Testimony

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

FOR A HEARING ON

"CISA Fiscal Year 2021 President's Budget"

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

Wednesday, March 11, 2020

Washington, DC

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

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

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

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

The FY 2021 President's Budget for CISA has been reorganized under new budget lines to fully reflect the operational vision for CISA. The CISA Act of 2018 reorganized the National Protection and Programs Directorate into an operational component, and the budget should reflect the new organization. For instance, management and operational watch activities that were previously spread across multiple budget lines are now merged into a single funding line that will serve as a nexus of cyber, physical, and communications integration. The new funding lines also combine all regional field operations, including Protective Security Advisors and Cybersecurity Advisors, into a single report channel. This enhance the ability of CISA to engage with critical infrastructure partners outside the beltway, where they are located. If adopted, this new structure will streamline authority, increase transparency, and better enable CISA to execute the funding.

CISA Priorities

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

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

CISA, our government partners, and the private sector, are all engaging in a more strategic and unified approach 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 isfundamentally one of partnerships and empowerment, and it is prioritized by our comprehensive understanding of the risk environment and the corresponding needs of our stakeholders. We help organizations manage their risk better.

The FY2021 President's Budget includes $1.1 billion for cybersecurity initiatives at CISA to detect, analyze, mitigate, and respond to cybersecurity threats. We share cybersecurity risk mitigation information with government and non- government partners. By issuing guidance or directives to federal agencies, providing tools and services to all partners, and leading or assisting the implementation of cross-government cybersecurity initiatives, we are protecting government and critical infrastructure networks.

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

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

CDM provides federal network defenders with a common set of capabilities and tools they can use to identify cybersecurity risks within their networks, prioritize based on potential impact, and mitigate the most significant risks first. The program provides federal agencies with a risk-based and cost-effective approach to mitigating cyber risks inside their networks. The FY 2021 President's Budget includes funding to continue deployment and operation of necessary

tools and services for all phases of the CDM program. Funding will cover completion of activities to strengthen management of information technology assets including for cloud and mobile-based assets and protection of data on networks that carry highly sensitive and critical information. By pooling requirements across the federal space, CISA is able to provide agencies with flexible and cost-effective options to mitigate cybersecurity risks and secure their networks.

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

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

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

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

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

For infrastructure security, the FY 2021 President's Budget includes $96 million for protecting critical infrastructure from physical threats through informed security decision-making by owners and operators of critical infrastructure. Activities include conducting vulnerability and consequence assessments, facilitating exercises, and providing training and technical assistance 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, from emerging threats such as unmanned aircraft systems. Funding supports CISA's school safety initiatives, including stewardship of the Federal School Safety Clearinghouse, the expansion of existing school security activities, and the development of additional resources and materials for safety to provide children with a safe and secure learning environment.

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

The FY 2021 President's Budget includes $158 million for emergency communications to ensure real-time information sharing among first responders during all threats and hazards. CISA enhances public safety interoperable communications at all levels of government across the country through training, coordination, tools, and guidance. We lead the development of the National Emergency Communications Plan to maximize the use of all communications capabilities available to emergency responders—voice, video, and data—and ensures the security of data and information exchange. CISA supports funding, sustainment, and grant programs to advance communications interoperability, such as developing annual SAFECOM Grant Guidance in partnership with Public Safety stakeholders, and partnering with FEMA Grants Program Directorate to serve as communications subject matter experts for FEMA-administered grants. We assist emergency responders and relevant government officials with communicating over commercial networks during natural disasters, acts of terrorism, and other man-made disasters through funding, sustainment, and grant programs to support communications interoperability and builds capacity with Federal, State, local, tribal, and territorial stakeholders by providing technical assistance, training, resources, and guidance. The program also provides priority telecommunications services over commercial networks to enable national security and emergency preparedness personnel to communicate during telecommunications congestion scenarios across the Nation.

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

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

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

The President's Budget asks for $24 million within the Science and Technology Directorate (S&T) to continue research and development efforts in support of CISA's cybersecurity mission. CISA and S&T have made tremendous strides in collaborating to advance joint priorities. In FY 2019, CISA and S&T awarded a project to create a 'pipeline' for low technology readiness level efforts to mature and transition into CISA. Workstreams in this pipeline are advancing threat-driven cyber analytics and development of a cyber risk framework. This project is an important first step in the larger plan for CISA and S&T to enhance analytics in conjunction with big data and machine learning. Subsequent efforts in FY2020 and beyond are planned to leverage hyperscale cloud platforms and significantly advance the data and analytics capabilities of CISA.

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

Conclusion

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

cyber-physical risk and cross-sector critical infrastructure interdependencies.

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

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