TESTIMONY OF

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

BEFORE THE

Subcommittee on Homeland Security
Committee on Appropriations
U.S. House of Representatives

ON

# Fiscal Year 2025 Budget for the Cybersecurity and Infrastructure Security Agency

April 30, 2024
Washington, D.C.

Chairman Amodei, Ranking Member Cuellar, and members of the Subcommittee, thank you for the opportunity to testify regarding the Fiscal Year (FY) 2025 President's budget for the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The FY 2025 President's budget of $3.01 billion for CISA reflects our commitment to the DHS mission to safeguard our homeland, our values, and our way of life.

As America's cyber defense agency and the National Coordinator for critical infrastructure security and resilience, 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. Securing our Nation's critical infrastructure is a shared responsibility requiring not just a whole-of-government, but a whole-of-nation approach. CISA is only able to accomplish our mission by building collaborative, trusted partnerships across all levels of government, the private sector, academia, and the international community.

I am honored to appear before this Sub-Committee to discuss how the President's budget for FY 2025 recognizes our essential role and provides necessary resources to achieve this mission. In FY 2025, CISA will remain focused on strengthening our Nation's cyber and physical defenses. A key component of our success will be our employees and I continue to be impressed with the talent, creativity, and enthusiasm of the dedicated CISA workforce.

CISA plays two key operational roles in this mission. First, we are the operational lead for federal cybersecurity, charged with protecting and defending Federal Civilian Executive Branch (FCEB) networks, in coordination with the Office of Management and Budget, the Office of the National Cyber Director, and agency Chief Information Officers and Chief Information Security Officers. CISA also leads asset response to significant cyber incidents in partnership with the Federal Bureau of Investigation (FBI) and the Intelligence Community for threat response and intelligence support respectively.

Second, as the National Coordinator for critical infrastructure security and resilience, we work with Sector Risk Management Agencies and other federal partners; State, local, tribal, and territorial (SLTT) governments; and industry to protect and defend the Nation's cyber and physical infrastructure from the full range of threats. We will continue to work closely with these partners to help protect our country's networks and critical infrastructure from the full range of threats through the timely sharing of 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 increase nationwide cybersecurity preparedness. The FY 2025 President's budget provides the resources needed to continue both of these broad efforts.

In particular, the FY 2025 President's budget includes $116 million in funding to implement the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA). On April 4, 2024, the CIRCIA Notice of Proposed Rulemaking (NPRM) was published for a 60-day public comment period. The final rule is required to be issued 18 months after the publication of the NPRM. CISA will need the FY 2025 investments in staffing, processes, and technology capabilities to utilize information provided pursuant to CIRCIA. FY 2025 will be a crucial year to strengthen and build CISA's capacity to receive, manage, analyze, secure, and report on incidents and ransom payments reported under CIRCIA, maturing our current ability to manage incidents, coordinate with and notify our interagency partners, and implement data protection requirements

including additional staff to receive and route around-the-clock inbound reports as we prepare for the final rule to go into effect in FY 2026.

The FY 2025 President's budget includes $1.7 billion for the Cybersecurity Division (CSD) to continue to build the national capacity to detect, defend against, and build resilience to cyberattacks to our critical infrastructure. CISA will continue working with federal partners to bolster their cybersecurity and incident response postures, and safeguard federal networks. CISA will also continue partnering with the private sector and SLTT governments to detect and mitigate cyber threats and vulnerabilities to our nation's critical infrastructure before they are exploited.

The budget provides $394 million to support the Joint Collaborative Environment (JCE) tools and capabilities to facilitate the ingestion and integration of data as well as orchestrate and automate the analysis of data that supports the rapid identification, detection, mitigation, and prevention of malicious cyber activity. The JCE will serve as an important mechanism to integrate and exchange operational data, information, analysis, analytics, and threat intelligence, regardless of sector or industry. As part of the JCE, the budget includes $384 million for the Cyber Analytics Data System (CADS). CADS will provide a modern, scalable, unclassified analytic infrastructure for CISA's cyber operators, while strengthening CISA's ability to improve cyber threat visibility, promote streamlined analytics, and ultimately drive action to mitigate risks. CADS capabilities will ingest data from a myriad of sources, apply robust automation and analytics, and provide CISA's cybersecurity teams with access to analytical results, threat insights, and detailed visualization with capabilities to share results and mitigations in real time.

The Continuous Diagnostics and Mitigation (CDM) program remains an invaluable tool for rapidly deploying protection to federal agencies, resulting in increased operational visibility and an ability to defend against threats both at the agency and federal enterprise levels. The budget requests $470 million for CDM to increase CISA's invaluable operational visibility inside agency networks that helps drive targeted and enterprise-wide cybersecurity improvement actions. Many intrusions are enabled by known exploited vulnerabilities. Using our CDM program and our vulnerability scanning tools, CISA identified and drove mitigation of over 15 million severe vulnerabilities across the federal government in FY 2023.

Halfway through FY 2024, CISA has made progress in Endpoint Detection and Response (EDR) deployment across sixteen agencies. These technologies give CISA an unsurpassed level of visibility into threats and incidents targeting federal networks, allowing faster detection, and, using authorities recently provided by Congress, we can now assist agencies in responding to cyber events in minutes rather than days or weeks. A total of eight agencies have fully completed EDR deployments, with an additional five agencies making substantial progress. CISA will continue to overcome agency-specific hurdles ranging from resource challenges to agencies opting for longer timeframes to complete deployment. In the first two quarters of FY 2024, CISA has successfully detected 1,924 threats on federal networks using EDR capabilities and is actively working to expand this program to all federal agencies."

The budget additionally includes $255 million to deliver risk reduction services locally to CISA stakeholders in their community. As of April 1st, 2024, the Integrated Operations Division (IOD) has delivered over 27,000 risk reduction services across all 50 states. Risk reduction services include security assessments, entity notifications, security assist visits, tabletop

exercises, information exchanging round tables, and webinars that leverage CISA's expertise in cyber, physical, chemical, communications, and elections security. IOD separately coordinates CISA operations at the headquarters and regional level to warn entities of imminent cyberattacks and help them to prepare for and respond to incidents that impact critical infrastructure. As part of our Pre-Ransomware Notification Initiative, CISA made over 1,200 notifications to critical infrastructure owners and operators throughout the Nation in FY 2023 that were on the verge of having their data encrypted by ransomware attackers, avoiding the attacks due to CISA's rapid intervention. Additionally, IOD provides intelligence context to support decision making, performs Agency-designated Emergency Support Functions, and monitors and disseminates cyber and physical risk and threat information to CISA stakeholders 24/7/365.

The budget includes $187 million for infrastructure security and resilience for CISA's efforts to enhance critical infrastructure protection through enabling risk-informed decision-making by owners and operators of critical infrastructure, as well as Federal and SLTT partners. CISA's Infrastructure Security Division (ISD) leads and coordinates national programs and policies on critical infrastructure security and resilience, including analyzing critical infrastructure and key dependencies, developing and conducting vulnerability assessments, developing guidance methodologies and risk management courses of actions, collaborating with the Department of Defense on assessing critical homeland defense plans, facilitating exercises, chairing the Interagency Security Committee and leading/coordinating the associated security for Federal facilities, providing training and technical assistance, and assisting state and local authorities in implementing and evaluating progress toward reducing risks and enhancing resilience. Thus far in FY 2024, ISD has delivered a total of 86 exercises to critical infrastructure sectors across 27 states and territories, in addition to 26 national or multi-jurisdictional exercises, reducing risk to critical infrastructure by identifying lessons learned and best practices that each sector can draw upon for future preparedness and security investments, enhancements, and developments. Approximately 92% of exercise participants state that the exercise resulted in enhanced preparedness and 94% state they will take steps to enhance preparedness based on the results of the exercise. In addition to exercises, ISD has delivered 146 infrastructure security and resilience assessments across 35 states and territories.

ISD also focuses on reducing the risk of targeted violence directed at our schools, communities, houses of worship, and other public gathering locations. In addition, ISD leads efforts to secure our Nation's chemical infrastructure through implementation of ChemLock which is a voluntary chemical security program created as a supplement to the Chemical Facility Anti-Terrorism Standards (CFATS) and targeted at those facilities that were not determined to be high-risk under the CFATS regulation. The budget also proposes to reauthorize the CFATS program and includes funding for the program. With the expiration of CFATS authorities, CISA can no longer require security measures at the more than 3,200 high-risk chemical facilities across the nation, can no longer accept facility chemical inventories and conduct risk assessments at an estimated 330 new facilities coming into possession of chemicals, has missed more than 1,300 inspections at these high-risk facilities of which 35% of the inspections typically reveal a security gap, and can no longer vet individuals with access to dangerous chemicals against the terrorist screening database – of which CISA estimates more than 70,000 individuals have gained access without these critical checks. This reauthorization will increase the security of our nation's chemical infrastructure.

The budget includes $130 million for emergency communications to ensure interoperability and to assist Federal and SLTT stakeholders. CISA's Emergency Communications Division (ECD) enhances public safety communications at all levels of government across the country through training, coordination, tools, and guidance. ECD leads the development of the National Emergency Communications Plan (NECP) and 56 Statewide Communications Interoperability Plans to maximize the use of all communications capabilities—voice, video, and data—available to emergency responders and ensure the security of data exchange. ECD provides priority access capabilities for voice, video, data and information services in the Next Generation Networks Priority Services (NGN-PS) program which are used by all branches of the federal government as well as many public and private sector critical infrastructure owners and operators. This investment in NGN-PS enhances continuity of operations and the ability of the national security and emergency preparedness community to communicate and assist local emergency responders to communicate over commercial networks during natural disasters, acts of terrorism, and other significant disruptive events. As of April 1st, 2024, CISA has over 1,330,000 stakeholders enrolled into the service. NGN-PS enables essential personnel to communicate when networks are degraded or congested. Priority communications are crucial to the continuity of operations when facing adverse conditions or incidents. CISA is focused on increasing access to its priority services among eligible personnel across all critical infrastructure sectors. Finally, ECD supports nationwide sharing of best practices and lessons learned through SAFECOM and Emergency Communications Preparedness Center governance bodies.

The budget includes $98 million for Stakeholder Engagement Division (SED) 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. With this funding, SED will continue to execute CISA's role as the National Coordinator and as the Sector Risk Management Agency (SRMA) for eight of the Nation's sixteen critical infrastructure sectors. In these roles, CISA ensures a coordinated approach to risk management for securing critical infrastructure that addresses the full spectrum of risks. CISA leads, organizes, and coordinates cybersecurity and infrastructure security actions across SRMAs and the federal government, collaborating between government and industry, and convening and sharing information with SLTT private-sector entities. For example, SED has conducted more than 25 engagements with industry, U.S. Government partners, and international stakeholders to understand AI-driven threats within the national security space. In partnership with the Federal Emergency Management Agency (FEMA), CISA will continue implementing the State and Local Cybersecurity Grant Program, including providing subject matter expertise and leading program evaluation efforts to ensure state and local entities can access grant resources to enhance cybersecurity resiliency and reduce cybersecurity risk. CISA will also bring awareness to stakeholders, including the general public and small & medium-sized businesses, on steps they can take to keep themselves, their families, friends, and their customers more safe and secure online. For example, CISA's Secure Our World public awareness program received more than a billion total impressions and has been re-shared thousands of times across various demographics, languages, and social media channels. We will help to grow the cyber workforce by working with K-12, universities, and community colleges.

Additionally, recognizing that much of the U.S. critical infrastructure interconnects and is interdependent with foreign assets, systems, or networks, CISA will continue its efforts alongside

the Department of State to strengthen the security and resilience of critical infrastructure by engaging international partners and allies to build situational awareness and capacity, facilitate operational collaboration, promote effective infrastructure risk management globally, and develop and promote international security and resilience. Working with international partners to reduce risk to our critical dependencies will allow us to set conditions for success in cooperation, competition, and conflict. CISA also manages key national, Presidential, and departmental committees, councils, and boards, including the Cyber Safety Review Board and CISA Cybersecurity Advisory Committee, to provide decision makers at all levels of government with recommendations and guidance to meaningfully improve the safety, security, and resilience of the critical infrastructure that we depend on every day.

Finally, the budget also includes $140 million for the National Risk Management Center (NRMC). The NRMC develops risk analytic products to inform decisions across all types of risks and all critical infrastructure sectors. These analytic products support investment and operational decision making throughout the public and private sectors. The budget provides continued funding for two vital efforts.

First, the funding will allow us to expand risk analysis and risk management across all critical infrastructure sectors. Work in this area includes efforts such as the FY 2024 risk analyses associated with the impacts of AI-use across critical infrastructure sectors and potential mitigation strategies. Additionally, CISA generates Infrastructure of Concern (IOC) lists for partners such as CISA's Regional Field Offices and FEMA. These lists are generated in response to multiple hazards such as a hurricane or a forest fire and prioritize critical infrastructure assets across all sectors likely to be impacted. In doing so, local authorities are informed in their mitigation and response planning. For example, the NRMC maintains an All-Hazards Analysis dataset (AHA), which is a dataset that captures both assets, systems, and the connections between them. CISA used this dataset in support of an FAA request to show the reliance of particular airports on common infrastructure outside of the transportation sector.

Second, the budget also provides funding to maintain analytic capabilities, including risk methodology and framework development to identify critical infrastructure interdependencies and cascading consequences. For instance, NRMC utilized a tool—called CASCADE, which is part of our Suite of Tools for the Analysis of Risk (STAR) when the State of Florida reported an issue with Lee County Utilities Water System due to extensive pipe breaks preventing water flow/pressure in the system. We have created a visualization depicting potential cascading impacts on hospitals and other critical infrastructure assets, which enabled partners to quickly identify additional key assets at risk. One practical example includes CISA's utilization of STAR/Cascade to evaluate KinderMorgan and the California-Nevada (CAL-NEV) Pipeline and their potential for cascading consequences to disruption of pipeline.

Again, 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. The risks we face are complex, geographically dispersed, and affect a diverse array of our stakeholders, including federal agencies, private sector companies, SLTT governments, and ultimately the American people. The FY 2025 President's budget requests the funding necessary for CISA to carry out these critical missions.

In closing, I would like to take a moment to recognize this Committee's strong support

for CISA. For myself, and on behalf of our CISA workforce, thank you for your support. We will continue to operate in an efficient and cost-effective manner. There is much to be done and I look forward to working with you to continue strengthening this Agency, and by extension, the security and resilience of the United States. Thank you and I look forward to your questions.