Testimony

Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"Resourcing DHS' 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"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND INNOVATION

Tuesday, April 30, 2019

Washington, DC

Chairman Richmond, Ranking Member Katko, and distinguished members of the subcommittee, thank you for the opportunity to testify regarding the Fiscal Year (FY) 2020 President's Budget for the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The FY 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 cyberspace is a core DHS mission. The FY 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 hyper connectivity, and our digital dependence has opened cracks in our defenses, creating new vectors through which our enemies and adversaries can strike us. This is a volatile combination, resulting in a world where threats are more numerous, more widely distributed, highly networked, increasingly adaptive, and incredibly difficult to root out.

CISA is strengthening our digital defense as cybersecurity threats grow in scope and severity. The FY 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 towards 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 five 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 FY 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 FY 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 FY 2020 Budget, $4.8 million over the FY 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 FY 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 FY 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 FY 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 FY 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 FY 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 FY 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 nationwide. 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 FY 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 FY 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 FY 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 FY 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 eight 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 four years. Congress previously approved $120 million for St. Elizabeths construction in FY 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 FY 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 midterm elections, over 500 CISA employees supported election security preparedness nationwide. 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 three-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 timeline 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 online 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.