Testimony

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"The Cybersecurity and Infrastructure Security Agency Fiscal Year 2023 President's Budget"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEE ON HOMELAND SECURITY

Thursday April 28, 2022

Washington, DC

Chairwoman Roybal-Allard, Ranking Member Fleischmann, and Members of the subcommittee, thank you for the opportunity to testify regarding the Fiscal Year (FY) 2023 President's Budget for the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The FY 2023 President's Budget of $2.5 billion for CISA reflects our commitment to the broader DHS mission to safeguard our homeland, our values, and our way of life.

In today's interconnected society, our Nation faces a wide array of serious risks from many threats, all with the potential for significant consequences that can impact our critical infrastructure, the whole of the economy, and the American way of life. The critical functions within our society are built as "systems of systems" with complex designs, numerous interdependencies, and systemic risks. While this structure provides for significant gains in efficiency and productivity, it also provides opportunities for nation-state actors and criminals to potentially undermine our national security, economic prosperity, and public health or safety, creating cascading effects across our Nation.

CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day. Established in 2018 to be America's cyber defense agency, CISA works to build collaborative, trusted partnerships across government, industry, academia, and with our international partners to ensure the collective cyber defense of the Nation. At the heart of this mission is partnership and collaboration. Securing our Nation's cyber and critical infrastructure is a shared responsibility requiring not just a whole-of-government, but a whole-of-Nation approach.

As part of this mission, CISA plays two key operational roles. First, we are the operational lead for federal cybersecurity, charged with protecting and defending federal civilian executive branch networks (the ".gov"), in close partnership with the Office of Management and Budget, the Office of the National Cyber Director, and agency Chief Information Officers and Chief Information Security Officers. Second, we serve as the national coordinator for critical infrastructure security and resilience, working with partners across government and industry to protect and defend the nation's critical infrastructure. In both roles, CISA leads incident response to significant cyber incidents in partnership with the Federal Bureau of Investigation (FBI) and the Intelligence Community.

Safeguarding and securing cyberspace and our Nation's critical infrastructure is a core DHS mission. I am truly honored to appear before this Committee today to discuss how the FY 2023 President's Budget recognizes the criticality of our mission and provides CISA's exceptional workforce with the resources needed to achieve this mission. Since being sworn in as Director in July, I continue to be impressed with the talent, creativity, and enthusiasm of the dedicated CISA employees I am entrusted to lead. As I share with my team nearly every day, I have the best job in government.

FY 2023 President's Budget: Priorities

Looking forward into FY 2023, CISA will remain focused on strengthening our Nation's cyber and physical defenses. We will continue to work closely with our partners across every

level of government, in the private sector, and with local communities to protect our country's networks and critical infrastructure from malicious activity. We will continue to share timely and actionable information, intelligence, and guidance with our partners and the public to ensure they have the tools they need to keep our communities safe and secure and increase nationwide cybersecurity preparedness.

The FY 2023 President's Budget provides the resources needed to continue these efforts. From an agency-wide perspective, it is organized around three overarching themes.

First, this budget represents a significantly increased investment in CISA by the Biden Administration. The $2.5 billion requested for CISA in FY 2023 provides approximately $377 million or about 18% more than requested in FY 2022. The FY 2023 President's Budget recognizes the value of historical investments, and CISA's growing role in enhancing the security and resilience of our Nation, and confidence in our ability to execute.

Second, the FY 2023 President's Budget prioritizes federal cybersecurity. Most importantly, it includes $174 million in new budget authority for CISA to continue the work established through the American Rescue Plan Act (ARPA) by expanding cybersecurity service offerings that protect federal networks against evolving cyber threats. These funds will allow CISA to expand network protection throughout the federal civilian executive branch and bolster cloud business applications, enhanced analytics, and stakeholder engagement. Placing this funding into CISA's base budget enables CISA and our partners to move forward knowing we can build on the progress made to date in critical operational and strategic cyber risk mitigation capabilities.

Third, the FY 2023 President's Budget makes critical investments in our mission enabling activities and functions that will mature the Agency and better support the execution of our operational capabilities. The Budget provides $250 million for Mission Support, an increase of $108 million above the FY 2022 President's Budget. This investment provides critical mission enabling initiatives including the establishment of CISA procurement operations, implementation of key cybersecurity improvements to CISA's own networks, expansion of workforce assistance offerings, and continued progress on the build out of CISA's headquarters facility at the DHS St. Elizabeth's Campus. We look forward to working with Congress to ensure robust resourcing for our mission enabling teams as they support the foundation of our operational efforts.

The FY 2023 President's Budget also provides for a number of more targeted investments focused on key CISA mission areas. I would like to take a moment to highlight a few of those investments and explain how they help strengthen our collective effort to protect the Nation.

Cybersecurity

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

The FY 2023 President's Budget includes $1.5 billion for CISA cybersecurity programs and activities that enable CISA and our partners to detect, analyze, mitigate, and respond to cybersecurity threats. We share cybersecurity risk mitigation information with government and non-government partners. We issue guidance and directives to federal agencies, providing tools and services to all partners, and lead or assist in the implementation of cross-government cybersecurity initiatives. We are protecting government and critical infrastructure networks.

Within this amount, the FY 2023 President Budget includes $71 million for the Joint Cyber Defense Collaborative (JCDC), an increase of over $18 million more than the FY 2022 request, to ensure CISA can continue expanding the cyber operational planning and partner engagement activities so crucial to our Nation's collective cyber defense. Established in August 2021 and leveraging legacy authorities as well as those granted to CISA in the FY 2021 National Defense Authorization Act, the JCDC leads collaborative public and private sector cyber defense planning and cybersecurity information fusion and analysis to reduce cyber risks to the Nation.

The JCDC brings together key Federal Government partners, including the Office of the Director of National Intelligence, the FBI, the National Security Agency, U.S. Cyber Command, the U.S. Secret Service, and relevant Sector Risk Management Agencies (SRMAs), with private sector partners to build, exercise, and implement cyber defense plans to both actively and proactively address the most significant risks facing our country. While the JCDC was founded only nine months ago, we have already demonstrated how proactive planning can enable operational collaboration to drive risk reduction at scale. The core of this collaboration has been our JCDC Alliance partners, which include 25 of the Nation's largest cybersecurity and technology companies.

The JCDC allows these partners to help us see the dots, connect the dots, and collectively drive down risk to the Nation at scale. I would submit that the JCDC's unprecedented collaboration is making us more resilient. Thanks to the JCDC, we stand shoulder-to-shoulder with our industry partners. Over the past six months, we have formed partnerships and worked together to understand and manage cyber threats, including the Log4Shell vulnerability and those related to Russia's invasion of Ukraine.

The JCDC construct continues to mature, and our partnership model is evolving as well. As one example, we recently announced the addition of several new JCDC partners with particular expertise in identifying and mitigating cyber threats to industrial control systems.

Going forward, CISA will continue to build and mature the JCDC construct. We are focused on advancing our capability to create, exercise, and execute joint cyber defense plans. Our upcoming planning efforts focus on pipeline infrastructure; critical dependencies between the financial, energy, and telecommunications sectors; and collaboratively supporting defense of the Nation's election infrastructure in preparation for the midterm elections. The JCDC has demonstrated the promise of a new model for public-private operational collaboration: joint cyber planning—including deliberate and crisis action plans—through collaboration across the public and private sectors to prepare for and address the Nation's most pressing cyber risks, combined with integrated and institutionalized exercises to continuously measure and improve our combined effectiveness.

Through these collaborative efforts, we enable common situational awareness, information fusion, and analysis that equips public and private partners to take risk-informed coordinated action. This journey is not CISA's alone. We are embarking on a rapid evolution in concert with our partners across the interagency and the private sector, with a shared goal of advancing our nation's security and resilience at scale.

To effectively execute our role as the operational lead for federal civilian security, CISA must maintain and advance our ability to actively detect threats targeting federal agencies and gain granular visibility into the security state of federal infrastructure. To effectuate these goals, the FY 2023 President's Budget also includes $407 million for the National Cybersecurity Protection System (NCPS) and $425 million for the Continuous Diagnostics and Mitigation (CDM) program. These programs provide the technological foundation to secure and defend federal civilian executive branch departments and agencies 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 and improves situational awareness of intrusion threats with near real-time detection. While EINSTEIN has demonstrated value since its inception, we are evaluating modernization of NCPS, including a transition to providing security capabilities via commercial shared services. The FY 2023 President's Budget includes $30 million for the deployment of a modern infrastructure and analytic environment that will enable our analysts to most effectively use increasing volumes of security data to identify and enable faster remediation of threats.

Even as we mature NCPS to advance our ability to detect and block threats, CDM remains a foundational capability for CISA and federal network defenders to identify cybersecurity risks within their networks, prioritize those risks, and mitigate the most significant ones first. The program provides federal agencies with a risk-based and cost-effective approach to mitigating cyber risks inside their networks and provides CISA with granular visibility to drive both strategic investments and urgent remediation, including by most effectively targeting our directive authorities. This includes $73 million to expand the Endpoint Detection and Response (EDR) initiative across high-priority agency hosts and endpoints across the Executive Branch departments and agencies to support efforts to close remaining crucial gaps at large

agency enterprises and to provide visibility into unauthorized, potentially malicious, or adversary activity targeting Federal networks. First authorized by Congress in the FY 2021 National Defense Authorization Act and initially funded in the American Rescue Plan Act, broad deployment of EDR capabilities allows CISA to execute our persistent hunt authorities to actively and continuously detect and drive eviction of adversaries across federal networks.

Within CISA's cyber defense capabilities, the FY 2023 President's Budget also includes $39 million for the CyberSentry program. Recently authorized in the FY 2022 National Defense Authorization Act, CyberSentry is a voluntary partnership with private sector critical infrastructure operators designed to detect malicious activity on the Nation's highest-risk critical infrastructure networks. CyberSentry is particularly focused on threats that attempt to move from an organization's business network to impact industrial control systems. The program allows CISA to operationalize sensitive threat intelligence to increase the speed of information sharing and produce real-time, effective, actionable information for critical infrastructure operators at risk from malicious attacks. The resources requested for FY 2023 will support growing CyberSentry operations and deploy capabilities to additional critical infrastructure partners to meet significant demand for the program.

Infrastructure Security

For infrastructure security, the FY 2023 President's Budget includes $175 million for efforts to enhance critical infrastructure protection from physical threats through enabling risk-informed decision-making by owners and operators. Our activities include collecting critical infrastructure information, conducting vulnerability assessments, facilitating exercises, and providing training and technical assistance. The Infrastructure Security Division leads and coordinates national efforts on critical infrastructure security, including reducing the risk of targeted violence directed at our Nation's schools, communities, houses of worship, and other soft targets. As the Sector Risk Management Agency for the chemical sector, CISA also leads efforts to secure our Nation's chemical sector infrastructure, enhancing security and resilience across the chemical industry to reduce the risk of weaponization. The FY 2023 President's Budget includes an increase of $4 million and additional personnel above the prior request for the planning and execution of additional cyber preparedness exercises in support of the JCDC, as well as to facilitate planning for Cyber Storm IX, the National Cyber Exercise, tentatively scheduled for Spring 2024.

Integrated Operations

The FY 2023 President's Budget includes $187 million for integrated operations. Our Integrated Operations Division provides seamless and timely support to CISA stakeholders across the Nation. The Integrated Operations Division coordinates CISA operations at the regional level and delivers CISA capabilities and services to support stakeholders in preparing for, mitigating, responding to, and recovering from incidents effecting critical infrastructure. Additionally, Integrated Operations includes monitoring and disseminating cyber and physical risk and threat information; providing intelligence context to support decision making; and performing Agency-designated Emergency Support Functions.

In addition to increases provided through the annualization of ARPA activities, the FY 2023 President's Budget includes an increase of $2.5 million above the prior request to support the deployment of additional Security Advisors to the regions. These additional personnel will expand CISA engagement with FBI cyber task forces in victim notification and cyber analysis and response activities, support direct analyst-to-analyst information sharing and shape the support that CISA regional personnel provide to stakeholders impacted by a cyber incident.

Emergency Communications

The FY 2023 President's Budget includes $170 million for emergency communications to ensure interoperability at all times and to provide assistance and support for Federal and State, local, tribal, and territorial (SLTT) stakeholders. CISA's Emergency Communications Division enhances public safety 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—voice, video, and data— available to emergency responders and ensure the security of data exchange. We also assist emergency responders communicate over commercial networks during natural disasters, acts of terrorism, and other significant disruptive events.

The FY 2023 President's Budget includes a transfer of $5.8 million from CISA's Emergency Communications to support the transition of CISA's regionally deployed Emergency Communications Coordinators (ECCs) from the Emergency Communications Division to the Integrated Operations Division. This transfer positions the ECCs organizationally alongside CISA's other regional staff to allow better synchronization of CISA service delivery to stakeholders and supports the maturation of CISA's regional service delivery model.

Additionally, the FY 2023 President's Budget includes $70 million to support critical investments in the Next Generation Network-Priority Services program to continue the expansion of the program to ensure all priority national security and emergency preparedness users can communicate during all circumstances to safeguard national security, manage emergency response and improve national resilience.

Stakeholder Engagement

The FY 2023 President's Budget includes $72 million for CISA stakeholder engagement activities focused on fostering collaboration, coordination, and a culture of shared responsibility for national critical infrastructure risk management with Federal, SLTT, and private sector partners in the United States, as well as international partners. This program includes implementation and stewardship of the National Infrastructure Protection Plan; management and oversight of national cybersecurity and critical infrastructure leadership councils, committees, and boards; and implementation of programs and projects intended to facilitate effective coordination with the national critical infrastructure stakeholder community.

The FY 2023 President's Budget includes an increase of approximately $8 million above the prior request to support the execution and staffing of CISA's Cybersecurity Advisory Committee, which provides strategic and actionable recommendations to CISA on a range of

cybersecurity issues and topics, and the Cyber Safety Review Board, which conducts after-action reviews and assessments of significant cyber incidents, threat activity, and agency responses.

The FY 2023 President's Budget also includes an additional $5 million to expand and enhance CISA's global engagement capability to ensure CISA can effectively coordinate with international partners to advance U.S. cybersecurity, infrastructure security, and emergency communications interests. Our global engagement program includes U.S.-based strategy, planning, analysis, and program management staff responsible for supporting the CISA attaché and liaison officer overseas; providing subject matter expertise, engagement planning, and analysis to CISA leaders relating to the FIVE EYES partnership; and working with foreign partners to help build capacity to defend against global cybersecurity, infrastructure security, and emergency communications threats impacting U.S. interests. The additional funds will allow CISA to expand direct engagements with international partners in the Western Hemisphere, Asia, and Europe on cybersecurity and infrastructure security issues of mutual interest and benefit through expert-to-expert exchanges, information sharing, and joint exercises.

National Risk Management Center

Finally, the FY 2023 President's Budget fully funds CISA's national risk management activities, including $115 million for the National Risk Management Center (NRMC). The NRMC is a planning, analysis, and collaboration center which works to leverage sector and stakeholder expertise to identify and address the most significant risks to the Nation's critical infrastructure, and to coordinate risk reduction activities to ensure critical infrastructure is secure and resilient both now and into the future. The NRMC strives to create an environment where government and industry can collaborate to enhance critical infrastructure resilience by focusing on collective risk to National Critical Functions including through key initiatives such as position, navigation and timing security, emerging communications technologies, and supply chain risk mitigation.

The NRMC houses CISA's Election Security Initiative, which leads CISA's work to ensure the physical security and cybersecurity of the systems and assets that support the Nation's election infrastructure. The FY 2023 President's Budget provides $46 million for a variety of activities and programs across the Agency that focus on the protection of election infrastructure. Our efforts focus on collaborating with those on the front lines of elections—state and local governments, election officials, federal partners, and vendors—to provide a full range of services, training, and information to help manage risks to the Nation's election infrastructure. Since the American people's confidence in the value of their vote is reliant on the security and resilience of the infrastructure that makes our Nation's elections possible, CISA is also committed to building national resilience to foreign influence activities that create risks for critical infrastructure. We help the American people and DHS stakeholders understand the scope and scale of activities targeting elections and critical infrastructure and enable them to take action to mitigate. CISA will remain transparent and agile in its vigorous efforts to secure America's election infrastructure from new and evolving threats.

Conclusion

I am honored to represent my dedicated teammates at CISA who work tirelessly in support of our mission to understand, manage, and reduce risk to our cyber and physical infrastructure. Our nation faces unprecedented risk, and CISA is at the center of our national call to action. In collaboration with our government partners, critical infrastructure entities, and international allies, and with the support of Congress, we will continue to make progress addressing this risk and maintaining the availability of critical services to the American people. The FY 2023 President's Budget requests the funding necessary for CISA to carry out these critical mission imperatives.

Before I close, I would like to take a moment to recognize this Committee's strong support for CISA. Your consistent efforts to fully resource CISA operational capabilities in response to complex and evolving threats has made our Nation safer. For myself, and on behalf of CISA workforce, thank you for your support. I look forward to working with you during the FY 2023 appropriations cycle to continue strengthening this Agency, and by extension, the security and resilience of our Nation's networks and critical infrastructure.

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