Institutions (MSI).

The fiscal year 2021 budget request allows for the continuation of the University-based COEs that are focused on homeland security mission needs. COEs that will receive funding in fiscal year 2021 will conduct research and development that aligns with the administration's priorities to strengthen border security, cybersecurity and infrastructure protection, and prioritize trans-national criminal investigations. S&T conducts rigorous evaluations of each Center's performance using established criteria to help inform project funding decisions that meet operator needs and

stay focused on transferring or transitioning research and technology outputs into field use.

S&T seeks to leverage and utilize the unique intellectual capital in the MSI community to address current and future homeland security challenges and to provide relevant learning opportunities to diverse and highly talented individuals and inspire the next generation of dedicated to homeland security professionals. Our efforts provide learning opportunities for students that already are pursuing Science, Technology, Engineering, and Mathematic (STEM)-related degrees. These awards support MSIs in their efforts to attract highly technical students and provide exposure and mentorship opportunities with DHS programs. S&T's efforts with MSIs are important for ensuring students develop the cross-functional skills essential to their flourishing and meeting the demanding needs of the homeland security missions. By establishing continuous relationships between COEs, MSIs, DHS component agencies, and private-sector entities, S&T is expanding partnering institutions and providing resources needed for students to gain meaningful work experiences that prove invaluable to the growth of their careers in homeland security-related areas.

S&T's mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of DHS components and our operational partners in homeland security.

Chairman Richmond, Ranking Member Katko, and Members of the committee, thank you again for the opportunity to appear before you today and for your continued support of S&T.

I look forward to answering your questions.

Mr. RICHMOND. I want to thank the witnesses for their testimony. I will remind each Member that he or she will have 5 minutes to question the panel.

I will now recognize myself for 5 minutes for questions.

Director Krebs, in January 2017 the Office of the Director of National Intelligence issued a report concluding that the Russian government meddled in the 2016 Presidential election, and that Russia's goal was to assist the campaign of now-President Trump.

Last month several news outlets reported that President Trump removed the acting director of national intelligence, Joseph McGuire, had the staff from his office brief bipartisan members of the House Permanent Select Committee on Intelligence on foreign threats to U.S. elections. Are you familiar with that?

Mr. KREBS. I am certainly aware of the intelligence community assessment of 2017, and recall seeing some of the press reports. Yes, sir.

Mr. RICHMOND. Initial reports indicated that ODNI staff told Members in the briefing that the Russian government, once it—was once again attempting to meddle in our elections to benefit President Trump's re-election. This is the same thing that Russia did in 2017, when they interfered in the U.S. election to help President Trump. Wouldn't that be the same assessment?

Mr. KREBS. I am sorry, is the—can you repeat the question? I am trying to understand what——

Mr. RICHMOND. Well, the intelligence is the same intelligence from 2017 that Russia is trying to interfere in the election.

Mr. KREBS. So I certainly can't talk to the intelligence. I would defer to the intelligence community on the specific assessments. We are planning as if the Russians and others are coming back for the 2020 election to again attempt to interfere.

Mr. RICHMOND. Let me just get to the—my main point on this is that we need to believe in the intelligence that we are getting. All of the reports indicate that the assessment and intelligence changed once the President didn't like it.

We, as Members of Congress, need to know that we are going to get the whole truth and nothing but the truth from our intelligence communities, because we have a responsibility to act whether we like it—don't like the information.

So the real question to you is can we believe and trust that the information we are getting from you, and you all in the intelligence community, is the whole truth and nothing but the truth?

Mr. KREBS. Yes, sir, absolutely.

Mr. RICHMOND. Let me shift a little bit to CFATS. I represent, probably, the No. 1 and No. 2 largest petrochemical district in the country. I am concerned that—where the proposed budget eliminates the CFS program. Last year officials from CISA testified before this committee that CFATS is a vital part of our Nation's counter-terrorism efforts, and very much a pressing need in view of the continuing level of chemical terrorism threats.

January 15, DHS issued an alert warning about heightened threats from Iran, specifically in the chemical sector. So can you share any information you have about what intelligence assessments or security assessments CISA has completed to support the elimination of the CFATS program, and how will eliminating CFATS make my constituents safer?

Mr. KREBS. So thank you for the question specific to the January alert related to the heightened tensions of Iran. I don't believe that was associated with any specific intelligence product targeting chemical—the chemical sector. That was more—again, back to my opening comment about being a customer-centric organization, that was a request that came in from the chemical sector that said, "Can you guys pull something together for the sector that will speak specifically to Iran and the things the chemical sector can do to protect the sector?"

So more broadly on the CFATS issue, I think where we are right now is that, you know, over 15 years or so of implementation of the CFATS program, there is no question that we have changed the risk management dynamics across that sector. At the same time, the threat landscape has also shifted. Some of the players that were heavy in the 2005 to 2007 period are not necessarily on the map any more. In the mean time, other actors have spread up. The economy, in and of itself, how it works, supply chain, chemicals and commerce have also shifted.

So I think part of what we are looking to accomplish here is, if you look back at CFATS in general and the application of the regulatory program to the sector, it really only encompasses about 3,300 facilities. So, if you look back at the fiscal year 2020 budget, that is about $72 million across 3,300 facilities.

What we are looking to accomplish here is, as we have fundamentally changed the way risk is managed in the chemical sector across at least 3,300 facilities, what opportunity do we have to extend that risk management opportunity across the 40,000 facilities of the chemical sector?

My sense is that, regardless of what happens here—and of course, we will implement whatever Congress and—passes, and the President signs, whether it is a re-authorization of CFATS or a shift to a voluntary program. But the bigger point here is we are

looking for this opportunity to more broadly change risk management posture across the chemical sector.

Mr. RICHMOND. My last question would be do you support a temporary extension of CFATS so Congress can determine the appropriate path forward, No. 1; and No. 2, do you maintain a list of unfunded priorities so that—if you have money, things that you would do?

Mr. KREBS. Sir, we do have a significant list of PDOs, or program opportunities that we would be able to—if funded, we would be able to execute, of course.

On your private—on your first question, you know, again, we are in a transition planning process right now with about a month, a little over a month or so, out from expiration of the program. So we are focused on transitioning right now. But whatever happens, again, we have the funding for the rest of the year to execute the program if there is a temporary extension put in. Thanks.

Mr. RICHMOND. Thank you, and I yield back. I now recognize the Ranking Member, the gentleman from New York, Mr. Katko, for 5 minutes.

Mr. KATKO. Thank you, Mr. Chairman. Mr. Krebs, I want to kind-of ask you about the Cyberspace Solarium report in general, but really talk about how it may impact the budget if those recommendations get implemented.

So I view this Solarium report as one of the critical things we can do in Congress this year, and I really believe that the next 9/11 could absolutely, positively be, God forbid, a cyber attack that is cataclysmic. I am not sure we are ready for it. I think this report recognizes that, and it recognizes—and it makes a series of recommendations.

I know part of it is on the defense side, and I—you know, we are more interested in the homeland side in this committee, obviously. So if you could, talk from the homeland side on what are some of the big things in that report, and how it might be—might impact the budget going forward, so we can plan for it.

Mr. KREBS. So thank you for that. It is interesting, and I am sure Congressman Langevin shares this. Being so close to the wheel and the development of the report, you see the recommendations, and they just make a lot of sense to us. But it is good that someone that is not developed in the—you know, was not involved in the process also thinks they make sense, and this doesn't just kind-of fall flat.

So the—kind-of the pickup I have seen today, at least, has been very, very positive that there is some innovative, bold recommendations in the report. But more importantly, there are recommendations within the report that are practical and eminently implementable. That is the most important aspect of the report in and of itself, that whatever is in it, that we can actually do it.

To your point about that defense/offense divide, that was one of the important policy signals that comes out of the report—to me, at least—that this is not just about investing in the Department of Defense and General Nakasone's teams. It is also about ensuring that CISA and the rest of the civilian cybersecurity space and the private sector have the direction, guidance, and resources they need to be able to implement.

Some of the key takeaways that I have, the report—I think I will focus on 3.

First is that it squarely puts CISA at the central coordination point for civilian cybersecurity defense, and that brings all the Federal partners together, but that also, importantly, brings the Federal—or the private sector, as well as State and local partners together.

There are going to be some significant employment implications here. Do we have the facilities that we need to truly set up a collaboration space? We are operating in about 9 different facilities in Baghdad.

Mr. KATKO. A bunch of them, and they do seem to be all over the place.

Mr. KREBS. We have 9 facilities in the National Capital Region that we have been in since 2005, when I was a contractor with the prior organization, one of the first inhabitants of the building. We need a refresh. So we are going through that process right now with the St. Elizabeths program.

We just need to make sure that we have the access for our private-sector partners to the facility, that we can accommodate regular access from private-sector partners, and make it an experience that they want to actually participate in. It is a kind-of if-you-build-it-they-will-come sort-of approach. So that aspect we are focused on.

There is another piece of it, continuity of the economy, that we are working through right now. That is kind-of, in some part, a manifestation of our National critical functions work that we launched last year. We are also seeing that play out right now across the COVID response. So we have developed a framework for analyzing broader supply chain impacts of COVID across 4 different elements.

The first is, is there a commodity disruption that would disrupt a business or a function?

The second is, is there a workforce disruption that you may not be able to continue delivering that service or function?

Then there are 2 kind-of demand-side issues. No. 1, you have over-demand, and that could be, like, the N95, you have too much demand and, therefore, you have a cratering within the function. On the flip side of that, you may see in transportation there is a lack of demand. So the function then degrades.

So those are the sorts of things that we want to push into that continuity of the economy. We have the rubric, but we are—you know, to fully implement that recommendation is going to require significant analytic investments within the agency.

Then last, workforce, workforce, workforce. As I mentioned in my opening, to be successful in this space, to be truly a customer-centric organization, I have to have personnel out in the field, not just engineers here in District of Columbia, but customer service professionals out where our customers are. That is going to require a significant investment in personnel.

Mr. KATKO. Thank you very much. It does sound like there is going to be more requests, from a financial standpoint, from the committee and from other committees to implement these plans. As we work them out and tease them out and get them into legislative

formats, we will definitely revisit those issues. So thank you very much for that.

Mr. Hentz, what—if you could, just describe quickly, what are the key legislative priorities for your organization this year?

Mr. HENTZ. Thank you, Chairman, Ranking Member. What we were——

Mr. KATKO. I will take Chairman.

Mr. HENTZ [continuing]. Trying to do right now is——

[Laughter.]

Mr. HENTZ. What we are trying to do right now is prioritize the list of requirements from our operational components.

To specifically answer your question, those priorities look like countering unmanned aerial systems, things like 5G and other supply chain risk mitigators. Obviously, support to border and commerce, as well as our support to emerging biological and chemical risk.

So those are our core primary equities right now that we are trying to focus on.

Mr. KATKO. Thank you very much. I am interested in that. I will yield back, but I just want to note in Syracuse, New York they are going to start building a 5G manufacturing facility, the first one in the country that is going to have all American components, which is critical for cybersecurity, going forward.

We also have one of the largest unmanned aerial system research corridors, from Rome Labs to Syracuse, New York. So we are at the tip of the spear with some of your priorities. So I look forward to working with you further on those, going forward. I hope we can continue the lines of communication.

With that I yield back, Mr. Chairman.

Mr. RICHMOND. The gentleman yields back. I now recognize the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Let me begin by thanking you for—and the Ranking Member for the supportive comments about the Solarium Commission project, and the report that we are issuing today, and, Mr. Chairman, for your leadership on the issue of cyber, and I look forward to continuing to collaborate with you on these—on this important topic.

Good morning to Director Krebs and Mr. Bryan, thank you very much for being here today. Mr. Hentz, I appreciate your being here today, I look forward to hearing what you have to say.

Director Krebs, I guess I want to begin with you, and express my appreciation to you for your participation in the Cyberspace Solarium Commission. Your contributions to that effort, and the dialog that took place, and the ultimate findings, your contributions were invaluable. Obviously, the report is being released today, and I am very proud of the work that we did bring, in bringing together many different stakeholders and coming up with a series of recommendations, as you pointed out, I think, are eminently doable, and that I hope will advance the ball on cybersecurity.

So my first question, the report identifies various ways that CISA should work with sector-specific agencies to improve information sharing and collaboration with private-sector entities. So, for example, the report highlights that we need more clarity in statute

of what is required of SSAs in order to ensure that you have the information that you need to do your job.

So, Director Krebs, do you agree that Congress should work to lay out the responsibilities of SSAs to both their private-sector partners and to CISA? That we should research them appropriately to perform these functions?

Well, I will stop there, and then I have other questions.

Mr. KREBS. So I think this is where we need to strike the right balance. It certainly makes a whole lot of sense to me that sector-specific agencies—of which I actually own 8 of them, between IT, comms, critical manufacturing, chemical, nuclear, emergency services—that we develop within those sector-specific agencies the specific requirements and attributes of those sectors.

You know, we can handle the core cybersecurity, whether it is the business side or the control system side. We can develop that core capability. But what I need is the specifics of the sector to be layered on top of that understanding, and I can't invest in significant treasury, or banking, finance, so that is absolutely the responsibilities that we would be looking to be clearly articulated.

Mr. LANGEVIN. Can you talk about how CISA plans to work toward implementing the recommendations, if you would?

Mr. KREBS. Well, I—so, right now, it—now that the report is out we have that kind of—the triage list, working through, of course, some of the templates that the—Executive Director Montgomery has pushed out. So we have got those identified, and the sorts of resources that we will need, the things we could do now, the things we will have to do down the road, but also working with the Commission on what will require legislative assistance.

You know, I think there is a significant amount of the recommendations that we can implement right now. But, obviously, with some of the requirements for—whether it is IOT standards or some of the additional requirements on critical infrastructure, that is going to require either Congressional action or some sort of regulatory proceeding.

Mr. LANGEVIN. So, like my other colleagues here today, I also want to be on record as saying that I am very concerned about the cuts to CISA's budget proposed by the administration.

Look, the National Risk Management Sector—Center, in particular, is a critical component of the Solarium Commission's recommendations, especially when it comes to syncing up the cyber expertise that CISA has with the sector-specific enterprise and the SSAs. So do you believe that the NRMC will be able to carry out its own mission, in addition to the ones recommended by the Solarium report, with the requested amount of funding?

Mr. KREBS. So I think—the way that I see the budget is—Ranking Member Rogers mentioned, you know, the proposal and the actual budgeting piece.

You know, I am on the formulation and implementation side. The way the 2021 budget was developed, given the timing of formulation, the timing of the 2020 appropriations, they were out of step. So the 2021 budget request, the President's budget request, was built on the 2019 enacted. So if you look at it in—through that lens, it is actually an increase over the 2019 enacted.

Because we didn't receive the fiscal year 2020 appropriations until late December, by that time the 2021 President's budget was already baked, from my—from where I sit, at least. So it was out of my control, that was already cooked. There was not time to kind-of re-peg it against the 2020.

So what you see, instead, in the President's budget request, are the key areas of focus for the agency. There is plenty of room for investment. The National Risk Management Center, for instance, has plenty of room for investment to get the additional analytic capabilities, we would need, if that is what the Congress decides.

Mr. LANGEVIN. Clearly, CISA is going to need additional resources to do the job that we are expecting you to do. I appreciate the job that you are doing, as director, and your team at CISA. Thank you for that.

With that, Mr. Chairman, I yield back.

Mr. RICHMOND. The gentleman from Rhode Island yields back. I now recognize the gentleman from Alabama, Mr. Rogers, for 5 minutes.

Mr. ROGERS. Thank you, Mr. Chairman.

Mr. Krebs, you know, it has been reported that there are over 300,000 cybersecurity job vacancies in the country at present. So we have a real challenge. That is across, you know, the private and public sectors. How many job vacancies do you have that you are struggling to fill?

Mr. KREBS. At the moment we have got about 655 vacancies within the agency, about 151 of those are cybersecurity. I have about a 95 percent retention rate on the cybersecurity side, which is good, and it is improving.

What we are doing right now, particularly as we continue to hire against the fiscal year 2020 funding—in that set, again, peg the FTE rate higher. We are trying to look at hiring as a—from a systematic approach. So left to right, from—you know, identifying the job to actually getting a person in a seat with the PIV card and a machine, ready to roll. That requires a whole host of partners within CISA and without. So, really trying to flush out who owns these things, what are the bottlenecks, and then what is the plan we are putting against it.

So a couple examples of choke points or bottlenecks that we are seeing, it is the hiring manager develops a position description. The problem with the hiring manager doing that is a hiring manager is a collateral job. It is an other-duties-as-assigned. So I have someone who is a program manager and an engineer, but also has to do a hiring manager job.

So we are saying, OK, maybe we relieve them of the hiring manager responsibility and have full-time hiring managers that—their job, at least on a 6-month, maybe cyclical basis, would be to just work position descriptions, just work the interview process. We think that can streamline and make a more efficient process.

We also have to look at——

Mr. ROGERS. Have you started that?

Mr. KREBS. Yes, sir. We did. We—a couple of weeks ago we launched a task force to focus just on this sort of thing.

Mr. ROGERS. I am sorry to interrupt you.

Mr. KREBS. So we are going to be plowing through those PDs and the selections, which then gets us to the subsequent piece, the security.

For instance, in the past we have looked at cybersecurity jobs as requiring top secret SCI clearances. We are challenging those assumptions. You know what? I might not need out in the field anybody that has a TS. Secret might be fine. So let's take a stab at that. If they need TS down the road, then we can put them in for that process. The TS is a—the top secret clearance is a significant additional time lag in hiring. So we are going to change the way we write PDs. Plus there are other policy and process issues.

Again, some of that security clearance review I have to outsource to other parts of the Department, so let's see what we can do there.

But also, like, just getting smarter about how we write position descriptions. So working in part with the Aspen Group and the—their cybersecurity working group, they issued a series of recommendations on how to improve cybersecurity hiring.

One of them that we have adopted is how do you—don't over-spec the position description. So you are trying to hire a job—someone into a job. Don't say you have got to be able to do 15 things. Just tell them the 2 or 3 things you need them to do. So those are the sorts of things.

We are just trying to bring a little bit of reality into the hiring process, and we have already seen a 12 percent decrease in our time to hire. So, in some cases, it is—that is only—you know, that goes from, like, 260 days to maybe 240 days, just trying to improve these numbers a little bit, and incrementally do it. But we think we have got processes in place. We will be able to dramatically cut the hiring process.

Mr. ROGERS. Do you feel—have you found that your salary and benefit packages is adequate to compete for talent?

Mr. KREBS. I—so thank you for bringing that up, because I neglected to mention it.

We have been provided a series of different retention and hiring incentives that we can use, including tuition reimbursement, up to 25 percent hiring—or, rather, retention bonus. So I can actually, I think, generally, compete in the market. Certainly not on the top, top, top, top end, but we can provide—between mission and pay and just quality of life, we think we can do a pretty good job here.

So it is just about getting out there, and making sure we are using smarter, you know, platforms, and really hitting some of the on-line—like, LinkedIn, and things like that, aggressively recruiting across those platforms.

Mr. ROGERS. Have you found that you have been able to bring in many CISA employees through the Scholarship for Service program?

Mr. KREBS. We have used that, and that is one of the key partners that we bring folks in, particularly at the—kind-of the lower and mid-level of the GS structure, not at the higher GS–15. But we need to take greater advantage of that, that is the way I see it.

For us, it is somebody is doing recruiting for us, and we have just got to go kind-of collect resumes. We can make on-the-spot—at the

SFS hiring fairs we can make on-the-spot offers and immediately get the process started, and that shaves 2 weeks off.

Mr. ROGERS. I would love to take the lead on helping you with that particular issue. I think the Scholarship for Service program is a very under-used tool. So if you will get with me, let me know whatever you need, I will take the ball and run with that.

Thank you, Mr. Chairman.

Mr. KREBS. Thank you.

Mr. RICHMOND. The gentleman from Alabama yields back. I now recognize the gentlewoman from New York, Miss Rice, for 5 minutes.

Miss RICE. Thank you so much, Mr. Chairman.

Director Krebs, as you responded in—as you said in response to a question by Mr. Langevin, it is clear that it is going to be up to Congress to translate many of the Cyberspace Solarium Commission's recommendations into legislation, or legislative proposals. But I think it is worth noting that the fiscal year 2021 budget request would not advance the Solarium's vision for CISA, which I think is problematic, to say the least.

But my question is how is—how do you plan to invest in 5G security and resilience, supply chain security, and election security with less money?

Mr. KREBS. So if you look at the past 3 years, we started from scratch. I will use election security as an example. We started from scratch. We had zero election-specific money. Over the past 3 years Congress has invested about $102 million in our election security effort. Last year was about—it was about $43 million. The fiscal year 2020 budget—2021 budget has, I think it is, about $30.5 pegged against election security.

What we are using that, those funds, to do is, yes, provide specific election capabilities, but also invest in broader capacity and capabilities within the agency on vulnerability management, threat hunting, any of those sorts of vulnerabilities—scanning capabilities, remote penetration testing. So we will continue to do that. The more we put in there, it will directly benefit elections, but also the broader critical infrastructure community.

But again, with more I can always do more. So, again, whatever you will, of course, appropriate, we will be able to implement and execute against.

Miss RICE. So I think one of the problems with the election interference is—putting aside what the intent is, putting aside what countries like Russia and China—what specific candidate they are trying to help, put that determination aside. When you look at just the overwhelming amount of disinformation that is out there, how do you address that issue?

So if a specific campaign sees this just repeated disinformation—that, obviously, we will just assume is negative—against one particular person, what do you suggest a campaign—and whether it is a Republican or a Democratic campaign, because disinformation is at the heart of what is happening here, and it—you know, the attempt to sway the opinions of everyday Americans.

So how would you suggest that people and campaigns handle that?

Mr. KREBS. So, stepping back a little bit in the broader disinformation issue, and countering disinformation, we tend to view it as a supply and demand problem. On the supply side, you actually—you have these—or the influence operators, whether it is Russia, Iran, China, whomever it is, doesn't matter, pushing that information. Right?

So there are capabilities across the intelligence community, the law enforcement community, within the private sector on the social media platforms that can disrupt that supply, but do it in a content-neutral way that is more about tagging actors, sharing those, illuminating campaigns.

You know, I got to give a lot of credit to the social media organizations for—you know, compared to 2016, we are light years ahead of where we were. Is there room to improve? Absolutely. There is more that can be done, particularly with encouragement, I think, from the Congress.

But there is another side to all of this.

So, specific to your question, if you see it, report, you know, send it in to the FBI, send it to the social media platforms. They have dedicated teams that are monitoring, but also have intake mechanisms so that they can identify and then take down these campaigns.

But the more important aspect of this—so we are—this is a Whack-a-Mole game if we are always chasing the latest disinfo campaign. What we have got to do is focus also on the demand side. The demand side is the American people. So how do we create a more discerning public, a more informed, educated public on the things that are happening across the news and the media and the social media platforms they see?

So that is what we have put a lot of effort into, and that—you know, I think probably the most known, well-known thing we have done there is the War on Pineapple, which was last year we launched a program that distilled down how disinformation operations work, how the Russians do it, but we did it not in a way that it is Russia, it is whether you like pineapple on your pizza or not. So it is a very kind of non-confrontational issue, but it is educational. We got Secretaries of State, election directors involved, pitted on either side. Even the—I think the armed forces of Canada got involved in the whole thing, so we had a foreign influence operator in here, but it doesn't matter.

[Laughter.]

Mr. KREBS. Anyway, it was educational. It actually took off. People started to get it.

So there is a civic education opportunity in front of us, and those are the things we are looking to do with the social media platforms, as well as academia and some of the other nonprofits that are involved here.

Miss RICE. I would like to follow up with you on that. Thank you very much.

I yield back.

Mr. RICHMOND. The gentlelady from New York yields back. I now recognize the gentleman from North Carolina, Mr. Walker, for 5 minutes.

Mr. WALKER. Thank you, Mr. Chairman.

Mr. Hentz, is that the correct—so yes. Since the military doctrines of Russia, China, North Korea, and Iran include EMPs, electromagnetic pulse attacks, with their cyber strategies, and that our civilian infrastructure is highly vulnerable to EMPs, how is DHS addressing the existential threat of an EMP attack so that Americans can be assured they are safe?

Mr. HENTZ. Thank you for the question. So what we have done, specifically, is formed a very tight relationship with CISA, who, from the Department, owns the mission space, per the 18 NDA, I believe it was, to ensure that there is a cooperative public-private partnership between their organization and critical infrastructure owner-operators.

What we have done, specifically, is a T&E assessment to help with a better understanding of how one might go about shielding their critical infrastructure, how to better obfuscate critical elements that might be subject to EMP, GMD, and other types of solutions, and then working with CISA, propagate that information throughout the mission spaces through which they operate to ensure that everyone has good hygiene practices.

But at the end of the day, what we are really driven by is a demand signal from CISA and its mission partners in the field to help inform what our R&D should be.

Mr. WALKER. Thank you for that answer.

Director Krebs, CISA has started their team closely monitoring the coronavirus, and is working with critical infrastructure partners to prepare for possible disruptions that—they may stem from wide-spread illnesses. How is the agency ensuring the disruptions are minimized to critical infrastructure sectors such as the emergency services sector, or the nuclear reactors, materials, and waste sector, both of which DHS has designated as the sector-specific agency in the event of a large outbreak?

Can you address some of that?

Mr. KREBS. Yes, sir. So we established within CISA about—it was early February we stood up an enhanced coordination cell, and designated a mission manager. So that really was—is the nexus of all COVID-related activity within the agency.

Under that we have got a series of lines of effort. The first line of effort is physical protective measures and recommendations. That typically takes CDC guidance, and then applies sector-specific guidance on top. That looks at different business models: "If you are heavy into public engagement, like a hotel or a sporting venue, here are the things you should be doing." But it also looks at industrial environments, including pipelines, chemical, electricity.

We also have a line of effort focused on cybersecurity. So, as organizations move to telework, what are the cybersecurity considerations? Because the attack profile changes. You might be using more VPNs, so make sure you have got your Citrix and other VPNs patched, things like that.

But also targeting and looking into the phishing campaigns that we have already seen the bad actors using as an incentive or enticement to get people to click on links.

We are also looking at these continuity of the economy aspects, as I already talked about, those 4 elements of how a function may be degraded.

Then, looking deeply at disinformation, as well, so working with our intelligence community partners of how is disinfo playing out across COVID, and this is important in the election space. Particularly, we had a call last week with about 600 State and local election officials about, you know, what are the hygiene practices they can take, but also what are we seeing in the disinfo space, and how can we dispel any sort of coronavirus or COVID impacts on voter turnout, for instance.

You are already starting to see some of those discussions take place into action. Earlier this week Secretary Frank LaRose from Ohio announced that any voting precincts in nursing homes or assisted living communities will be moved out——

Mr. WALKER. OK.

Mr. KREBS [continuing]. They will not be taking place. So we think that is a great outcome that we need to—we want to continue pushing that information——

Mr. WALKER. A very thorough answer. My follow-up, would a decrease in funding for fiscal year 2021 threaten the functionality or security of any of these components that you mentioned if an outbreak were to occur?

Mr. KREBS. So I think, based on the 2020 budget, we have been able to build capacity. The 2021 budget will allow us to continue that activity. I think what you would see is enhancements wouldn't be able to happen, necessarily. That is one thing that we are looking at right now on COVID with the National Risk Management Center, in particular, what additional analytic capability do we need to bring in right now to do prospective analysis. That, of course, is going to continue, likely, past the fiscal year break.

Mr. WALKER. So security, not necessarily compromised, but enhancements moving forward would be inhibited. Is that fair?

Mr. KREBS. I think steady—it is—you know, we can maintain what we have, but we see the threat landscape shifting, and so, you know, the ability to further invest in capabilities, I think, would benefit.

Mr. WALKER. Thank you, Mr. Chairman. I yield back.

Mr. RICHMOND. Thank you, the gentleman from North Carolina yields back. I now recognize the gentlewoman from Michigan, Ms. Slotkin, for 5 minutes.

Ms. SLOTKIN. Great. Thanks to both of you for being here.

Mr. Hentz, I am interested in this idea of how the Department of Homeland Security can move new ideas, particularly on the issue of border security, new technology that might help us secure our borders more efficiently. How do you take that right now, from pilot project to actual scaled use?

It is a problem we have in the Defense Department. I am on the Armed Services Committee. I have a bill that is trying to bridge this gap. But can you explain to us, and potentially explain some of the gaps we have in going from great idea that maybe the private sector has to a scalable, usable piece of technology?

Mr. HENTZ. Sure. So thank you for the question.

The first thing that we try to do is get a really refined understanding of what the operational gap is from that component.

So, in this case, let's say, we are working with CBP. We established them as a board of director-type member for our innovation

approach. What we have done is stood up capabilities such as the Silicon Valley Innovation Program—it is more so about the idea of finding unique innovation in industry—and we paired those innovators, those non-traditional performers, with those operators.

Once they completely understand the use case, what we do is almost like a shark tank-like type of approach to determining whether or not their solution is actually, No. 1, usable and effective in an operational environment, and then, No. 2, does it then scale?

Now, where the deficiency is, such—I think you are going for, is that we, as an S&T organization, we don't have acquisition authority. So, while we may go off and find these unique end-state types of solutions that are coming out of the emerging market, it is still incumbent upon the operator, like a CBP or a CISA, to program for those acquisitions. Because we don't have that authority, we don't then, by definition, go off and buy that solution for that operational component.

So I think that that is one of the main——

Ms. SLOTKIN. Yes.

Mr. HENTZ [continuing]. Deterrence for quick adaptation.

The other is more predictability around other transactions authorities. By us using other transactions authorities, or the operators using 880 authority, that would also give the Department a head start, a jump, if you will, where it is not a big, traditional acquisition.

Ms. SLOTKIN. Yes. So I am working on a bill with some of my colleagues across the aisle called the Intel at Our Borders Act, which basically requires the Department to provide a comprehensive strategy on how to integrate some of these new, emerging technologies. It is actually something CBP, our local folks in Michigan, the Northern Border, have been super excited about. They have helped us draft the bill.

So more to follow, but we would love any notes for the record on what would be helpful for you to actually make this more effective.

Director Krebs, I just want to thank you for your approach to this committee. I know it is a strange thing for both of you to be up here sort-of defending your budget which cuts your budget, but knowing that we will put money back in your budget. That is a complicated thing to do, and I want to thank you for having your—I think it is—he is your assistant director for cybersecurity—Bryan Ware came up and did a briefing, sort of a get-to-know-you thing, and that stuff makes such a difference when you are talking to a committee that is looking to help your department. So thank you for doing that.

Can you tell me—we—I constantly do these events with my local governments, who feel pretty wholly unprepared to manage cybersecurity on their own. They just—some of them are working part-time, this is not their primary job. They are trying to do their best. I know that we have put in—again, like, this committee has been great about talking about building up resources for our local officials to provide for themselves.

But in your perfect world, you know, it seems like we can't keep doing this, where we are expecting really small communities to defend themselves. They hold the private data of our residents. So what has to happen? Where are we going? Help us forecast how we

are going to better protect ourselves, since our local communities are on the front lines.

Mr. KREBS. So it is going to require—and, yes, I think about this almost nonstop, and nowhere is this more acute than in election security, of course, with 8,800 jurisdictions across the country that are managing, in a lot of cases, significantly outdated systems. They are just operating from a lack of funding.

So I think there are a couple of challenges here.

First is just the governance aspects, when you have just this diversity of ways that States manage, or are able to manage, based on home rule or otherwise, requirements across distributed counties and jurisdictions.

There is also a funding issue, of course. The States just have significantly different funding profiles than the Federal Government that can run a deficit.

Then, just the availability to services. There is not a lot of acquisition leverage or procurement leverage when you are talking about a local jurisdiction.

So, at the governance piece, we are continuing to just raise awareness with State governments, with State legislatures. You know, my theory is that awareness leads to investment, which builds capabilities. We are going to have to continue beating the drum on cybersecurity awareness. That is, I know, sometimes a shocking thing to hear, that people still need to be made aware of cyber risks, but it just—it remains the case. We need the leadership to understand this.

The second thing on the funding, understanding that there are a couple different bills floating around on providing grants to State and locals, I think those are certainly useful things we need to work through, and we need to get to a spot where, like FEMA has, the Disaster Relief Fund, you know, what does a cyber equivalent look like? But, at the same time, we are not sitting back and waiting. We—in the recent FEMA/Homeland Security grant program, which I am sure you all heard from your chiefs of police and emergency management, we did put some requirements in there for cybersecurity and election security investments, which, over the last 7, 8, probably 10 years, has been a National preparedness report, key area of lack of preparation.

Then, last, what more can I do in the Federal Government space to provide additional services out to Federal partners? So the continuous diagnostics and mitigation platform, for instance, is something that we can open up. It is on the GSA schedule, we can do that. Some States don't have the ability to buy from GSA, so we need to change that behavior, but also make things affordable.

The DOTGOV Act, which allows for the actual .gov domains to open up. There is a $400 requirement. Four hundred dollars in local jurisdictions in Michigan or elsewhere, that is a difference-maker. That can be, you know, somebody's bonus. So these are the things we need to work through.

Then last, we are making—we are working through standing up a protective DNS service for the Federal Government. How do we open that recursive protective DNS program or platform for State and locals, as well? I see centralization and opening up services

like that as the key to changing risk outcomes for State and local partners.

Mr. RICHMOND. The time of the gentlelady from Michigan is expired. I now recognize the gentlelady from Illinois, Ms. Underwood, for 5 minutes.

Ms. UNDERWOOD. Thank you, Mr. Chairman.

Several weeks ago a school district that serves my community in Crystal Lake, Illinois was hit with a ransomware attack. The school officials did pretty much everything right. They took the servers off-line, they protected sensitive data, they avoided major disruptions in student learning, they planned ahead. They even had a cyber insurance policy. But it still took over a month to get the student computers back on-line, and the attack cost over $800,000, not all of which is covered by even good insurance.

The fact is that ransomware attacks our business, and that business is good. While both CISA and Congress have made important steps, they aren't enough for schools like those in Crystal Lake.

So, Director Krebs, can you tell us more about the profile of these kinds of attackers, and are they nation-state actors or affiliates, organized cyber criminals, lone actors? Can you just say something about the——

Mr. KREBS. Yes, ma'am. I am smiling because your "ransomware is business, and business is good" line, I have used that before, and it is absolutely what is going on.

Ms. UNDERWOOD. Yes, sir.

Mr. KREBS. So the way we look at ransomware right now is there are kind-of 3 things that are going to have to change.

First is we have to continue investing in the defensive side. Yes, they did all the right things, but I am sure that, when you go and do the post-mortem, there were elements that could have been implemented to protect. You know, really, what we are finding is just some simple measures like multi-factor authentication, appropriate Windows administration, lease privilege, things like that can just stop it from happening, and then go to the next partner. The—or the target.

The second thing we have to do is disrupt the economic model, disrupt the business model.

Ms. UNDERWOOD. Right.

Mr. KREBS. It—like you said, business is good. That is why it continues. So how do we disrupt that? Are there things we can do, the Congress can do to target the ransomware actors, to take a look at actually paying out ransomware, whether that is a public policy issue or not? I think that is a good question that we need to take a hard look at.

Then the third thing we have to do is what more can the Federal Government do, not just from a defensive side, but from more of an aggressive, almost defend-forward perspective, do to disrupt these behaviors? You know, we know where these guys operate. They are not in the United States, they are in Russia and elsewhere. What can we do to put additional pressure on them from the intelligence community and from the Department of Defense and——

Ms. UNDERWOOD. But would you characterize the actors—how would you characterize the attackers themselves?

Mr. KREBS. The actors themselves are criminals.

Ms. UNDERWOOD. OK.

Mr. KREBS. They are straight-up criminals. Not necessarily, you know, in this case—you know, I mentioned Russia, so it is not like they are necessarily FSB, but they are cyber criminals operating in the sovereign space of some of our adversaries in some cases.

Ms. UNDERWOOD. Yes. So I thank you for outlining those next steps that we can all take to protect our communities and critical assets that we all have within our own organizations from ransomware attacks.

I do think that there is more room for leadership from CISA and from law enforcement here.

Mr. KREBS. Yes, ma'am.

Ms. UNDERWOOD. My constituents weren't sure, for example, whether to leave the evidence of the attack intact, or to try to get the operation up and running quickly to serve their students.

So, if you can just offer, you know, advice for what to do for communities that are experiencing this type of attack——

Mr. KREBS. So we have issued a significant amount of guidance and best practices, not complicated, 80-page guidance stuff, but 1-page, 2-page sort-of guidance for our partners.

One thing that I don't think we have explored quite enough is working with you and Congress, understanding the influence you have back home——

Ms. UNDERWOOD. Right.

Mr. KREBS [continuing]. With your partners in the school districts and the public health community. Please encourage them to work with us. There are things that we could do to help them to make sure that they don't have that bad day.

Ms. UNDERWOOD. Right.

Mr. KREBS. Because $800,000 to a small community in your jurisdiction——

Ms. UNDERWOOD. It is significant.

Mr. KREBS. It is. That can be back-breaking in some cases——

Ms. UNDERWOOD. So do you think that there are technical standards that hardware and software products should meet in order to limit their vulnerability to ransomware attacks?

Mr. KREBS. Again, a lot of this ransomware is just a matter of somebody clicking on a link. It is often delivered by spear phishing. In some cases it is delivered by a remote desktop protocol, ports being open, things like that. So this is not necessarily a hard sec or software sec issue. It is configuration. It is Windows administration, Windows administration, Windows administration.

Ms. UNDERWOOD. Right.

Mr. KREBS. Those are the sorts of things that we need to invest in. It is just awareness, and how can we just configure from the get-go better postures.

Ms. UNDERWOOD. OK. So Mr. Cuccinelli, your colleague, is going to be coming to testify before the larger committee this afternoon, and he has said that CISA has been assessing "issues of concern," potential impacts to infrastructure from coronavirus in the event of significant community spread in the United States. Those are clips of his quotes.

Significant community spread is already happening. So, Director Krebs, can you just talk about what impacts to critical infrastructure that you are seeing, and what should our States and localities expect to come in the weeks and months?

Mr. KREBS. Yes, ma'am. So we are trying to break it out from the tactical today, and the PPE, or the personal protective equipment——

Ms. UNDERWOOD. Yes.

Mr. KREBS [continuing]. That is out there into the more strategic, longer-term analysis. I talked about it a little bit earlier, but through our National Risk Management Center, and the National critical functions approach, what we are trying to do is understand what those key elements of degradation might be.

We have identified 4 key aspects. The first is disruption of a commodity, of a key commodity, like a widget in a—that would go into a car, some sort of device that would go into a car that would prevent it from rolling off the line, for instance.

The second is workforce disruption. So whether it is absenteeism, sick-outs, or other sorts of issues, particularly across different business models.

The third and fourth are more about the demand. So, in some cases, like N95 you would have an increase of demand, where you can't meet it.

Ms. UNDERWOOD. Right.

Mr. KREBS. Then the other, the fourth element, is a cratering of demand. That could be, in some cases, transportation. So we try to pull those all together.

We are seeing automotive, we are seeing IT and comms disruptions, and then also soft goods.

Ms. UNDERWOOD. Well, as you are publishing documents to the communities about those, can you keep our committee informed? We appreciate it.

Thank you, and I yield back.

Mr. RICHMOND. The time of the gentlelady is expired. I want to thank the witnesses for their valuable testimony, and the Members for their questions.

The Members of the committee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions.

Without objection, the committee records shall be kept open for 10 days.

Hearing no further business, the committee is adjourned.

[Whereupon, at 12:13 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM HON. SHEILA JACKSON LEE FOR CHRISTOPHER C. KREBS

Question 1. Director Krebs, I represent Houston, Texas. It is one of the largest metropolitan cities in the country, hosts one of the busiest international airports and is also home to one of the largest export hubs in America. As of yesterday, there were 13 cases of COVID–19 in Texas.

First, what are you doing, and what is the Government doing, to spread true information about the virus and its potential impacts?

Answer. Response was not received at the time of publication.

Question 2. In last week's CISA Insights document, you identified 4 risk management strategies related to supply chain security and the Coronavirus (COVID–19).

For the record, can you tell me what advice CISA is giving to help States and industry prepare and be resilient against a COVID–19 pandemic?

Answer. Response was not received at the time of publication.

Question 3. How is the Department of Homeland Security preparing State and local election administrators for the November Election given Coronavirus will still be with us until there is a vaccine?

Answer. Response was not received at the time of publication.