RESOURCING DHS'S CYBERSECURITY AND INNOVATION MISSIONS: A REVIEW OF THE FISCAL YEAR 2020 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

FIRST SESSION

APRIL 30, 2019

Serial No. 116–14

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
37–454 PDF WASHINGTON : 2019

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
JOHN RATCLIFFE, Texas
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi

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*
JOHN RATCLIFFE, Texas
MARK WALKER, North Carolina
VAN TAYLOR, Texas
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 2020 BUDGET REQUEST FOR THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY AND THE SCIENCE AND TECHNOLOGY DIRECTORATE

Tuesday, April 30, 2019

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 2:28 p.m., in room 310, Cannon House Office Building, Hon. Cedric L. Richmond (Chairman of the subcommittee) presiding.

Present: Representatives Richmond, Jackson Lee, Langevin, Rice, Underwood, Katko, Ratcliffe, Walker, and Taylor.

Also present: Representative Thompson.

Mr. RICHMOND. The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation will come to order.

The committee is meeting today to receive testimony on the fiscal year 2020 budget request for Cybersecurity and Infrastructure Security Agency, and the Science and Technology Directorate.

Good afternoon. I would like to thank the witnesses for being here today to discuss an important priority for this committee, funding the cybersecurity, infrastructure security, and innovation missions at the Department of Homeland Security.

Well, before we begin, I would like to send my condolences to the victims and families of the recent synagogue shooting in California. We are keeping Poway community in our thoughts and prayers this week.

But thoughts and prayers aren't enough. We also need to demand more of the President and his administration in the face of the rising threat of white nationalism and anti-Semitism seriously.

Returning to the topic of today's hearing, I want to begin by thanking the full committee Ranking Member Rogers and subcommittee Ranking Member Katko for joining committee Democrats in writing to appropriate us to seek additional funding for CISA's cybersecurity mission.

I ask unanimous consent to insert a copy of the letter into the record. Hearing no objection, the letter is inserted.

[The information follows:]

LETTER SUBMITTED BY HONORABLE CEDRIC L. RICHMOND

April 10, 2019.

The Hon. NITA LOWEY,
Chairwoman, Committee on Appropriations, U.S. House of Representatives, H–307 The Capitol, Washington, DC 20515.

The Hon. KAY GRANGER,
Ranking Member, Committee on Appropriations, U.S. House of Representatives, 1016 Longworth House Office Building, Washington, DC 20515.

DEAR CHAIRWOMAN LOWEY AND RANKING MEMBER GRANGER: As Congress navigates the Fiscal Year 2020 (FY 2020) appropriations process, we urge you to increase the Homeland Security Subcommittee's fiscal year 2020 302(b) allocation. By providing additional funding in fiscal year 2020, the Appropriations Committee can ensure Congress is able to properly resource Federal cybersecurity and critical infrastructure protection efforts at the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

The American people and our government depend increasingly upon the Internet for daily conveniences, critical services, and economic prosperity. This extraordinary level of connectivity, however, has also introduced progressively greater cyber risks for the United States. Protecting sensitive information on government networks and ensuring access to safe food, reliable electricity and transportation, clean water, and secure election infrastructure through cyberspace also introduces new vulnerabilities and potentially catastrophic consequences from cyber incidents. Long-standing threats from nation-states, terrorists, transnational criminal organizations, and other malicious actors continue to evolve in scope, scale, and complexity as our adversaries move their activities into the digital world. More than ever, cyber threats now exceed the danger of physical attacks.

Despite the warning signs, investment in our Federal civilian cybersecurity capabilities simply has not kept pace. Threats to our Federal networks and critical infrastructure constantly evolve, and our adversaries' capabilities outpace our defenses. In today's world, a flat cybersecurity budget is just as dangerous as a cut. If our fundamental cybersecurity capabilities are not fully resourced, vulnerabilities will continue to go unaddressed, and America's embrace of digital infrastructure risks becoming a source of strategic liability.

Congress must rethink the way we resource this mission. Additional investments are necessary to ensure the United States is not only capable of responding to the global threat, but that we are preparing for future threats as well. We urge the Committee to break from the status quo and increase the Homeland Security Subcommittee's 302(b) allocation commensurate with the threat. It is imperative that the Homeland Security Subcommittee's 302(b) allocation enable CISA to mature and grow the services it provides to secure Federal and critical infrastructure networks.

We appreciate your leadership on this issue and applaud the Committee's historic support of DHS's cybersecurity and infrastructure protection activities. Increased funding provided over the past few years has helped CISA bring Federal departments and agencies into the National Cybersecurity Protection System, sped deployment of Continuous Diagnostics and Mitigation tools and capabilities across the Federal enterprise, and dramatically expanded our nation's election security efforts. Now that CISA has demonstrated it is up to the task, it is time for Congress to resource the agency to fully execute its critical homeland security mission.

Thank you for your thoughtful consideration of our request.

Sincerely,

Mr. RICHMOND. From election security to supply chain security, we ask more of DHS's cybersecurity arm every year.

Despite CISA's growing mission, its budget has remained stagnant. Since taking office, the President and those around him have paid a lot of lip-service to the issues related to cybersecurity and innovation. But there hasn't been much follow-through.

In February, for example, the President touted his innovation agenda, but his fiscal year 2020 budget slashes funding for the S&T by nearly one-third.

In September, former Secretary Nielsen stated that cyber attacks now exceed the risk of physical attacks. Yet, the President's fiscal year 2020 budget would cut CISA's cybersecurity funding.

Last Fall, the White House released the National cyber strategy, which among other things, promised to further enable the Department of Homeland Security to secure Federal department and agency networks. But the fiscal year 2020 budget failed to request additional funds or additional authorities for CISA's Federal network security mission.

Although officials throughout the administration have declared that election security is a priority, no one in the White House has been directed to coordinate a Federal response, and it has never been a budget priority.

Instead, this National security issue seems to be viewed as a hot potato in the President's inner circle, not worthy of a whole-of-Government approach.

To complicate matters, all of this is happening in the absence of a White House cybersecurity coordinator, which the White House eliminated last year.

The Mueller report makes clear that our adversaries will continue to meddle in our elections. DHS and the FBI have issued numerous warnings about threats Russia, China, Iran, and North Korea, among others, pose to our critical infrastructure.

The threats we face are constantly evolving. Our cybersecurity capabilities and the technology we deploy must do the same. In short, the time has come for less talk and more action. If the White House won't lead, then Congress will.

I am hopeful that our bipartisan efforts to secure the additional funding for CISA's cybersecurity activities will be successful. I urge appropriators to reject the drastic cuts proposed to S&T's budget.

As the Chairman of this subcommittee, I take my oversight responsibility at CISA and S&T seriously. That said, it is hard to do effective oversight when Congress has given an agency a mission that the President's budget doesn't fully support.

In the mean time, I look forward to understanding how this committee can help CISA clarify its cybersecurity responsibilities among its interagency partners, particularly in the absence of a permanent Secretary.

Now that CISA has publicly released a National critical functions list, I will be interested in understanding how it will coordinate across sectors and the interagency to develop the risk register.

I will be interested to know how we can support S&T's efforts to equip DHS's components and first responders across the country with the technology they need to do their jobs better and safer.

I look forward to the conversation we will have today, and I yield back the balance of my time.

[The statement of Chairman Richmond follows:]

STATEMENT OF CHAIRMAN CEDRIC L. RICHMOND

APRIL 30, 2019

I would like to thank the witnesses for being here today to discuss an important priority for this committee: Funding the cybersecurity, infrastructure security, and innovation missions at the Department of Homeland Security. But before I begin, I would like to send my condolences to the victims and families of the recent synagogue shooting in California. We are keeping the Poway community in our thoughts this week. But thoughts and prayers aren't enough. We also need to demand more of the President and his administration in the face of the rising threat of white nationalism and anti-Semitism seriously.

Returning to the topic of today's hearing, I want to begin by thanking Full Committee Ranking Member Rogers and Subcommittee Ranking Member Katko for joining committee Democrats in writing to appropriators to seek additional funding for CISA's cybersecurity mission. From election security to supply chain security, we ask more of DHS's cybersecurity arm every year. Despite CISA's growing mission, its budget has remained stagnant. Since taking office, the President and those around him have paid a lot of lip service to issues related to cybersecurity and innovation but there hasn't been much follow-through. In February, for example, the

President touted his innovation agenda but his fiscal year 2020 budget slashes funding for S&T by nearly one-third. In September, former Secretary Nielsen stated that "cyber attacks now exceed the risk of physical attacks."

Yet the President's fiscal year 2020 budget would cut CISA's cybersecurity funding. Last fall, the White House released the National Cyber Strategy, which, among other things, promised to "further enable the Department of Homeland Security (DHS) to secure Federal department and agency networks." But the fiscal year 2020 budget failed to request additional funds or additional authorities for CISA's Federal network security mission. And although officials throughout the administration have declared that election security is a priority, no one in the White House has been directed to coordinate a Federal response and it has never been a budget priority. Instead, this National security issue seems to be viewed as a "hot potato" in the President's inner circle, not worthy of a "whole-of-Government" approach. To complicate matters, all of this is happening in the absence of a White House Cybersecurity Coordinator, which the White House eliminated last year. The Mueller Report makes clear that our adversaries will continue to meddle in our elections. And DHS and FBI have issued numerous warnings about threats our adversaries—from Russia and China to Iran and North Korea—pose to our critical infrastructure.

The threats we face are constantly evolving. Our technology must do the same. In short, the time has come for less talk and more action. If the White House won't lead, then Congress will. I am hopeful that our bipartisan efforts to secure the additional funding for CISA's cybersecurity activities will be successful, and I urge appropriators to reject the drastic cuts proposed to S&T's budget. As the Chairman of this subcommittee, I take my oversight responsibility of CISA and S&T seriously. That said, it's hard to do effective oversight when Congress has given an agency a mission that the President's budget doesn't fully support. In the mean time, I look forward to understanding how this committee can help CISA clarify its cybersecurity responsibilities among its interagency partners, particularly in the absence of a permanent Secretary. And I will be interested to know how we can support S&T's efforts to equip DHS components and first responders across the country with the technology they need to do their jobs better and safer.

Mr. RICHMOND. Members of the committee are reminded that under the committee rules, opening statements may be submitted for the record.

[The statement of Honorable Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

APRIL 30, 2019

Chairman Richmond, and Ranking Member Katko thank you for today's hearing on "Resourcing DHS's Cybersecurity and Innovation Missions: A Review of the Fiscal Year 2020 Budget Request for the Cybersecurity and Infrastructure Security Agency and the Science and Technology Directorate."

I thank today's witnesses:

Panel 1

- The Hon. Christopher C. Krebs, director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security; and
- Mr. William Bryan, senior official performing the duties of the under secretary for science and technology, Science and Technology Directorate, U.S. Department of Homeland Security.

This hearing will allow the committee to examine the President's fiscal year 2020 request for the Cybersecurity and Infrastructure Security Agency (CISA) and Science Technology Directorate (S&T) within the Department of Homeland Security.

As hard as one person in our Government is working to stop cyber attacks there are likely another thousand attempting to breach a system or device owned by a United States citizen.

Last September, former Secretary Kirstjen Nielsen stated that "cyber attacks have exceed the risk of physical attacks," yet the President's budget request fails to adequately prioritize DHS's cybersecurity mission.

The fiscal year 2020 budget requests $1.608 billion in appropriations for all of CISA's activities excluding the Federal Protective Service (FPS), which is funded by fees.

The fiscal year 2020 request is a $73 million cut from the fiscal year 2019 enacted levels of $1.681 billion.

The President's budget makes cuts across CISA's missions.

Cuts to Federal network security run counter to the objectives of the National Cyber Strategy, the DHS Cybersecurity Strategy, and the DHS Cybersecurity Strategy Implementation Plan.

For example, the September 2018 National Cyber Strategy issued by the White House states that:

"The Administration will act to further enable the Department of Homeland Security (DHS) to secure Federal department and agency networks . . . This includes ensuring DHS has appropriate access to agency information systems for cybersecurity purposes and can take and direct action to safeguard systems from the spectrum of risks." It also states that the administration will "continue to deploy centralized capabilities, tools, and services through DHS."

I find it baffling that this administration talks tough about cybersecurity but cuts funding to essential cybersecurity programs.

The President's budget proposal neither seeks additional authorities to empower DHS to secure the .gov domain, nor does it seek additional funding to deploy centralized cybersecurity capabilities.

As adversaries seeking to undermine our Nation's public elections and disrupt the cyber ecosystem that fuels our economy become more sophisticated and prolific, they must be outmatched by a capable and response DHS.

The threats made possible by the internet are numerous and include:

- Bot-nets;
- Ransom-ware;
- Zero Day Events;
- Mal-ware;
- Denial-of-Service Attacks;
- Distributed Denial-of-Service Attacks;
- Pharming;
- Phishing;
- Data Theft;
- Data Breaches;
- SQL Injection;
- Man-in-the-middle Attack.

The list goes on, but suffice it to say that as hard as one person in our Government is working to stop cyber attacks there are likely another thousand attempting to breach a system or device owned by a United States citizen.

According to the Mueller Report and the report from our intelligence communities entitled, "Background to Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution."

Russia used every cyber espionage tool available to influence the outcome of the 2016 Presidential election to conduct a multi-faceted campaign that included theft of data; strategically-timed release of stolen information; production of fake news; and manipulation of facts to avoid blame.

I have two concerns, which are:

- the security and integrity of the elections process; and
- the use of sophisticated cyber attacks fueled by botnets.

I have been persistent in my efforts to protect the rights of disenfranchised communities in my district of inner-city Houston and across the Nation.

Throughout my tenure in Congress, I have co-sponsored dozens of bills, amendments, and resolutions seeking to improve voters' rights at all stages and levels of the election process.

This includes legislation aimed at:

1. Increasing voter outreach and turnout;
2. Ensuring both early and same-day registration;
3. Standardizing physical and language accessibility at polling places;
4. Expanding early voting periods;
5. Decreasing voter wait times;
6. Guaranteeing absentee ballots, especially for displaced citizens;
7. Modernizing voting technologies and strengthening our voter record systems;
8. Establishing the Federal Election Day as a National holiday; and
9. Condemning and criminalizing deceptive practices, voter intimidation, and other suppression tactics.

I also authored H.R. 745 in the 110th Congress, which added the legendary Barbara Jordan to the list of civil rights trailblazers whose names honor the Voting Rights Act Reauthorization and Amendments Act.

This bill strengthened the original Voting Rights Act by replacing Federal voting examiners with Federal voting observers—a significant distinction that made it easier to safeguard against racially-biased voter suppression tactics.

In the 114th Congress, I introduced H.R. 75, the Coretta Scott King Mid-Decade Redistricting Prohibition Act of 2015, which would prohibit States whose Congressional districts have been redistricted after a decennial census from redrawing their district lines until the next census.

The voting rights struggles of the 20th Century are now joined by voting rights threats posed by the 21st Century.

Russia an adversary of the United States, engaged in repeated attempts to interfere in the 2016 Presidential election, which prompted an unprecedented "all-of-Government" effort to alert local and State election administrators to be aware of the threat.

Russia was reported to have breached 21 local and State election systems, with later reports suggesting this number was larger than initially reported.

In February 2018, special counsel Robert Mueller released indictments of 13 Russians, at least one of whom has direct ties to Russian President Vladimir Putin.

The Mueller Report was released and the most relevant sections dealing with Russia's interference using technology have been redacted.

That Russia used cyber intrusions to attack United States political institutions to collect data to manipulate the media and the public with the purpose of influencing the outcome of the 2016 Presidential elections is now an undisputed fact.

Because of what was known at the time, on January 6, 2017, Homeland Security Secretary Johnson, as one of his last official acts under the Obama administration, designated election systems as critical infrastructure, and created a new subsector under the existing Government Facilities Sector designation.

On that same day, President-Elect Trump was briefed by the intelligence community that Vladimir Putin had directed the cyber attack on the United States of America.

Since then, intelligence officials have continued to warn that foreign governments—including Russia, Iran, and China—could attempt to interfere in U.S. elections.

In February 2018, 6 intelligence agency chiefs issued a dire warning about the Kremlin's on-going efforts to influence the U.S. elections.

On January 29, 2019, the director of national intelligence testified before the Senate Select Committee on Intelligence that our adversaries "probably already are looking to the 2020 U.S. elections as an opportunity to advance their interests.

The House Committee on Homeland Security has the responsibility of providing for the cybersecurity of Federal civilian agencies as well as the security of the Nation's 16 critical infrastructure sectors from cyber and other threats.

The Election Infrastructure Subsector covers a wide range of physical and electronic assets such as storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of State and local governments.

The work to secure our Nation's election system from cyber threats is on-going, which is why this hearing on the administration's cybersecurity budget priorities is relevant.

The U.S. Department of Homeland Security's (DHS) mission in cybersecurity and infrastructure protection is focused on enhancing greater collaboration on cybersecurity across the 16 critical infrastructure sectors and the sharing of cyber threat information between the private sector and Federal, State, and local partners.

BOTNET THREAT AND THE INTERNET OF THINGS (IOT)

While connected devices are transforming our personal and working lives in a multitude of ways, they are also a growing security risk—attackers are hijacking these devices and turning them into internet of things botnets.

Botnet attacks have become commonplace, with CenturyLink Threat Research Lab estimating that 195,000 such attacks take place every day and Accenture putting the average cost at $390,752.

As new wireless technologies enter the commercial and consumer space attackers are finding different ways to launch more complex and devastating exploits.

The proliferation of IoT-enabled devices is making for new rich targets for attackers who are increasingly using IoT devices to build their botnets.

We must be steadfast in our resolve to have a strong shield to defend civilian and critical infrastructure networks for all threats foreign and domestic.

We must develop an effective deterrent to foreign tampering in our domestic affairs and especially in the critical area of local, State, or Federal public elections.

I look forward to the testimony of today's witnesses. Thank you.

Mr. RICHMOND. We now have Mr. Katko to read his opening statement.

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

So also, thank you to the Chair of is the whole committee, Mr. Thompson, for being here, as well.

Our Nation faces digital and physical threats daily, hourly, by the minute, by the second, really, that have the potential to disrupt, damage, and destroy their targets.

These threats are only growing in magnitude, frequency, and sophistication in the years ahead. We have had several major attacks in my district alone in the last few weeks. They are going to continue, obviously.

The Federal Government must work with partners across the public and private sectors, not only to prevent and deter current threats, but also to evolve to meet those of the future.

Congress recognizes the need, and last year passed the Cybersecurity and Infrastructure Security Agency Act of 2018.

This act created the Cybersecurity and Infrastructure Security Agency, or CISA for short, to serve as the Nation's risk adviser, providing for the timely sharing of information, analysis, and assessment and facilitating mitigation and resilience, building to partners across Government and industries.

Their motto is to "Defend today and Secure tomorrow." Their mission is expansive. CISA is responsible for securing the civilian Federal networks, comprised of 99 civilian agencies, monitoring emerging threats across sectors 24/7/365, securing our Nation's chemical facilities, partnering with public and private sector to protect soft targets in crowded places, and identifying and addressing risks to our National critical functions.

It is crucial that CISA has a budget and the human capital necessary to be successful. Today, we will take a closer look at their plans and how they intend to carry out and achieve their mission.

I am also interested in hearing from National critical functions' list in the new binding operational directive release today.

Today, we also will hear from the Science and Technology Directorate for 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.

Like my colleague, the Chair of this committee, said, Mr. Richmond, there is bipartisan support to increasing your budgets. We understand the critical function you play. We understand that you need more money to be able to do it properly. I fully support that notion.

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

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

APRIL 30, 2019

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.

The Federal Government must work with partners across the public and private sectors not only to prevent and deter current threats, but also to evolve to meet those of the future.

Congress recognized this need and last year passed the Cybersecurity and Infrastructure Security Agency Act of 2018. This Act created the Cybersecurity and Infrastructure Security Agency, or CISA, to serve as the Nation's risk advisor, providing for the timely sharing of information, analysis, and assessment, and facilitating mitigation and resilience building to partners across Government and industries.

Their motto is to "Defend today and Secure tomorrow," and their mission is expansive.

CISA is responsible for: Securing the civilian Federal networks, comprised of 99 civilian agencies; monitoring emerging threats across sectors 24/7/365; securing our Nation's chemical facilities, partnering with public and private sector to protect soft targets and crowded places; and identifying and addressing risks to our National critical functions.

It is critical that CISA has the budget and the human capital necessary to be successful.

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

Today we also will hear from the Science and 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. KATKO. Before I yield back, Mr. Chairman, I want to ask that we add Congressman Rogers' written testimony to the record, since he was unable to be here.

Mr. RICHMOND. Without objection.

[The statement of Ranking Member Rogers follows:]

STATEMENT OF THE HONORABLE MIKE ROGERS

APRIL 30, 2019

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

The threat landscape is continuing to evolve both in the cyber and physical space. Threats can be technological, man-made, or natural, and can emerge from nation-states, criminal organizations, terrorists, and others seeking to cause havoc.

In our increasingly connected world, even the most seemingly unsophisticated of threats has the potential to do great damage.

The Cybersecurity and Infrastructure Security Agency partners with all levels of government and across industries to better manage and mitigate risk to secure against these threats.

CISA is spearheading initiatives to secure our supply chain, working with States to protect our elections, monitoring networks, securing chemical facilities and planning and preparing for emerging threats.

CISA's work is critical and I was pleased to join with Chairman Thompson to request an increase to CISA's funding for this upcoming year.

I look forward to hearing from CISA about their plans to defend today and secure tomorrow.

Thank you to S&T for appearing before us today. I look forward to hearing from you on the fiscal year 2020 budget request.

Thank you and I yield back.

Mr. KATKO. With that, Mr. Chairman, I yield back.

Mr. RICHMOND. I now recognize the Chairman of the full Committee on Homeland Security, Mr. Bennie Thompson, from Mississippi for an opening statement.

Mr. THOMPSON. Thank you, Mr. Chairman. Thank our witnesses for their presence today.

I am pleased to have the opportunity to examine an issue critical to our National security posture, the budget requests for the Cybersecurity Infrastructure Security Agency, CISA, and the Science and Technology Directorate.

The past month at the Department of Homeland Security has been a tumultuous one. The President dismissed the Secretary, the under secretary for management, the director of the Secret Service, and the acting director of Immigration and Customs Enforcement.

At the same time, the Mueller report, even in its redacted form, crystalizes the threats of foreign election interference, as the 2020 elections approach.

Over the weekend, 1 person died and 3 were injured during a Passover services at a California synagogue, 6 months to the day of the Pittsburgh synagogue shooting that killed 11, underscoring the growing threat of domestic terrorism at the hands of emboldened white nationalists, as we are a month away from hurricane season, and there is no Senate-confirmed FEMA administrator.

In short, the Nation is facing increasingly complex threats, and requires sturdy leadership to confront them. That is why I am pleased that Director Krebs and Acting Under Secretary Bryan are here to talk about the budgets for components charged with leading civilian cybersecurity efforts, protecting critical infrastructure and developing technologies that make us safer and more secure.

For the record, I have serious concerns regarding the President's fiscal year 2020 budget request for both CISA and S&T. Last September, the former DHS Secretary observed that cyber attacks now exceed the risk of physical attacks. Since the President submitted his last budget request, the FBI and DHS issued a joint technical alert warning about Russian cyber attacks against critical infrastructure.

Ransomware attacks have already wreaked havoc on local governments from Atlanta to Albany, and the Federal Government announced that the Chinese government engaged in a 12-year cyber espionage campaign targeting intellectual property and trade secrets.

The list is far from complete. After each incident, we have looked at CISA to help us understand and mitigate the consequences and secure the ecosystem from future attacks.

Moving forward, we look to CISA to continue its work improving the cybersecurity posture of 99 Federal agencies, ensure a secure 5G rollout, and help State and local governments keep bad actors out of our election systems.

Yet, the President's budget would decrease funding for CISA's cybersecurity budget from fiscal year 2019 levels. In a context of the current threat environment, even level funding is as dangerous as a cut.

I commend CISA's leadership for proactively attacking many of these threats head-on, including by making its cybersecurity capabilities available to Presidential campaigns.

The Mueller report provided for greater details on the scale and scope of Russian election interference efforts, particularly, how the Russians manipulated and hacked information from campaigns to sow deeds of discord and sway votes.

I am glad that CISA is willing to do its part to prevent all forms of election interference. But I am worried that we are writing checks in this fiscal year 2020 budget that we can't cash, especially given its important responsibilities to other critical infrastructure sectors.

Toward that end, I will be interested to know the level of engagement CISA will be able to undertake under the budget request, and how it will grow its support if Congress provided additional funding.

I would also like to raise concern about the funding level requested for S&T. For too long, we have deferred investment in innovative security technologies to fund operation in funding the President's Southern Border wall.

But these cuts have consequences, from reducing first-responder training and technology, testing opportunities, by closing National urban security technology laboratories, to shrinking homeland security researcher communities, by cutting university programs and Centers of Excellence.

The program fiscal year 2020 budget shortchanges the future for political wins today. I will fight to restore funding to improve innovation activities at S&T.

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

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

APRIL 30, 2019

I am pleased to have the opportunity to examine an issue critical to our National security posture: The budget request for the Cybersecurity and Infrastructure Security Agency (CISA) and the Science and Technology Directorate. The past month at the Department of Homeland Security has been a tumultuous one. The President dismissed the Secretary, the under secretary for management, the director of Secret Service, and the acting director of Immigration and Customs Enforcement. At the same time, the Mueller Report—even in its redacted form—crystalizes the threat of foreign election interference as the 2020 elections approach.

Over the weekend, 1 person died and 3 were injured during Passover services as a California synagogue—6 months to the day of the Pittsburgh synagogue shooting the killed 11—underscoring the growing threat of domestic terrorism at the hands of emboldened white nationalists. And we are a month away from hurricane season and there is no Senate-confirmed FEMA administrator. In short, the Nation is facing increasingly complex threats and requires steady leadership to confront them. That is why I am pleased that Director Krebs and Acting Under Secretary Bryan are here to talk about the budgets for components charged with leading civilian cybersecurity efforts, protecting critical infrastructure, and developing technologies that make us safer and more secure.

For the record, I have serious concerns regarding the President's fiscal year 2020 budget request for both CISA and S&T. Last September, the former DHS Secretary observed that "that cyber attacks now exceed the risk of physical attacks." Since the President submitted his last budget request:

- the FBI and DHS issued a joint technical alert warning about Russian cyber attacks against critical infrastructure;

- ransomware attacks have wreaked havoc on local governments from Atlanta to Albany; and,
- the Federal Government announced that the Chinese government engaged in a 12-year cyber espionage campaign targeting intellectual property and trade secrets.

This list is far from complete, and after each incident, we have looked to CISA to help us understand and mitigate the consequences and secure the ecosystem from future attacks. Moving forward, we will look to CISA to continue its work improving the cybersecurity posture of 99 Federal agencies, ensure a secure 5G rollout, and help State and local governments keep bad actors out of their election systems. Yet the President's budget would decrease funding for CISA's cybersecurity budget from fiscal year 2019 levels. In the context of the current threat environment, even level funding is as dangerous as a cut. I commend CISA leadership for proactively tackling many of these threats head-on, including by making its cybersecurity capabilities available to Presidential campaigns. The Mueller Report provided far greater detail on the scale and scope of Russian election interference efforts, particularly how the Russians manipulated hacked information from campaigns to sow discord and sway votes. I am glad that CISA is willing to do its part to prevent all forms of election interference. But I'm worried it is writing checks its fiscal year 2020 budget can't cash, especially given its important responsibilities to other critical infrastructure sectors. Toward that end, I will be interested to know the level of engagement CISA would be able to undertake under the budget request and how it would grow its support if Congress provided additional funding.

I would also like to raise concerns about funding level requested for S&T. For too long, we have deferred investments in innovative security technologies to fund operations and funding the President's Southern Border wall. But these cuts have consequences. From reducing first responder training and technology-testing opportunities by closing National Urban Security Technology Laboratory to shrinking homeland security researcher community by cutting university programs and Centers of Excellence, the President's fiscal year 2020 budget shortchanges the future for political wins today. I will fight to restore funding to important innovation activities at S&T.

Mr. RICHMOND. Thank you, Mr. Chairman.

I will now 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 the DHS's cybersecurity activity since 2017. He has been an integral player in shaping and developing the Department's election security capabilities.

I would also like to welcome William Bryan, the senior official performing the duties of the under secretary, who has been leading the Science and Technology Directorate since May 2017.

Prior to his service at DHS, Mr. Bryan held multiple leadership roles at the Department of Energy and Department of Defense.

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

I now ask each witness to summarize his statements for 5 minutes, beginning with Director Krebs.

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

Mr. KREBS. Chairman Richmond, Ranking Member Katko, and Members of the subcommittee, thank you for today's opportunity to testify regarding the Cybersecurity and Infrastructure Security Agency, or CISA's, 2020 budget request.

CISA leads the National effort to safeguard and secure Federal networks and critical infrastructure from cyber and physical threats. In this sense, we serve as the Nation's risk adviser.

To further our efforts in this mission, it is critical that across Government industry we have clarity and common sense and purpose on what it is we need to protect. Earlier today I announced that we reached a new milestone within CISA, by identifying a set of National critical functions.

The NCFs are functions of Government in the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, National economic security, National public health or safety, or any combination thereof.

NCFs represent an evolution in the Nation's risk management efforts by focusing on how entities or organizations enable functions or services across the economy, allowing for a better understanding of cross-cutting risk factors in the increasingly interdependent nature of connected infrastructure.

The National critical function's effort is just one example of how CISA is leading the Nation's risk management efforts and will serve as a road map to guide CISA activities in the coming years.

Today, I would like to briefly touch on five of those activities; protection of Federal networks, election security, operational technology, supply chain risk management, and soft-target security.

Across the Federal Government, we have better I.T. capabilities Government-wide. We are on a path to standardization, and leadership awareness at the Cabinet level is increasing.

By issuing guidance or directives to Federal agencies, providing tools and services and implementing cybersecurity initiatives, we are protecting Government and critical infrastructure networks from malicious actors.

Binding operational directives have yielded significant results for Federal cybersecurity. For instance, we have reduced the time agencies were taking to patch critical vulnerabilities from an average of 219 days in 2015, to an average around 20 days today. In many cases, that is better than industry. But we can do better.

Yesterday, I issued an updated directive requiring even shorter mitigation time frames for a broader category of vulnerabilities.

In January, we also issued an emergency directive to protect Federal networks from a global campaign tampering with the internet's phonebook, known as DNS. This year's budget will develop efforts to centralize DNS resolution for the Federal Government.

Perhaps the highest-profile threat today is attempts by nation-state actors to interfere in our elections. Over the last 2 years, we have become close partners with the election community.

Our efforts to protect 2020 are already under way. We will focus on broadening the reach and depth of our assistance, emphasizing the criticality of election auditability, prioritizing the need to patch vulnerabilities, and developing locality-specific cybersecurity profiles.

Operational technologies, such as industrial control systems, are those components that operate our critical infrastructure. The increasing integration and connectivity of these technologies has vastly increased the potential impact of cyber threats.

Included in this year's budget is a request for a voluntary pilot that will deploy network sensors to detect malicious activity on

critical infrastructure networks, including industrial control systems.

Next, supply chain security is also critical to managing risk. CISA chairs DHS's seat on the Federal Acquisition Security Council. This council, established by law last December, will provide a coordinated approach across the Federal Government to supply chain security.

Our success depends on collaboration with industry experts, though. CISA's supply chain risk management task force has brought together 20 Federal agencies and 40 of the largest companies in the information technology and communications sectors to reach consensus on how to best manage risk.

CISA also remains focused on physical threats. On Saturday, we were once again deeply saddened to learn of the tragic shooting in a synagogue in Poway, California.

Far too often, our Nation is confronted with another violent attack on places such as entertainment venues and places of worship or schools. Earlier this month, CISA updated and released a resource guide on securing such soft targets and crowded places.

Before closing, research and development is critical to CISA's mission. CISA and S&T are committed to effective coordination on R&D. We are working together on R&D for cyber data analytics, and we will make R&D investments in mobile security to include emerging 5G security requirements.

We are also looking at innovative approaches to securing soft targets and crowded places from attacks.

In closing, I would like to thank the committee for its continued support of CISA and our mission. The authorities and resources provided over the years have helped raise this baseline of cybersecurity and mitigated countless threats to Federal networks and critical infrastructure. Thank you.

[The prepared statement of Mr. Krebs follows:]

PREPARED STATEMENT OF CHRISTOPHER C. KREBS

APRIL 30, 2019

Chairman Richmond, Ranking Member Katko, and distinguished Members of the subcommittee, thank you for the opportunity to testify regarding the fiscal year 2020 President's budget for the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The fiscal year 2020 President's budget of $3.17 billion for CISA, which includes $1.6 billion in budget authority for fees collected from Federal agencies in support of the Federal Protective Service, 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 cyber space is a core DHS mission. The fiscal year 2020 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 mission is to defend 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."

In passing the Cybersecurity and Infrastructure Security Agency Act of 2018, Congress recognized that CISA's role in fostering collaboration between and across Government and the private sector has never been more important. The threats from cyber attacks and terrorist activities to natural disasters are more complex, and the threat actors more diverse than at any point in our history.

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 hyperconnectivity, 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 2020 President's budget continues investments in Federal network protection, proactive cyber protection, and infrastructure security.

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.

Cybersecurity operations at CISA 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.

The fiscal year 2020 President's budget includes $694 million for Federal network protection, which includes Continuous Diagnostics and Mitigation (CDM), National Cybersecurity Protection System (NCPS), and Federal Network Resilience. 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, near-real time detection and prevention of malicious cyber activity.

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 2020 President's budget includes funding to continue deployment and operation of necessary tools and services for all phases of the CDM program. 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.

Within the President's fiscal year 2020 budget, $4.8 million over the fiscal year 2019 request is included to support our responsibilities to improve the cybersecurity of high-value assets within the Federal Government. With improved governance, CISA can ensure that Federal agencies are managing cybersecurity risk at a level commensurate with each agency's own risk tolerance and that of the Federal Government. These efforts will ensure that agencies achieve a minimum cybersecurity baseline through assessments, technical assistance, and architectural and design support.

The fiscal year 2020 President's budget also includes an increase of $4.4 million to begin development efforts to centralize the authoritative Domain Name System (DNS) resolution services for the Federal Government. The managed service will provide centralized DNS management for the Federal Government and a rich set of analytics that sit on top of traditional DNS services.

The fiscal year 2020 President's budget includes $371 million for proactive cyber protection. Within this category, approximately $248 million is dedicated to CISA's

National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC is CISA's operational cybersecurity center, and it provides capacity for the U.S. Government to respond rapidly to multiple significant incidents or risks. The NCCIC operates 24 hours a day, 7 days a week at the intersection of the Federal Government, State and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The NCCIC provides a broad range of information-sharing and technical assistance capabilities to assist Government and private-sector entities across all 16 sectors of critical infrastructure. In addition to information sharing and incident response, these 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.

Within the proactive cyber protection funding, $11 million is included to support the CyberSentry pilot. This voluntary pilot 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.

The fiscal year 2020 President's budget request also includes $24.1 million for State and local government cybersecurity and infrastructure assistance prioritized for election security. These resources will institutionalize and mature 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.

The fiscal year 2020 President's budget fully funds CISA's risk management activities, including $68 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. Included within the fiscal year 2020 President's Budget is a realignment of $18.4 million to consolidate core risk management programs under unified leadership. NRMC is working to publish the National Critical Functions (NCFs) list, which will enable the Federal Government and our partners to prioritize risk management actions.

For infrastructure security, the fiscal year 2020 President's budget includes $246 million for protecting critical infrastructure from physical threats through informed security decision making by owners and operators of critical infrastructure. Activities include conducting 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, including on our Nation's schools, and from emerging threats such as unmanned aircraft systems. The budget also includes a $1 million increase for the Bomb-Making Materials Awareness Program. This increase will expand capability to detect and disrupt terrorist attacks before they occur by transitioning effort to a fully-funded program of record. The funds will build a service delivery approach that achieves the scale necessary to have a strategic impact.

The fiscal year 2020 President's budget includes $167 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 assists emergency responders and relevant Government officials with communicating over commercial networks during natural disasters, acts of terrorism, and other man-made disasters.

The fiscal year 2020 President's budget includes $1.6 billion in budget authority for the Federal Protective Service (FPS). FPS provides law enforcement and protective security services to Federally-owned, -leased, or -operated facilities. FPS provides a comprehensive, risk-based approach to facility protection that allows it to prioritize operations to prevent, detect, assess, respond to, and disrupt criminal and other incidents that endanger Federal facilities and people on their properties. Federal agencies pay fees to FPS for the services they provide, and the fiscal year 2020

President's budget includes the rollout of a new fee model. The new fee model more accurately bills customers for the security services they need, and puts FPS on a path toward a more sustainable path than the previous cost-per-square-foot model.

Finally, the fiscal year 2020 President's budget also provides $224 million to consolidate CISA in a new state-of-the-art headquarters facility at DHS's St. Elizabeths Campus. CISA currently must operate from 8 different locations spread across the National Capital Region, a physical layout that poses challenges to leadership command and control requirements and which contributes to administrative and travel inefficiencies. Additionally the existing facilities do not have the capacity to fully meet CISA's requirements, and most of the leases expire in the next 4 years. Congress previously approved $120 million for St. Elizabeths construction in fiscal year 2019 which, in combination with $130 million in available carryover funds, will be used to construct the core shell for the new CISA headquarters building. The fiscal year 2020 funds are included in the DHS Management Directorate's budget and will be used for the build-out of tenant spaces, including information technology, electronic physical security, outfitting and other requirements important to maximizing CISA's ability to succeed.

A CASE STUDY: ELECTION SECURITY

One of the highest-profile threats we face today is attempts by nation-state actors to maliciously interfere in our democratic elections. Leading up to the 2018 midterm elections, DHS worked hand-in-hand with Federal partners, State and local election officials, and private-sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. This partnership led to successful implementation of a model that helps illustrate how CISA's cyber and critical infrastructure security missions complement each other, and the critical role CISA plays in bringing stakeholders at all levels together to address a common threat. We are now working to build upon these efforts during the 2020 election cycle.

In the weeks leading up to the 2018 mid-term elections, over 500 CISA employees supported election security preparedness Nation-wide. CISA provided free technical cybersecurity assistance, continuous information sharing, and expertise to election offices and campaigns. Elections Infrastructure Information Sharing and Analysis Center (EI–ISAC) threat alerts were shared with all 50 States, over 1,400 local and territorial election offices, 6 election associations, and 12 election vendors.

In August 2018, CISA hosted a "Tabletop the Vote" exercise, a 3-day, first-of-its-kind event to assist Federal partners, State and local election officials, and private-sector vendors in identifying best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery. Through simulation of a realistic incident scenario, exercise participants discussed and explored potential impacts to voter confidence, voting operations, and election integrity. Partners for this exercise included 44 States and the District of Columbia; the Election Assistance Commission (EAC); the Department of Defense; Department of Justice; Federal Bureau of Investigation; Office of the Director of National Intelligence; National Institute of Standards and Technology (NIST); National Security Agency; and the U.S. Cyber Command.

Through the "Last Mile Initiative," CISA worked closely with State and local governments to outline critical cybersecurity actions that should be implemented at the county level. This effort partnered CISA with State governments to produce county-specific cybersecurity snapshot posters. The posters contained valuable information for auditors, staff, and voters, including a checklist and time line election officials should follow to ensure security of the elections in their county. For political campaigns, CISA disseminated a cybersecurity best practices checklist to help candidates and their teams better secure their devices and systems.

On Election Day, CISA deployed field staff across the country to maintain situational awareness and connect election officials to appropriate incident response professionals, if needed. In many cases, these field staff were co-located with election officials in their own security operations centers. CISA also hosted the National Cybersecurity Situational Awareness Room, an on-line portal for State and local election officials and vendors that facilitates rapid sharing of information which gave election officials virtual access to the 24/7 operational watch floor of the NCCIC. This setup allowed CISA to monitor potential threats across multiple States at once and respond in a rapid fashion.

CISA goals for the 2020 election cycle include improving the efficiency and effectiveness of election audits, continued incentivizing the patching of election systems, and working with States to develop cybersecurity profiles utilizing the NIST framework. We will also continue to engage any political entity that wants our help. CISA

offers these entities the same tools and resources that we offer to State and local election officials, including trainings, cyber hygiene support, information sharing, and other resources.

CISA has made tremendous strides and remains committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. In February, CISA officials provided updates to election officials on the full package of security resources that are available from the Federal Government, along with a roadmap on how to improve coordination across these entities. CISA also worked with our intelligence community partners to provide a Classified briefing for these individuals regarding the current threats facing our election infrastructure.

We will remain transparent and agile in combating threats and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit across State, local, Tribal, and territorial governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the Nation are upgraded and secure, with vulnerable systems retired. These efforts require a whole-of-Government approach. The President and this administration are committed to addressing these risks.

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 for your testimony.

I now recognize Mr. Bryan to summarize his statement for 5 minutes.

STATEMENT OF WILLIAM BRYAN, SENIOR OFFICIAL PERFORMING THE DUTIES OF THE UNDER SECRETARY, SCIENCE AND TECHNOLOGY DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BRYAN. Good afternoon, Chairman Richmond, Chairman Thompson, 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 2020, which includes a request for $582.1 million for the Science and Technology Directorate within the U.S. Department of Homeland Security.

The Department's research and development activities support a broad range of DHS missions, including domain threat awareness, delivering mitigation strategies and creating novel technology and approaches for 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.

Therefore, it is my mandate to ensure an efficient, effective, and nimble organization is in place to address the R&D needs of the Department and our partners. Whether 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.

On October 1, 2018, I revitalized our structures, processes, and procedures, setting the foundation for S&T to be more agile and responsive, ready to move quickly in response of changes in the threat environment and to make use of existing technologies that can be adapted and leveraged to expedite the development of vital capabilities.

The revitalization strengthens our relationships to DHS components, first responders, and our customers, and results in a more integrated approach to innovation, requirements gathering, and problem solving.

I have realigned current R&D projects and funding to support the Department's key priorities going forward. For example, the opioid detection project to support CBP, the next-generation explosives trace detection program to support TSA and our abilities to support counter-unmanned aircraft systems' efforts across the Department.

Another key priority is cybersecurity. The 2018 DHS cybersecurity strategy emphasizes the importance of robust, cross-departmental cybersecurity R&D.

The fiscal year 2020 budget request proposes that most of DHS's cyber research and development resources are included in CISA's request. Over the last 8 months, CISA and S&T have collaborated on a plan for execution of the fiscal year 2019 funding in addition to the future year portfolio planning for 2020 and beyond.

Our teams, jointly, have identified, prioritized, and validated research and development priorities for the S&T work program, each of which can be mapped to a Departmental cybersecurity priority.

It should be noted that CISA is not our only customer for cybersecurity R&D since many of our activities with other components have a cyber nexus that must be addressed.

The fiscal year 2020 request continues to support S&T's Silicon Valley Innovation Program, or SVIP, which leverages innovative commercial capabilities from across the country through non-traditional Government contractors to rapidly deliver technology that meets validated component requirements.

To date, over 400 small business have applied to participate in SVIP solicitations. S&T has worked with 35 small start-up companies and leveraged over $400 million in private-sector investment that aligns on-going private-sector activity with DHS operational component requirements.

The budget will allow S&T to continue our commitment to first responder and disaster resilience R&D, with an additional $10.9 million to fund programs requested by FEMA that will increase re-

siliency, preparedness, and risk mitigation in support of FEMA's strategic plan.

The budget request also includes $7.1 million to continue funding the Chemical Security Analysis Center, or the CSAC. The CSAC identifies and assesses chemical threats and vulnerabilities in the United States and develops the best responses to potential chemical hazards.

CSAC has been instrumental in supporting the Nation with research and development for the rapid detection of synthetic opioids. S&T's mission is to deliver effective and innovative insights, methods, and solutions for the critical needs of DHS components and our operational partners.

Through our revitalization efforts and within the available resources provided by the 2020 budget, S&T plans to continue to build upon that mission.

Chairman Richmond, Ranking Member Katko, and the 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 follows:]

PREPARED STATEMENT OF WILLIAM BRYAN

APRIL 30, 2019

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 2020, which includes a request of $582.1 million for the Science and Technology Directorate (S&T) within the U.S. Department of Homeland Security (DHS).

The Department'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 we deliver 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.

Therefore, it is my mandate 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. In order to accomplish this, we have revitalized our structures, processes, and procedures to ensure that S&T provides impactful solutions to the ever-changing threats faced by our Nation. We will 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.

Over the past few months, we have set the foundation for S&T to be more agile and responsive, ready to move quickly in response to changes in the threat environment, and to make 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 revitalization strengthens our relationships to DHS components, first responders, and other customers, and results in a more integrated approach to innovation, requirements gathering, and problem solving.

In the fiscal year 2020 request, S&T reorganizes the Apex thrust area to, Innovative Research and Foundational Tools, which realigns current R&D projects and funding, enabling the efficient management and execution of knowledge products and capabilities to better support DHS components and front-line operators. This reorganization will focus on identifying optimal approaches and solutions that address the operators' needs through our Technology Centers (formerly Apex Engines), Technology Scouting, and initiatives that foster S&T's partnerships with industry and universities. R&D investments under this thrust area will improve requirements generation by conducting more thorough operational analysis and mission prioritization. These tools support S&T's operational blueprint model by enabling a matrixed approach to meeting customer requirements, either through identifying existing technology and innovation or by initiating new R&D efforts.

S&T is dedicated to developing or adopting innovative tools for DHS components, and the fiscal year 2020 budget request supports that effort. For example, the S&T Opioid Detection project will pilot advanced technologies, including narcotics anomaly detection algorithms and chemical sensing technologies, in CBP international mail facilities in fiscal year 2020. Additionally, the Next Generation Explosives Trace Detection (Next Gen ETD) program will support TSA's 2017 Strategic Five-Year Technology Investment Plan for Aviation Security, which calls for the deployment of Next Gen ETDs in 2020 and the development of technologies and concepts of operation that enhance passenger experiences during screening.

The 2018 DHS Cybersecurity Strategy emphasizes the importance of robust cross-Departmental cybersecurity R&D. I believe that having a strong cybersecurity R&D program is critical for DHS. The fiscal year 2020 President's budget request proposes that most of DHS's cyber research and development resources are included in Cybersecurity and Infrastructure Security Agency's (CISA) request. Over the last 8 months, CISA and S&T have collaborated on a plan for execution of the fiscal year 2019 funding, in addition to the future-year portfolio planning for fiscal year 2020 and beyond. CISA and S&T have jointly decided on cybersecurity R&D focus areas and requirements to foster partnerships and coordinate efforts between Government, industry, academia, National laboratories, and international entities to improve the global cybersecurity posture. CISA and S&T are working together to collectively leverage our knowledge, capabilities, and technology to protect our Nation's infrastructure from being undermined by our adversaries. To accomplish this, CISA and S&T leadership have identified, prioritized and validated research and development priorities for the S&T work program—each of which can be mapped to a Departmental cybersecurity priority. To do so, CISA has included S&T program managers in discussion of CISA technology road maps and technical areas in emerging risk; and S&T has included CISA in its domestic and international work programs. CISA has identified cybersecurity R&D areas where there is a need for cyber analytics as well as "big data" and "data lake" applications for cyber operations. Additionally CISA has requested that S&T focus a significant percentage of its current Cyber Security R&D portfolio on mobile devices, mobile application security, and emergency communications, to include emerging 5G LTE security requirements.

The fiscal year 2020 request continues support for S&T's Silicon Valley Innovation Program (SVIP), 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, over 400 small businesses have applied to participate in SVIP solicitations. S&T has worked with 35 small start-up companies and leveraged over $400 million in private-sector investment that aligns on-going private-sector activity with DHS operational component requirements.

The budget will allow S&T to continue our commitment to First Responder and Disaster Resilience R&D with an additional $10.9 million to fund programs requested by FEMA that will increase resiliency, preparedness, and risk mitigation in support of the FEMA Strategic Plan. Specifically, this proposed funding increase will establish a program to support a public safety and broadband implementation through research, development, testing, and evaluation of technologies that support end-user implementation.

The fiscal year 2020 President's budget request includes $7.1 million to restore funding for Chemical Security Analysis Center (CSAC) operations. CSAC identifies and assesses chemical threats and vulnerabilities in the United States and develops the best responses to potential chemical hazards. CSAC will continue directly supporting on-going work with customers, including work on chemical multifunction de-

tectors, analysis and response to chemical incidents, and development of mitigation strategies to protect the public. CSAC has been instrumental in supporting the Nation with research and development for the rapid detection of synthetic opioids.

The fiscal year 2020 President's budget request maintains S&T's Test and Evaluation (T&E) program at $7.7 million. T&E helps DHS acquisition programs to be completed at a lower cost and on schedule. While many factors determine the success of an acquisition, conducting T&E allows DHS program managers to identify issues earlier and address concerns faster based on a scientific and independent evaluation. S&T's T&E efforts support every major program on the Department's Major Acquisition Oversight List (MAOL) by providing valuable independent and scientific based input at each Acquisition Review Board before a program advances to initial or full production or deployment decisions.

The fiscal year 2020 budget request allows for the continuation of the university-based Centers of Excellence (COE) that are focused on homeland security mission needs. COEs that will receive funding in fiscal year 2020 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 are focused on transferring or transitioning research and technology outputs into field use.

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. Through our revitalization efforts and within the available resources provided by the fiscal year 2020 President's budget, S&T plans to continue and build upon that mission.

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 both witnesses for your testimony.

I now recognize myself for 5 minutes for questions.

This is not a trick question, I just really would appreciate a yes or no as to the best of your ability.

Our intelligence agencies and the Mueller report both confirm Russian election interference. Do you have any reason to dispute those assertions from our intelligence community and the Mueller report?

Mr. KREBS. No, sir.

Mr. RICHMOND. Do you agree that election interference is a real and dangerous threat that must be addressed?

Mr. KREBS. Yes, sir. I do.

Mr. RICHMOND. With that, let me ask you some other questions that are not yes or no.

Who at the White House is leading the whole of Government election security effort?

Mr. KREBS. So presently we work closely with the NSC on election security-related policy issues. We have clear guidance from Ambassador Bolden and the National Security Council on what it is they expect of us to do.

When it comes down to actual execution of election security efforts across the interagency, we also have very clear understanding of our lanes in the road between the intelligence community, the FBI, the law enforcement community and my team at DHS CISA.

The intelligence community works to find out what the bad guys are doing. The FBI works to help take them off the table, arrest or whatever. Then, my team works with State and local election officials to provide them an understanding of the threat landscape

and provide them the tools, capabilities, training exercise, what other capacity-building capabilities, in support of their efforts.

Mr. RICHMOND. I know that you would be interested in information sharing. The FBI is focused on collecting evidence and building a case.

I guess I am a sports guy, so I do sports analogies, and I understand that everybody has their different routes to run and their different assignments. Somebody is going to block; somebody is going to do that.

Who is the quarterback, is my question? Who is making sure that everybody is running their routes, blocking who they are supposed to block and tackling who they should tackle?

Mr. KREBS. So there are head coaches, there are defensive coordinators and there are offensive coordinators in this analogy.

Mr. RICHMOND. Who is the head coach?

Mr. KREBS. So the President is the head coach. We have offensive and defensive coordinators across the bat, but when you talk about this law enforcement coordination piece and the investigatory piece, we have improved relationships with the FBI on sharing information, deconfliction of actual on-network sorts of activities, where I am trying to get in there and help the victim recover their networks, while the FBI is trying to figure out who is doing this, who the bad guy is, whether it is Russia or whomever.

There is a process. Now I will say, the process needs to improve. The FBI has a long history of processes and procedures. They have been at this game a bit longer than my team has. We are still evolving. I still see CISA as an agency is a bit of a start-up.

So we are still working internally to build the processes that we need so that we can work with the Defense Department. We can work with the FBI. We can work with the intelligence community to ensure that we are doing the things that we need to do to ensure the victims are protected.

Mr. RICHMOND. Is there one person who wakes up every day to make sure that you all are coordinated, and that is their sole responsibility? So who would be the offensive and defensive coordinator?

But I am talking about somebody whose own responsibility, look, the President has a whole bunch of things that he has to work on. But is there someone in the White House or anywhere else that wakes up to make sure that you all are coordinated with the FBI, who is coordinated with the CIA and that everybody is doing what they are supposed to do?

Mr. KREBS. There is an entire directorate within the National Security Council that is focused on cybersecurity. There is a director focused on the resilience.

So there are a number of officials at the White House and the Executive Office of the President and the NSC that support our efforts. Again, from a policy perspective, you know, we are the operational agencies. I have all the authorities I need to go do my job.

So when I wake up every day, I am figuring out how to make sure State and local election officials are getting the support they need, just like the FBI when they go out and they do their job, and the intelligence community they do their job.

Mr. RICHMOND. The fiscal year 2020 budget request, if enacted, will cut CISA's budget below the 2019 funding levels. How would you manage those cuts, and how would spread them across CISA?

Mr. KREBS. So I think you have to think through the budget formulation process.

So the fiscal year 2020 budget process was started in about 18 months or so ago, actually, before I was really in a leadership position at the agency. It is, truly, what I would call, and this is an NPPD budget, so it is a legacy budget.

What we are doing right now is, we are standing up. As we are standing up CISA, we are trying to figure out what we want to be when we grow up. So 2 years from now, where do we want to be positioned?

There are a number of unmet requirements, I think, that we are discovering. I think today's release of the National critical functions, alone, is representative of the potentiality of this agency.

So we identify 55 functions. This is an evolution of the risk management thinking beyond 16 sectors. This is 55 functions that really, truly impact National security, economic security, public health and safety.

So I can address at current a number of these functions. I think election security is a great example. Congress has invested in my agency, to date, close to $60 million purely focused on election security.

I don't think outside of Federal networks, I don't think I have another critical infrastructure sector that Congress has invested specifically to that level.

If you factor in the, well, $22.3 million in the fiscal year 2020 request, that is over $80 million on a National critical function.

Mr. RICHMOND. I am a minute over, so I will just ask you a very simple question. If we doubled your budget, would you spend it all?

Mr. KREBS. Yes, sir. Absolutely.

Mr. RICHMOND. Thank you.

With that, I will yield to the Ranking Member Mr. Katko.

Mr. KATKO. Thank you, Mr. Chairman, I appreciate it.

Just a quick question, well, not a quick question. This is more of a detailed question, actually. In Albany, New York, not far from my district, there was a recent ransomware attack that could have affected the police department's patrol vehicles. I am horrified to think what could have been done if they got into those systems.

How does CISA perform outreach to State and local governments like these? Can that outreach be improved with proper funding?

Mr. KREBS. I think we have a lot of room to grow in State and local engagement. It is interesting that you mention Albany, New York, because actually one of our key partners in engaging with State and local officials, election or otherwise, is based in Albany. It is the Multi-State Information Sharing and Analysis Center.

We fund the MSISAC on an annual basis. You have heard me talk about our Albert sensors before, or our network net flow and intrusion detection systems. They manage that process for us.

So what more can I do? This is not something that gets fixed overnight. Working with State and local officials, again, election or not, the progress has to first be made on the relationship-building in the trust side.

I have a lot of tools that, if I was given more resources, I could scale those tools. But the thing I can't buy overnight, I can't go build with an engineer, is the relationship and the trust between these officials.

So it is going to take time, it is going to take people, and it is going to take relationship development. But with the appropriate resources, I can get all those things done in due time.

Mr. KATKO. I mean, and I would like to follow up on another area. What percentage of the homeland security grants, to your knowledge, go toward cybersecurity?

Mr. KREBS. I would have to get back to you on the specifics of the budget, the grant budget. But I will say this, that the last year was the first year that, in the Homeland Security Grant Program, that there was two important elements: A requirement for an investment justification for cyber expenditures, as well as the requirement to include a CIO or CISO on the decision board at the State level.

That has been carried through to this year. But, you know, it is out of the same big pot of money that we have a number of other requirements set against and we have historically had those requirements set against.

Mr. KATKO. Now, last week I had the pleasure to spend quite a bit of time at Syracuse University in their quantum computing research area. To say that my head hurt when I got done is an understatement. They are very smart people, but quantum computing is a real threat. It is a very real threat in the cyber area, as far as our cyber defenses.

So as CISA is thinking about securing tomorrow, how are you preparing for the potential effects of quantum and other emerging technologies on critical infrastructure?

Mr. KREBS. So as I think of emerging technologies, whether it is quantum or artificial intelligence, machine learning, some of those things are here in certain respects. I have to look at both sides of the opportunity, as well as the potential risk; 5G is actually a fantastic example of this right now.

So one of the things that I am doing, that I plan to do is we will use this National critical functions set, 55 functions, to work with stakeholders to understand what the potential impacts on them may be.

Ultimately, critical infrastructure in the United States—and I don't have the primary source here—85 percent owned and operated by the private sector. We have heard that number time and time again.

So when I want to understand where the risk is, where I want to understand what the potential impacts are, I go to the source. I go to the people that own the networks and get a sense of what their concerns are. I am able to then bring intelligence community, the law enforcement community.

I really do sit in an interesting spot in Government and industry, that intersection of the I.C., law enforcement in the private sector and within those Government conversations, I am the advocate for the private sector.

Mr. KATKO. So what I mean, just so we are clear, could you explain to the committee just at an elementary level, because every-

one understands the threat that quantum computing is, but, basically, it is fair to say if the bad guys get the quantum computing capability before we do on a large scale, that our networks are going to be much more vulnerable. Is that fair to say?

Mr. KREBS. I think, particularly from an encryption, you know, post-quantum computing presents a number of risks to our current security configurations, encryption, password management, things of that nature. So it is something that the Federal Government is investing in quite significantly right now.

Mr. KATKO. Last, and I will be quick here. With the 55 National critical functions, you issued today, you spoke about them for a moment but I want you to expand them just briefly. How do you envision this is different from our critical infrastructure sectors and lifeline sectors? How can we assure that this does not leave anyone behind?

Mr. KREBS. So the way I think about this is, is we are increasingly connecting, is we are more interdependent. This framework, which it really is a framework more than anything, allows us to think about those things that are more important. It is not about specific organizations, businesses, banks, energy companies, whatever.

It is about the thing they do and the thing they deliver, and who is involved in delivering that service. So it actually allows us to expand and open up the aperture so that we are not leaving people behind.

I think in the current formulation it is possible that we are not hitting all the right bits and pieces of the supply chain, for instance, small and medium-size businesses.

This gives us a better appreciation of some of those niche or boutique companies that may deliver a really critical service that doesn't fall neatly within the 16 sectors.

Mr. KATKO. Well, thank you very much. I yield back the balance of my time.

Mr. RICHMOND. Thank you.

The Chair now recognizes for 5 minutes the gentleman from Mississippi, Mr. Bennie Thompson.

Mr. THOMPSON. Thank you, Mr. Chairman.

Acting Under Secretary Bryan, I will try to be a little specific on my questions. For instance, in the budget that is proposed, the Coastal Resilience Center at the University of North Carolina at Chapel Hill is scheduled for elimination. Do you support that?

Mr. BRYAN. Mr. Chairman, I support the President's budget. Having said that, I certainly appreciate the resources Congress has provided over the years and the support to the S&T folks and the mission that we have.

All of our Centers of Excellence provide great value. In fact, that particular Center of Excellence has handled about 137 technical requests and has received additional resources from outside of S&T for the work that they are doing.

But under the proposed budget, we are going to have to look at some Centers of Excellence two of them, frankly that would have to be shut down and halt the start-up of three other ones, should the President's budget be executed.

Mr. THOMPSON. So is that a yes or no?

Mr. BRYAN. All I am saying, Chairman, all the Centers of Excellence provide value. Tough decisions had to be made, when you have to reduce your budget.

Fortunately, over the past few years, we have not had to execute on some of those tough discussions that we have had to have with the budget that we have been given.

But again, we have to look at the priorities of the Department and look at some of the other mission areas of the other Centers of Excellence in making those decisions.

Mr. THOMPSON. Well, I would assume that is a maybe? You know, they do a lot with coastal resilience and we have lost immeasurable coastal properties. The Chairman's area of Louisiana is a good example of the losses.

So I would like to have the benefit, if not at this hearing, as to how we plan to replace that capacity, because it appears to be something that is vital to everything.

Coupled with that, you talked about 35 small companies you have been given contracts to as it relates to small business opportunities and what have you.

Do you have the data on how many women-owned or minority-owned or anything like that?

Mr. BRYAN. Mr. Chairman, we can get back beyond the specifics of that. We do have some programs focusing on Historically Black Colleges and Universities, as well as minority-serving institutions. If you don't mind, I can share some of those activities?

Mr. THOMPSON. Well, I would love to have it.

Mr. KREBS. Certainly.

Mr. THOMPSON. Thank you very much.

Mr. Krebs, the supply chain problem that we have identified a good bit, have you looked at how we can better manage supply chains so it does not continue to be a vulnerability?

Mr. KREBS. We have a number of efforts on-going right now. Last year we established an ICT supply chain risk management task force. I mentioned in my opening that 20 members of the Federal Government, 20 members of the I.T., and 20 members of the comms.

Basically what we are trying to do through this task force is to bring together a diverse group of players who all play in the supply chain risk management space somewhere, at some point and create more of a consistent lexicon or understanding of (A), how to share threat information.

I get information from Kaspersky Labs for instance, how can I share that out in a protected manner to people that can take action and remove the threat?

Mr. THOMPSON. Thank you. Election security.

Mr. KREBS. Yes, sir.

Mr. THOMPSON. Now that everybody agree that the Russians are a problem and that we need to do something about it, some of us are thinking about 2020 and what can we do between now and then to protect our system of elections? What is your suggestion to Members of Congress as to what we can do?

Mr. KREBS. Sir, I think about protecting 2020 every day. In fact, a couple of months, a month or so ago, out at the RSA conference in San Francisco, I gave a keynote and I actually had bumper

stickers made up that said, #Protect2020. We are all in on protecting the 2020 election.

Where I think we are going to get the most amount of progress over the next year-and-a-half, No. 1, is continuing to extend our engagement with State and local election officials. We had about 1,400 of them prior to 2018 but there are 8,800 total. So I have got to keep pushing out.

We are also going to help understand where the risk truly is in the system. What are the things that are not just vulnerable but most susceptible, where the highest consequences are?

Then once we get down, which I think we are pretty close, we need to figure out what resources are going to be required to close out those vulnerabilities. Whether anybody likes it or not there is a technology deficit in State and local governments in general but it is specifically in the election community.

So what are the resources, whether they come from the Federal Government or from State and local legislatures—that is a conversation that we need to have. We need to get resources to these people so that they can protect their system.

Mr. THOMPSON. So what you are saying is, is that technology deficit, unless it is fixed, potentially serves as a danger to the conduct of our 2020 elections?

Mr. KREBS. Sir, I think just like any other I.T. problem, which in some cases the election security issues is just an I.T. security issue, there are 15-plus-year-old machines or equipment out there that may not be managed anymore. There may not be updates available. They may be out of cycle.

So how do we get those systems, those known antiquated vulnerable systems out of the system and put the more secure stuff in? At the same time build auditability into the process and really hammer the importance of auditability across the election process.

Mr. THOMPSON. So in other words, somebody needs to provide some resources for that to occur?

Mr. KREBS. Sir, it has got to come from somewhere, yes, sir.

Mr. THOMPSON. Thank you.

I yield back, Mr. Chairman.

Mr. RICHMOND. The Chairman now recognizes Mr. Walker from North Carolina for 5 minutes.

Mr. WALKER. Thank you, Mr. Chairman. I would also like to ask the overall committee Chairman for a copy of that report on the HBCU outreach by the under secretary. We need a copy that. We would appreciate that.

Director Krebs, how does your agency interact with the Science and Technology Directorate? Can you mention the relationship?

Mr. KREBS. So SOPD Bryan, is that what I am supposed to call you? That is my old title, the senior official performing the duties here. I actually have a embed. So I have a couple of folks from his shop that work with my folks on a regular basis.

I define a set of requirements that I need support on from an R&D perspective, share that with Mr. Bryan and then he is able to align his research and development programs against my requirements. It was a top priority for both of us as we came in to ensure that we were pulling the same direction and that we

weren't, you know, in often competing research and development priorities.

Mr. WALKER. Sure. What do you consider that, to use your words, a top priority?

Mr. KREBS. Right now, I am looking at mobile security, 5G security for instance. There is a great deal of opportunity in front of both of us in terms of understanding what the risks are and how we can deploy more secured more mobile technology.

Also looking at general data analytics and I have an incredible amount of data that I am able to collect off of Federal agencies. But I don't have the tools or the horsepower and the pipes to do the right kind of work across it and analyze the true threats. So, you know, he is helping me pull together what the tools and the infrastructure would look like.

Mr. WALKER. Nice transition to the under secretary, same question for you. How would you describe your relationship or the interaction with the Cybersecurity Infrastructure Security Agency and why is that alliance important to advancing overall DHS positions?

Mr. BRYAN. One of priorities when I took over this position was to increase the relationship. We are a customer service organization. So we have to create an environment where the components and the customers and first responders have to want to work with S&T because of the value added that we bring to them.

That was not always the case across the board with the relationship between S&T and some of the components. The relationship between the former NPPD and the former leadership within S&T was not all that good. So there was not a lot of leveraging of capability.

So Director Krebs and myself both determined that we were going to fix that and we structured our and built our organizations in such a way so that I actually have a team dedicated just to servicing CISA.

I have teams dedicated to servicing every component within the Department of Homeland Security. So we are no longer in a position where you ask us for or give us a requirement and we take that and sit on it for a year and take another year to figure out how we are going to solve it. We actually have people, as he mentioned, embedded and so when a requirement comes in we can tackle it right away.

Mr. WALKER. Sure. Little bit of a concern on the duplicative efforts between the two. Can you address that and would the transfer of funds from the S&T to CISA, will that help eliminate some of the duplicity?

Mr. KREBS. So we have worked hard over the last year-and-a-half-plus to remove any redundancy or duplication of efforts. It doesn't matter where the money ends up. The job is going to get done. The job is going to get coordinated across the two of us.

If I end up with the money, I will be working with Bill and his team to transfer and execute the funds in the research program accordingly.

Mr. WALKER. Any concern from either one of you that this would create challenges fulfilling the DHS cybersecurity missions as a whole?

Mr. KREBS. Bill? I don't have any——

Mr. BRYAN. I have no concerns.

Mr. KREBS. I think this is a matter of leadership and I think they both weigh into it.

Mr. WALKER. They switched up. I have a little bit, about 80 seconds left. Although many areas within the S&T's budget requests had funding and reductions or transfers, one key thrust area that was increased with the RD&I or the Research Development and Innovation funding for border security.

Do you think this is the result of DHS's commitment to finding a solution to the crisis at the border?

Mr. Bryan.

Mr. BRYAN. Yes, I do. Not just are the crisis of the Southern Border but also the influx of opioids. So a lot of that increase had to do with helping to figure out how to find those opioids as they come in through the mail system and other places as well.

Mr. WALKER. Sure. As the Ranking Member privileged to serve on the Intelligence and Counterterrorism Subcommittee, I would like to hear your perspective on how the RD&I funding is helping to develop innovative technology products or other solutions to protect overall our Nation.

Mr. BRYAN. Well, a key element of our innovation, frankly, was within our Silicon Valley Innovative Program. That was a big benefit for us because we were able to tap into innovators, entrepreneurs, small companies, citizen scientists to help us with some of our most pending critical situations.

Mr. WALKER. OK.

Mr. BRYAN. Now, we have lost that authority, that OTFA authority which we are trying to get back, but the Silicon Valley Innovative Program was just one of many ways we are able to tap into that innovation quickly.

Mr. WALKER. OK, 10 seconds left. This last question, how has the CSA's work aligned with the 2018 DHS cybersecurity strategy? What remains to be done? If you would just hit the second part of that question, the strategy?

Mr. KREBS. Sir, we have to continue rolling out into the critical infrastructure community. The Federal network's base is pretty straightforward. It is the critical infrastructure community. I need to be able to get my tools. One thing I need to be better at is marketing and engagement. So we are going to put a lot of effort there.

Mr. WALKER. Thank you, Mr. Chairman.

Mr. RICHMOND. Thank you.

The gentlemen from Rhode Island, Mr. Langevin, is recognized for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to welcome our witnesses here today and thank you for you testimony. Thank you the job that you are doing. Before I get into my questions, I just want touch on, Chairman Richmond's question early on when we talked about, you know, who is in charge, who coordinating.

You know, the reality is that we still don't have someone in charge. I understand the analogy with the President but, you know, since we are talking sports analogies that would be equivalent to, you know, maybe the, you know, the team owner.

But, you know, who is actually executing and you don't have a Bill Belichick that person who was basically fired by the cybersecurity coordinator. So nobody really has the policy and budgetary authority to reach across Government that is pulling this together.

So that is something that we still need to focus on. I still say that we need a Senate-confirmed director with policy and budgetary authority to do that, but we will leave that for another time.

Director Krebs, I appreciate the work that you and your team are doing at CISA. But as you know, I also sit on the House Armed Services Committee and from that perspective I am fully vested in assuring that CISA has the capacity wherever possible to complete its core mission without drawing on Pentagon resources.

So developing that expertise is essential for DHS, again not having to always rely on reach-back to cyber command or NSA for expertise. You know, based on my experience, you know, I have that capacity building so where it relies on a DHS work force.

So to that end, does the budget request reflect internal efforts to train and importantly retain the DHS cybersecurity work force?

Mr. KREBS. Thank you for the question, and I would probably pick, if you asked me a different NFL head coach other than Belichick, not a Patriots fan. Look, the——

Mr. LANGEVIN. We will have to agree to disagree on that one. I think he is doing pretty good.

[Laughter.]

Mr. KREBS. When we look at the budget, particularly from a personnel perspective, we are still growing as an agency. We are still filling billets. I think I got about 1,300 folks.

Let's see, I have 1,100 cybersecurity professionals in place. There are about 361 vacant positions right now, about 40 percent of those we either have a pending decision or a hiring action against. So our vacancy rate is not huge but it is so we need to be filling those spots.

We have cross-training mechanisms in place. We are working to cross-train across not just CISA and not just DHS but through part of the President's management agenda.

We will be pushing out a cybersecurity work force academy across the entirety of interagency. But at the same time, we are looking down the road of what does our incoming pipeline look like?

Partnering with the Scholarship for Service Program to bring in college graduates and graduate programs, working with organizations like the recently announced cyber talent initiative, MasterCard-Microsoft work day just launched. You know, we need to be innovative in thinking about ways that we can bring folks in, retain them.

But, you know, if we lose them to industry it is not the worst thing in the world because if they are with me for 5, 6, 7, 8 years and then go out to industry that means I am building an alumni network that I haven't previously had, particularly along the lines of the FBI and the service academies. So we are looking at all different angles in terms of building that capacity.

Mr. LANGEVIN. Right. It is essential. I mean even USCYBERCOM says that attracting and retaining the best talent is a challenge.

So gonna follow up on this, you know, do you believe that CISA is an attractive place for technical and operational cybersecurity experts? How does the budget support efforts to make it more attractive?

Mr. KREBS. I am flat out, yes. I think it is one of the best places to work in the Federal Government. I mean, you get to go work with the critical infrastructure community, you get to work with the Federal agencies and hunt for Russian, Chinese, North Korean, Iranian actors on a daily basis. That is just plain fun.

Mr. LANGEVIN. So let me ask this before my time runs out. You know, you pledged again to work with any jurisdiction that needs cybersecurity help on the elections. But do you actually now have the personnel to do that, as well as to meet your other demands and priorities customers?

Mr. KREBS. I think at the moment we are finding that the request for our support is escalating in particular from the State and local community. I think elections have shown us that, that there is a huge unmet need out there. So as I look to the out years we are going to need to boost our capabilities, absolutely.

Mr. LANGEVIN. You know, I hope you are going to be asking for the right resources to do that and we stand ready to support you, so——

Mr. KREBS. Yes, sir.

Mr. LANGEVIN. I know my time is expired.

Thank you, Mr. Chairman, I yield back.

Mr. RICHMOND. You are welcome.

The gentleman from Texas, Mr. Taylor, is recognized for 5 minutes.

Mr. TAYLOR. Are you sure? All right. Thank you, Mr. Chairman, appreciate that.

Just going back to the conversation we had before we started this hearing in terms of municipal subdivisions of, you know, some cities', you know, utility districts. A lot of those governmental entities have personal data, right?

So they have got addresses, names, Social Security numbers, credit card information. What are the penalties in Federal law for a data breach for those organizations?

Mr. KREBS. So not necessarily an expert in specific jurisdiction by jurisdiction but there are certain cases where there are very narrowly tailored regulatory programs in place that speak to data breach issues. But general speaking it is State by State of what the requirements are to notify the public, to notify any potential victims.

Mr. TAYLOR. What actions are we taking at the Federal level to try to help cities, counties, special purpose districts, you know, subdivisions underneath the States to secure their data, to deal with cyber attacks?

Mr. KREBS. So every service pretty much that I can provide to the Federal Government I try to shift that out to State and local governments. Little-known fact, but the continuous diagnostics and mitigations program, which is basically an economies of scale where we buy a bunch of services and products for the Federal agency, that list is available to State and local government.

So what I need to do is I have really good technical capabilities. I have really good tools and services. What I need to do a better job of is building awareness across State and local governments of what those things are, how they can use them.

Quick example, last year was a really bad year for State and local governments between Charlotte and Mecklenburg County, Baltimore, Atlanta, Colorado Department of Transportation all got popped for ransomware. We took that, saw the trend lines and executed a ransomware awareness campaign, webinars, local engagement.

My field force was engaging on a local basis. We saw an uptick in services, but we have got to keep it hitting harder. We got to keep hitting it harder. A lot of these jurisdictions don't have the resources or the wherewithal to protect themselves.

Mr. TAYLOR. Shifting over to the National Risk Management Center which has only been on-line for 10 months, can you speak to what has happened there and then can—where we have come in 10 months, and where you sort-of see the future?

Mr. KREBS. Yes, sir. So the concept behind the National Risk Management Center was to take an existing organization or a subcomponent within my organization. It was more of an internal research or risk analysis feature that took a task from internal, you know, my leadership team and some other stakeholders.

Our concept was to flip it around and turn it into a storefront for industry to come in and set our risk and analytics, strategic risk analytics agenda.

So in the mean time things we have done, first and foremost, today's National critical functions effort. That was spearheaded by the National Risk Management Center, again, an evolution of risk management thinking.

The ITC supply chain risk management task force managed by the National Risk Management Center, never been done before at this scale across the interagency and within industry.

The election security efforts run out of the National Risk Management Center. But fundamentally, this is about identifying, understanding strategic risk, and driving initiatives to manage that risk today and in the future.

Mr. TAYLOR. Then you mentioned this briefly in your opening remarks about the domain name system or DNS and then can you just speak to, what are we, need to do there and sort-of what is the problem and what is the future solution?

Mr. KREBS. Right, it is the internet phone book on how you end up on that URL or that website that you are looking for.

What we found in early January during the shutdown was that somebody out there had figured out a way, not particularly sophisticated but just a concerted effort at global scale, of how to tamper or, highjack is not the right word, but tamper with that process and comprise accounts.

So what we did first and foremost was figured out what was happening across the Federal interagency and locked it down and had a better awareness. That is what we accomplished through the emergency directive.

Going forward what we think we can do is centralize some of those DNS records management processes across the Federal Government because, again, I have 99 agencies to work with.

What we want to do is provide as much centralization of services as possible so we can lock that process down. In addition, the way a lot of malware works from its command-and-control infrastructure is it beacons back and forth to the mothership using DNS lookups.

So if we can sit on top of that process we will have a better understanding of what is going on across the Federal interagency.

Mr. TAYLOR. All right.

Thank you, Mr. Chairman, I yield back.

Mr. RICHMOND. Thank you.

I now recognize the gentlelady from New York, Congresswoman Rice.

Miss RICE. Thank you, Mr. Chairman. So, Mr. Krebs, I think you were talking before I don't know if I heard this correctly but would you describe it as a resistance with State and local governments to working together with you on election security? Or is that not the right word?

Mr. KREBS. If you had asked me 2 years ago, I may have, kind-of, may have said yes. Look, I like thinking through this process from where we were, where we are now, and where we need to go. In 2016 when this all went down and we were not really as a government, State and local or Federal, really aware of the potential risk to the election process.

So when the Federal Government engaged, and it is something that is historically and by statute legislative tradition a responsibility of State and local governments, there was an immediate recoil. There was an immediate antibody that said we have got this. We don't need your help.

But from the intelligence community perspective, from DHS, we understood the risks, I think. So but when you don't have trust and you are trying to work in this space, it is an uphill climb.

But in the intervening 2 years, particularly in the run-up to 2018, just the commitment, the engagement, the providing resources and the communication that we are not trying to take elections over.

Miss RICE. Right.

Mr. KREBS. We don't want to regulate elections. We are here to help. The ship has turned entirely, 180 degrees from where we were. We work with all 50 States.

We have sensors, those Albert sensors, we just shipped the 50th. So that means every State's secretary of state at the highest level is going to be working with us on the intrusion detection system.

I am really optimistic about where we are going, but the technology deficit remains. There is work to be done. We have got to figure out how to improve and modernize and upgrade these systems.

But a lot of it is also a people problem, so we have got to continue to educate, continue to share that phishing remains one of the biggest threat vectors that the bad guys are using, particularly the Russians.

Miss RICE. So in 2016, most of the Russian efforts were targeted at the party committees, whether it was the DNC or the DCCC and the individual campaigns of elected officials.

When you testified before the full committee in February, you stated that you didn't see a problem with using the information sharing—ISAC, the Information Sharing Analysis Center—model to develop a more formal information-sharing arrangement between DHS and the political party committee and, for that matter, individual elections.

I mean, we are all up here in a constant election mode, and I can tell you I am sure I don't know the best ways to keep the political side, and this is not talking about politics here, but the fact is that those are where the attacks are happening.

So have you been able to set up an arrangement, whether it is the Republican side or the Democratic side, these party committees?

Mr. KREBS. So prior to the 2018 mid-term, we did work with all the National-level committees and some State-level committees. That is going to continue to be a priority for us, the committee level as well as the specific campaigns.

We will provide services. We will continue to do those things that we offer for States, whether it is vulnerability scanning, information-sharing mechanisms, we are going to offer those up. But I would ask, each of you are in cycle right now. Do you know if your campaign is working with us? You know, that is a good question to ask.

In the mean time, the DNC, Bob Lord, the CIO over there, I think has done a really good job of talking about the basics of security, cyber hygiene, you know, using commercial-grade email, using encrypted messaging apps, multifactor authentication, really basics.

If you do the basics, if your campaigns do the basics, I am not talking go buy some super sophisticated security widget, if you do the basics, you can address 90 some-odd percent of the threat.

Miss RICE. Right. I agree with you.

Mr. Bryan, the President's budget again proposes closing the National Urban Security Technology Laboratory, NUSTL, in Manhattan, New York. NUSTL supports the successful development, evaluation and transition of Homeland Security technologies into field use for first responders.

I have also reintroduced legislation to permanently authorize the lab which passed the House unanimously in the last Congress. Many police commissioners and fire chiefs have expressed grave concern over the President's desire to close NUSTL and hamper efforts to prevent and respond to terrorist attacks.

Every first responder agency in the New York metropolitan area utilizes NUSTL technologies, including the NYPD, the FDNY, and certainly in my district the Nassau County Police Department on Long Island. How does closing the only lab entirely focused on preparing and protecting first responders against threats of terrorism make any sense?

Mr. BRYAN. Again, ma'am, I can't say enough positive things about NUSTL myself. It is a capability and an asset with relationships they have formed in New York to be able to do the kind of

work that they are doing, and you have articulated all that very well.

My role right now and what I have to do is look at should we have to lose that capability, what would we do with the work that is going on?

Miss RICE. But do you have the power or do you feel like you have the power to voice your concern about maybe cutting in a different area other than this? That is my question. I mean, I understand the loyalty. I understand that the orders come from the top down.

But if you have a very deep, real concern, which it sounds like you do, about getting rid of this NUSTL, you know, what are the remedies? There has to be a remedy.

Mr. BRYAN. Yes, the only remedy I have and all I can do is look to where those capabilities could be performed elsewhere.

Miss RICE. But clearly they are unique to this infrastructure.

Mr. BRYAN. Yes, ma'am.

Miss RICE. I think we just have to continue that conversation. I think more people in positions like yours and Mr. Krebs' hopefully, you know, stand up and push back when things like this want to be done by the administration. Thank you both very much.

Thank you, Mr. Chairman.

Mr. RICHMOND. You are welcome.

Now the other gentleman from Texas, Mr. Ratcliffe, is recognized for 5 minutes.

Mr. RATCLIFFE. Thank you, Chairman.

I want to thank the witnesses for being here. For those that have been on this subcommittee for a while, they know that it has been an effort over multiple years on this committee to elevate DHS's cybersecurity mission through CISA.

So I was especially pleased that the President's budget request included increased funding for what is our Nation's lead civilian cybersecurity agency. I think that shows that this administration is serious about prioritizing our defenses against new and emerging cybersecurity challenges, and I have a lot of confidence that that will hopefully continue because it has to continue.

It is obvious to both of you that cybersecurity now touches literally every aspect of the world we live in. It is central to every sector of our economy. It is vitally important for protecting the most sensitive information of every American, and that makes it one of our foremost National security challenges.

In my time on the committee, I have tried to press the Department to continue to improve its work in providing the private sector with actionable real-time cyber threat intelligence, to improve as a forum for cross-sector cybersecurity work, and now to continue its good work on the continuous diagnostic and mitigation program, a program that I believe is vitally important to our cybersecurity posture.

So to that point, Director Krebs, I want to ask you, the administration's budget request includes an increase for CDM to continue providing those necessary tools and services for all phases of the program that enable our Federal I.T. networks to strengthen our security posture of those cyber networks.

I would like you to, if you can, expand on the reasons behind the increase in funding for CDM.

Mr. KREBS. Thank you, sir. Your long-term support of CISA has been a huge part of our success in getting us into an agency from NPPD. In terms of CDM, CDM is certainly one of those kind of arrows in the quiver as we protect the Federal network.

CDM is one of the reasons, one of the capabilities of why we have improved so dramatically since the OPM breach. In particular, the understanding and the ability to look across those 99 agencies and understand what, for instance, operating systems are running within their environment and help work with those agencies to get them on a road map or a path to a more secure configuration.

When I talk about dividing operational directive for patch management, vulnerability management, we are able to see what is going on in those agencies in terms of those critical vulnerabilities or those high vulnerabilities. So we can actually measure now. We have the visibility so we can see, and we can take action.

CDM will continue to be, for us, long term, whether it is understanding what is on the network, who is interacting on the network and ultimately getting down to the data protection level. It will be a core element, one of the crown jewels of Federal network security for us.

Mr. RATCLIFFE. So to that point then, is the funding level that is included, is it sufficient to advance the procurement and the installation of CDM's capabilities all the way through phase four?

Mr. KREBS. Well, I mean, when you think about the life-cycle of the program, of CDM, and it is important to keep in mind that every agency, there are 99 agencies, every agency has a different level of maturity. So some agencies may be ready to go to Phase Four well before other agencies.

So two elements of that. One, we have to continue investing in agencies and getting them up to speed and getting their systems modernized. But also it allows for a policy conversation on what do we want the future of Federal networks to look like?

My view is that having 99 different agencies to manage independently is long-term an untenable position. I think there is a model that the Department of Defense has in the DODN where they have broader span of control over the elements of the Department of Defense.

When we think about these 99 agencies, what I want to be able to do is provide more centralized services, so take some of the risk out of the hands of the departments and agencies.

Earlier this week, we were named the qualified service management offering for security services, which puts us in a shared service model out to those other Federal agencies, but really getting to a point where CIOs and CISOs or CIOs thinking more about citizen services rather than securing their infrastructure. Let my team help manage that process.

Mr. RATCLIFFE. Director, my time has expired, but just to follow up on that, because you and I have talked about this a lot, we need to be better at breaking down the initial barriers to provide agencies with real-time situational awareness and risk-based accountable information, all of which are vitally important and imperative to our Federal cybersecurity efforts.

The bottom line is this funding level, will it do that? Will it expand the CDM program to more agencies and in the end allow CISA to better protect and manage those high-value assets?

Mr. KREBS. So certainly, with more I can do more. With more people, I can work with CIOs of agencies to help them develop their plans. I can help push out a security baseline for secured configuration across the agencies. So certainly, you know, I can do more, and I can do more faster.

Mr. RATCLIFFE. I appreciate the Chair's indulgence. I yield back.

Mr. RICHMOND. You are welcome.

The gentlelady from Texas, Mrs. Jackson Lee, is recognized for 5 minutes.

Ms. JACKSON LEE. I thank the Chair and the Ranking Member for this hearing, and it couldn't be more important.

I am just going to briefly start with you, Mr. Bryan. As you well know, I spoke to you a couple of months ago with a major university who had a concern, and I have not yet heard, and it is an important issue for them. They work very hard, and I am just wondering when you will reach my office with a response?

Mr. BRYAN. Yes, ma'am. If I am not mistaken, a formal response was drafted, and I will follow up on where that went. But in the short order, I can tell you that the discussion was based on two projects that they were considering at the university.

One of them has already been approved, and we are adjudicating the other one as we speak, so it should not take much longer before a final decision is made.

Ms. JACKSON LEE. So maybe we will reach each other. It did not lapse, which was their concern, that they did not get out of the queue.

Mr. BRYAN. That is correct.

Ms. JACKSON LEE. So they are in the queue?

Mr. BRYAN. Yes.

Ms. JACKSON LEE. Let me thank you very much.

Let me just pursue, Mr. Krebs, this whole idea of the budget, and I do appreciate at least the suggested budget of the President. How many staff are in your sector?

Mr. KREBS. So across the agency, we are at about 2,200 personnel, Federal full-time equivalent.

Ms. JACKSON LEE. This is dealing with cybersecurity issues?

Mr. KREBS. Cybersecurity I am at about close to 1,200 in terms of cybersecurity.

Ms. JACKSON LEE. Yes, I am just talking about cybersecurity.

Mr. KREBS. Cybersecurity, yes, ma'am, about 1,200.

Ms. JACKSON LEE. OK. Let me read, Pittsburgh, the Tree of Life, Robert Gregory Bowers; Mother Emanuel, Dylann Roof; Christchurch, Brenton Harrison Tarrant; San Diego, John Earnest; and most recently, Los Angeles, a terrorist suspect arrested yesterday, Mark Steven Domingo.

I would say a good percentage of those used the cyber system to proffer their hate or to take from it their hate. I think, Mr. Krebs, you have acknowledged the kinds of persons that are utilizing the cyber system.

How many of those people do you have working on these kinds of hate efforts, dastardly acts that result in the murder of Americans and sometimes the murder of people around the world?

Mr. KREBS. So on the physical side of this, Tree of Life is a great example. One of my protected security advisors up in Pittsburgh had worked with Tree of Life Synagogue, had done a security assessment, a walk-through of the facility and identified areas for perhaps improved egress.

In fact, the rabbi at the Tree of Life Synagogue had credited my team for saving lives.

Ms. JACKSON LEE. I am particularly talking about the use of the cyber system to promote hate.

Mr. KREBS. Yes, ma'am.

Ms. JACKSON LEE. What are we dealing with?

Mr. KREBS. So this is a domestic terrorism issue, in part. Recently, the office, and I would have to get back with you on the structure and the engagement, but in Office of Terrorism Prevention this was just last week or 2 weeks ago out of the Office of Policy that is focused on, much like countering ISIS, how do we address issues like this of on-line speech?

Fundamentally, when I look at the problem there, there are First Amendment challenges with this challenge right now, or with this issue right now. But my team is focused. When you say cyber systems, really what you are talking about is social media, email, and other forms of I.T. and communications.

That does not fall within the traditional cybersecurity definition, and it does not fall within my traditional cybersecurity authorities.

Ms. JACKSON LEE. Well, let me move on, because I think it should. Let me ask unanimous consent to place in the record the Computer Week, "Why Connected Devices Are Transforming Our Personal and Working Lives in a Multitude of Ways."

They are also a growing security risk of attackers who are hijacking these devices and turning them into an internet of things botnets. So I would ask to place that in the record.

Mr. RICHMOND. Without objection.

[The information follows:]

ARTICLE SUBMITTED BY HONORABLE SHEILA JACKSON LEE

HOW BOTNETS POSE A THREAT TO THE IOT ECOSYSTEM

APRIL 2019

Nicholas Fearn, Computer Week

https://www.computerweekly.com/feature/How-botnets-pose-a-threat-to-the-IoT-ecosystem

While connected devices are transforming our personal and working lives in a multitude of ways, they are also a growing security risk—attackers are hijacking these devices and turning them into internet of things botnets

Connected technology already plays a dominant role in our daily lives. From mobile phones to tablet PCs, smart devices allow us to communicate with friends and family, keep up-to-date with what is happening in the world, stay entertained, accelerate productivity in the workplace, and much more.

But although the connected ecosystem is pretty expansive in 2019, it is about to get even bigger in coming years. We are on the cusp of an era when nearly everything around us has some form of internet ability, such as home appliances, cars, office equipment, city infrastructure, and health care devices.

For many, the internet of things (IoT) will mark the next major revolution for mankind. According to figures from Statista, there will be 31 billion devices connected to the internet by 2025, and Gartner predicts that the average family home will have 500 smart devices by 2022. Meanwhile, IDC claims that spending on the IoT will reach $745 bn in 2019.

However, while IoT technology offers a great deal of opportunity, it is also causing a major security epidemic. Hackers are increasingly exploiting connected devices to harvest sensitive data, send spam, take control of networks and launch cyber attacks around the world.

Botnet attacks have become commonplace, with CenturyLink Threat Research Lab estimating that 195,000 such attacks take place every day and Accenture putting the average cost at $390,752. It is clear that the continued expansion of the IoT ecosystem means more potential access points and weak areas that need to be mitigated. But how can that be achieved?

A growing crisis

Traditionally, criminals have used malware to infect devices. However, as the connected ecosystem expands and new technologies enter the market, they are finding different ways to launch more complex and devastating attacks. Botnets are a good example of this.

Mike Benjamin, head of Black Lotus Labs at CenturyLink, says botnets are becoming a pervasive problem across the internet and attackers are increasingly using IoT devices building their botnets. This, he claims, is creating a big security problem for consumers and businesses.

Botnets are particularly challenging because they evolve over time and new forms constantly emerge, one of which is TheMoon. Benjamin tells Computer Weekly: "Threat researchers at CenturyLink's Black Lotus Labs recently discovered a new module of IoT botnet called TheMoon, which targets vulnerabilities in routers within broadband networks."

Benjamin explains that a previously undocumented module, deployed on MIPS devices, turns the infected device into a Socks proxy that can be sold as a service. "This service can be used to circumnavigate internet filtering or obscure the source of internet traffic as a part of other malicious actions," he says.

Attackers are using botnets such as TheMoon for a range of crimes, including credential brute forcing, video advertisement fraud and general traffic obfuscation. "For example, our team observed a video ad fraud operator using TheMoon as a proxy service, impacting 19,000 unique URLs on 2,700 unique domains from a single server over a 6-hour period," says Benjamin. "TheMoon is a stark reminder that the threat from IoT botnets continues to evolve. They are becoming more sophisticated and capable of more significant damage."

Botnets are always advancing

Like Benjamin, 451 Research IoT analyst Ian Hughes believes botnets are a prevalent security risk because they are always changing. He says that over the past few years, many forms of botnet have been created in line with the evolution of the technology industry and with advances in software engineering.

"Pre-cloud, the target would be viral infection on PCs through installation of patches to programs, usually accidentally by the user," says Hughes. "With the increase in connectivity, and the use of the internet and the web in a cloud era, the options for nefarious code to be run on machines increased.

"Not only did the technology introduce more potential holes, but the ability for individual and groups to share information with one another, such as code, made weaknesses in systems much more well-known. Systems have also evolved from specific hardware and software combinations, which, when bespoke, are harder to gain control of en masse, to ones running general-purpose virtual machines, containers or services."

And as more devices connect to the internet, this challenge will only grow, says Hughes. "We have an increasing number of devices with relatively cheap compute power on board, all connected to the internet and able to run any form of software, and be managed remotely," he says.

"We also have a growing and eager market to instrument areas such as industrial manufacture, as well as the consumer space with IoT, which offers great benefits, but also increases the attack surface and options for bad actors to engage with. With an ever-more connected environment, a device such a simple surveillance video camera, in the case of the Mirai botnet, can have some of its processing hijacked and directed at almost anything else."

To tackle botnets, Hughes says all networks and all devices need not only high levels of security monitoring and regular updates, but also known levels of trust

within a system. "These levels of trust are starting to be built upwards from the chip manufacturers as well as the device and software industry," he says. "Of course, it only takes one release of a product at any level cutting some corners to get to market, to leave something wide open for hackers."

Poor security

It is clear that the continued adoption of IoT devices is creating a unique opportunity for attackers. Steven Furnell, senior IEEE member and professor of information security at Plymouth University, notes how poorly secured connected devices can be exploited.

"We've seen numerous reports of individual devices being exploited, we've seen a growth in malware, and we've had the Mirai botnet already demonstrating the significant potential to harness vulnerable devices," he says.

"What this clearly illustrates is that we've failed to learn from the past. Around 15 years ago, we had wireless access points being sold without encryption enabled and with default passwords. Security was available, but it required users to be aware enough to switch it on and change from the defaults.

"Unsurprisingly, many didn't do so, and exploitation of unprotected access points was commonplace as a result. It was only once that wireless networks had become synonymous with vulnerability that the position ultimately changed, and manufacturers moved to enabling security out-of-the-box by default."

Furnell believes the IoT ecosystem is experiencing a similar situation, putting pressure on manufacturers to develop more robust security mechanisms to protect users. "We have since seen the same sort of thing happen with IoT devices," he says. "Devices have shipped either without security, without it enabled, or with universal defaults—all of which render them vulnerable to misuse, including the potential for enlistment within botnets.

"Moving forward, the fundamental point is that IoT devices need to have security available and we cannot leave it to individual users' discretion about whether to enable it. There have been some positive moves. Last year, the Department for Digital, Culture, Media and Sport and the National Cyber Security Centre issued a code of practice for the security of consumer IoT devices.

"This proposes a set of 13 practices that developers, manufacturers and retailers could adopt to improve security, with the first of these being the elimination of universal defaults for usernames and passwords."

Cracking down on botnets

Although there is no silver bullet solution for mitigating the risk of botnets, there are a number of helpful best practices. "When deploying an IoT device of any type, the three most important questions need to be: Have we configured strong credential access? What is our update strategy for firmware changes? What URLs and IP address does the device need for its operation?" says Tim Mackey, senior technical evangelist at Synopsys.

"When IoT devices are deployed within a business environment, best practice dictates that a separate network segment known as a VLAN should be used. This then allows for IT teams to monitor for both known and unknown traffic impacting the devices. It also allows teams to ensure that network traffic originates from known locations.

"For example, if a conference room projector is accessible via Wi-Fi, the network the device uses should be restricted to only internal and authenticated users. Public access to the device should always be restricted. Following this model, exploitation of the device would then require a malicious actor to first compromise a computer belonging to an authenticated user."

Mackey says regular IT audits of IoT networks should then be performed to ensure only known devices are present, with the device identification mapped back to an asset inventory containing a current list of firmware versions and a list of open source components used within that firmware.

"This open source inventory can then be used to understand when an open source vulnerability impacting a library used within the firmware has a published vulnerability," he says. "Armed with this information, a proactive update and patching model can be created for corporate IoT devices.

"Also, inspection of the firmware should identify what external APIs (application programming interfaces), URLs and services the firmware is configured to operate against.

"These endpoints should be confirmed with the supplier as legitimate with confirmation of their function. Once confirmed, the IoT network that the device associated with the firmware is configured for can then have firewall restrictions defined, allowing the IoT devices access only to their known API dependencies. These tasks

should be considered part of an overall device access model consistent with the principles of zero trust."

Spencer Young, regional vice-president for Europe, the Middle East and Africa at security firm Imperva, says the best way to discover and mitigate a botnet is to find its command and control (CnC) server. "The most effective way is to look into the communication between the CnC and its bots," he says. "Once you start searching for exploit attempts, you can start to pick up possible indicators of a botnet.

"For example, if the same IPs attack the same sites at the same time while simultaneously using the same payloads and attack pattern, it is fairly likely that they're part of the same botnet.

"However, all initiatives to combat the growth of botnets through industry standards and legislation are likely to continue to occur only on a regional or country level. As far as industry-wide efforts go, it is hard to imagine a scenario in which a global security standard for botnet detection and defence could be agreed upon, applied and enforced."

Given the regulatory challenges and continued rise in the number of connected devices, botnet attacks are likely to keep increasing. Young says that as our devices evolve, both in terms of sophistication and connectivity, so will botnets. This, he believes, will mean that operators will be provided with more capacity and new, more advanced attack options.

So preparation is key, says Young. "To mitigate future attacks, all businesses must be prepared to defend against an attack when it arises," he says. "Investing in the ability to parse your cyber threatscape, successfully identify botnet attacks and build an intelligent defence is not just a security concern—it's a frontline business issue."

If one thing is certain, it is that the threat of botnets will only increase as the connected ecosystem rapidly expands and new connected technologies enter the market. And while attackers will continue to find new ways to take control of networks and leverage botnets, there are clear ways in which IT practitioners and organisations can mitigate the risk here—most notably the issue of improving weak security mechanisms.

It may be that attackers are often one step ahead, but by being more proactive, security teams can also leapfrog ahead on occasions.

Ms. JACKSON LEE. Let me ask a question again, Mr. Krebs, on maybe something that is within your jurisdiction. What is being done to incentivize election officials to report suspected malicious cyber activity, and how arduous are the reporting processes? What did we learn from the tabletop vote exercise?

If you can hold that question? Then the second one is on the issue of botnets, which are networks of private computers infected with malicious software and controlled as a group without the owner's knowledge, i.e., to send spam messages or launch attacks against networks or computing services.

One of the new exploits involved using voiceover IP on the internet to launch an attack that targets a phone number for calls that are auto-dialed or redirected for the purpose of preventing legitimate telecommunications from occurring. We know what the Russians did in 2016. Is your office considering this type of threat to public elections posed by botnets?

If you would answer those two serious questions.

Mr. KREBS. Yes, ma'am. So in terms of general incentives to election officials, steady engagement, regular engagement providing them an understanding of the things we can do to help them out. Our incentive is the support service.

We provide them assistance. We help them manage the risk to their systems, build a relationship, build trust and confidence that I can help them. If they have a bad day, they will come to me. I have confidence that we are building those relationships and we will get there.

In terms of specific botnet mitigation, two fronts on this. In the Executive Order 13800, there was a requirement to develop a botnet report. We worked on that with Commerce and TIA, set out a work plan with industry on countering botnets.

So we are addressing this from two angles. One, working with industry to actually address the botnet challenge more holistically. But also we work with election officials to help them understand the threat posed by botnets and put counter-botnet or botnet, I am sorry, DDoS mitigation capabilities in place in their system.

So if they do experience some sort of DDoS attack then, which is effectively what we are talking about here, then they have the security mitigations in place.

Ms. JACKSON LEE. You said it was Executive Order 1300?

Mr. KREBS. 13800.

Ms. JACKSON LEE. 13800.

Mr. KREBS. Yes, ma'am. May 2017.

Ms. JACKSON LEE. All right. Let me thank you very much.

I yield back.

Mr. RICHMOND. I thank the gentlelady.

I thank the witnesses for their valuable testimony and 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 record shall be kept open for 10 days.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 3:46 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON FOR CHRISTOPHER C. KREBS

Question 1. CISA carries out a broad cybersecurity mission that includes protection of 99 Federal agency networks, hundreds of thousands of U.S. critical infrastructure entities, and covers the waterfront of infrastructure and networks that support our day-to-day life. And, CISA does so on a budget that is one-eighth that allocated to the Pentagon. If CISA's budget doubled tomorrow, what are some of the priorities you would pursue?

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

Question 2a. Since 2014, Congress has repeatedly expanded CISA's cybersecurity authorities and responsibilities, including late last year when Congress voted to make CISA an operational component. Nevertheless, CISA's budget has remained fairly flat and, if the fiscal year 2020 request were enacted, it would actually see its budget cut.

How does this square with the challenges of reorganizing, staffing, and operating this new agency?

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

Question 2b. This is a pivotal time for CISA. Might forcing CISA to operate on a less-than-adequate budget have lasting effects on the success of the agency?

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

Question 3. Earlier this year, the DHS Inspector General reported that CISA's election security activities are being carried out by a skeleton crew, and outreach to local election officials are stretching CISA's field teams extremely thin. The fiscal year 2020 budget requests $22 million for support to State and local election officials. Is this enough to reconcile the need for "improved planning, more staff, clearer guidance" and other deficiencies identified by the IG?

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

Question 4a. In 2013, a fertilizer plant exploded in West, Texas, killing a dozen first responders. Last year, a Houston facility caught fire after a back-up generator failed during Hurricane Harvey. This year alone, there have been multiple explosions at chemical facilities in Texas that caused major portions of the city to shut down and residents being told to shelter in place for days. The CFATS program is a vital National security program that requires security measures at the Nation's highest-risk chemical facilities. The fiscal year 2020 budget proposes slashing CFATS budget by $18 million. How can you justify such a dramatic cut to a program that is operating effectively, has bipartisan support, and has such demonstrable value to the chemical sector?

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

Question 4b. On February 26, 2019, this committee held a hearing on CFATS with the director of the Infrastructure Security Compliance Division. At that hearing, I requested and was promised information on CFATS-covered facilities. Following that hearing, I submitted Questions for the Record for which no response has been provided. Moreover, I was asked to submit some of my requests in a separate letter, which I did, and yet again have not received a response. What is the status of this correspondence?

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

Question 5. As National interest in cybersecurity has grown, I worry that we are losing focus on DHS's long-standing mission to protect physical assets. As CISA reorganizes and plans for the future, what is your long-term goal for the Infrastructure Security Division?

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

Question 6. On April 26, 2019, the Office of Management and Budget (OMB) issued a memorandum titled, Centralized Mission Support Capabilities for the Federal Government which pre-designates CISA as the lead for cybersecurity shared services across the Federal networks. I support this designation but am concerned

that OMB's draft plan designates the Department of Justice (DOJ) as the functional lead for Security Operations Center (SOC) as a Service with DHS preforming an oversight role. This structure may prove to be unsuccessful given previous challenges in their interagency relationship. What is the rationale for establishing DOJ as the lead for "SOC as a Service" instead of establishing it within CISA, which is statutorily responsible for securing Federal networks?

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

Question 7a. With respect to the National Risk Management Center (NRMC)—can you describe how the series of initiatives, or sprints, that began last year will feed into a larger strategy to help Government and the private sector better manage risk?

Are these initiatives intended to be short-term engagements or will they become permanent?

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

Question 7b. Are responsibilities from the Infrastructure Security Division being transferred to the NRMC? If so, what impact does the shift in responsibilities have on morale at the Infrastructure Security Division?

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

Question 8. Recently, the NRMC released a list of 55 "National Critical Functions" (NCF). The shift from protecting "critical sectors" to "critical functions" is a major realignment. Until now, the Federal framework for securing critical infrastructure has been based on DHS, as the lead Federal coordinator, working with designated Sector-Specific Agencies who act as liaisons and coordinators within a sector. The NCF list is a more integrated approach, and efforts to secure a single function will likely cross into multiple sectors and require more coordination. How do you expect CISA's role as coordinator to evolve in order to secure this more expansive, complex list of functions?

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

Question 9. Thus far, DHS has released a 3-page overview of the National Critical Functions. What more do you expect to release to the public, and to Congress? What is your time line for doing so?

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

Question 10. CISA plans to build upon its National Critical Functions work to build a Risk Register, which will identify scenarios that could degrade these functions, tier them by severity, and enable better prioritization of mitigation activities for critical infrastructure. What is the time line for the creation of the Risk Register?

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