Chairman Joyce, Ranking Member Cuellar, and Members of the Subcommittee, thank you for the opportunity to testify regarding the Fiscal Year (FY) 2024 President's Budget for the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The FY 2024 President's Budget of $3.1 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 national functions. These functions are built as "systems of systems" with complex designs, numerous interdependencies, and inherent risks. While this structure allows for significant gains in efficiency and productivity, it also allows opportunities for nation-state actors and criminals, foreign and domestic, to undermine our national security, economic prosperity, and public health and safety, creating cascading effects across our Nation.

As the Nation's cyber defense agency, CISA is charged with leading 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 and branches of government, the private sector, academia, and the international community. CISA's Joint Cyber Defense Collaborative (JCDC), for the first time, enables the government, the private sector, and U.S. international partners to come together to develop joint cyber defense plans and enable real-time information sharing.

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 (FCEB) 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.

I am truly honored to appear before this Committee today to discuss how the President's Budget for Fiscal year 2024 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, 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 2024 President's Budget: Priorities

Looking forward into FY 2024, 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.

Building on the generous investments made by the Congress in FY 2023, the FY 2024 President's Budget provides the resources needed to continue these efforts. This budget represents a significant increased investment in CISA by the Biden Administration. The $3.1 billion requested for CISA in FY 2024 provides approximately $545.6 million or about 22% more than requested in FY 2023. The FY 2024 President's Budget recognizes the value of historical investments, and CISA's growing role in enhancing the security and resilience of our Nation, the work yet to be done, and confidence in our ability to execute.

The FY 2024 President's Budget continues to make 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 $493.1 million for Mission Support. CISA's Mission Support program provides enterprise leadership, management, and business administrative services that sustain day-to-day management operations for the Agency. This is essential to ensure we can hire a diverse and talented workforce and execute our missions with the technology and speed that keep us ahead of our adversaries.

Included in the FY 2024 President's Budget Mission Support account is a transfer of $191.7 million to centralize CISA Enterprise Wide Shared Services (EWSS) into the Mission Support PPA. This net zero transfer will allow for better management and greater transparency and oversight of the Mission Support requirements that sustain and support the whole CISA enterprise while providing the flexibility to address new and emerging threats that we may face.

In addition, the FY 2024 President's Budget includes $97.7 million in funding to support work to implement the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA). This funding will ensure CISA has the staffing, processes, and technology capabilities in place to successfully implement and utilize information provided through CIRCIA. The funding will support additional outreach efforts regarding the notice of public rulemaking and the planning efforts required to educate covered entities and CISA stakeholders on the cyber incident reporting requirements, reporting protocols, and reporting methods, as well as voluntary reporting options. In additional to the rulemaking process, this funding will ensure CISA can receive, manage, analyze, secure, and report on incidents reported under CIRCIA, maturing our current ability to receive and analyze incident reports, manage incidents, coordinate with and notify the interagency, and implement incident data protection functions required by CIRCIA, including additional staff to receive and route around-the-clock inbound reports.

Cybersecurity

The Cybersecurity Division (CSD) spearheads the national effort to ensure the defense and resilience of cyberspace. The FY 2024 President's budget includes $1.8 billion to build the national capacity to detect, defend against, and recover from, cyberattacks. CSD will continue working with federal partners to bolster their cybersecurity and incident response postures and

safeguard FCEB networks that support our nation's essential operations. CSD will also continue our critical work partnering with the private sector and State, Local, Territorial, and Tribal (SLTT) governments to detect and mitigate cyber threats and vulnerabilities before they become incidents.

The FY 2024 President's Budget initiates the Joint Collaborative Environment (JCE), which will enable CSD to develop an internal analytic environment that enables more efficient analysis of mission-relevant classified and unclassified data through automation and correlation to identify previously unidentified cybersecurity risks. The JCE enables CSD to fulfill its mission and better integrate cyber threat and vulnerability data across our federal, SLTT, and private sector stakeholders, and rapidly work with those stakeholders to reduce associated risk.

To effectively execute our role as the operational lead for federal civilian cybersecurity, CSD 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 2024 President's Budget request includes funding for the National Cybersecurity Protection System (NCPS) at $67.4 million; and Cyber Analytics Data System (CADS) at $424.9 million.

In FY 2024, portions of the NCPS will transition to the new CADS program with intrusion detection and intrusion prevention capabilities remaining under the legacy program. CADS will provide a robust and scalable analytic environment capable of integrating mission visibility data sets, visualization tools, and advanced analytic capabilities to cyber operators. CADS tools and capabilities will facilitate the ingestion and integration of data as well as orchestrate and automate analysis that supports the rapid identification, detection, mitigation, and prevention of malicious cyber activity.

Together with 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. The FY 2024 President's Budget requests $408.3 million for CDM. This investment in CDM enhances the overall security posture of FCEB networks by providing FCEB agencies and CISA's operators with the capability to identify, prioritize, and address cybersecurity threats and vulnerabilities, including through the deployment of Endpoint Detection and Response (EDR), cloud security capabilities, and network security controls.

The FY 2024 President's Budget also includes $48.2 million for CyberSentry. 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 provides best-in-class commercial technologies that allow both CSD analysts and each partner organization to rapidly detect threats that attempt to move from an organization's business network to impact industrial control systems. While CyberSentry is intended only for the most at-risk or targeted critical infrastructure entities, the resources requested for FY 2024 will support growing CyberSentry operations and deploying capabilities to additional critical infrastructure partners to meet significant demand for the program based upon operational successes achieved to this point.

Integrated Operations

The FY 2024 President's Budget includes $244.5 million to enable seamless and timely support to CISA stakeholders across the nation, meeting our partners where they are in communities in every state. The Integrated Operations Division (IOD) 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 that impact critical infrastructure. Additionally, IOD 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.

Infrastructure Security

The FY 2024 President's Budget includes $177.6 million for infrastructure security 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. To achieve this, CISA's Infrastructure Security Division (ISD) leads and coordinates national programs and policies on critical infrastructure security, including conducting vulnerability assessments, facilitating exercises, and providing training and technical assistance. ISD's mission focuses on efforts such as reducing the risk of targeted violence directed at our Nation's schools, communities, houses of worship, and other public gathering locations. In addition, ISD leads programmatic efforts to secure our Nation's chemical infrastructure through implementation of the Chemical Facility Anti-Terrorism Standards (CFATS) regulation.

Emergency Communications

The FY 2024 President's Budget includes $126.6 million for emergency communications to ensure interoperability and to assist and support 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 also assists local emergency responders to communicate over commercial networks during natural disasters, acts of terrorism, and other significant disruptive events. As directed by statute, the Emergency Communications program supports nationwide sharing of best practices and lessons learned through facilitation of SAFECOM and Emergency Communications Preparedness Center governance bodies.

Stakeholder Engagement

The FY 2024 President's Budget includes $85.5 million for CISA 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 roles and functions as the Sector Risk

Management Agency (SRMA) for eight of the Nation's 16 critical infrastructure sectors and will lead coordination with SRMAs, with the broader national voluntary critical infrastructure partnership community, and across all sectors to ensure the timely exchange of information and best practices. In partnership with the Federal Emergency Management Agency (FEMA), SED 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. Additionally, in partnership with FEMA, SED will develop and implement the proposed Critical Infrastructure Grant program to complement our efforts to build sustainable cybersecurity while protecting the Nation's most vital critical infrastructure by shoring up the cyber defenses of those small, discrete, resource poor component level suppliers that provide irreplaceable supplies or services to systemically important entities.

National Risk Management Center

Finally, the FY 2024 President's Budget includes $144.5 million for the National Risk Management Center (NRMC). NRMC develops analytic insights to identify and advance risk mitigation opportunities that improve national security and resiliency across critical infrastructure sectors. These analytic products support investment and operational decision making throughout the public and private sectors.

The FY 2024 President's Budget continues two critical efforts housed within NRMC related to SRMAs and National Critical Function (NCF) Analytics. First, funding will allow us to continue efforts to expand risk analysis and risk management across high priority critical infrastructure sectors. This risk analysis provides insight into cross-sectoral risk and significant sector-specific risks to support CISA in routinely identifying and prioritizing focused risk management opportunities to create tangible risk reduction outcomes.

Second, the FY 2024 President's Budget provides funding to continue our NCF efforts to enhance analytic capabilities, including methodology and framework development to identify and characterize critical infrastructure interdependencies within and across NCFs. This includes applied analysis to meet specific analytic requirements in the infrastructure community to enable CISA to understand consequences that extend beyond a single sector.

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. The risks we face are complex, geographically dispersed, and affect a diverse array of our stakeholders, including federal civilian government agencies, private sector companies, SLTT governments, and ultimately the American people. The FY 2024 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. For myself, and on behalf of our CISA workforce, thank you for your support. As one team unified behind our shared mission, we will continue to operate in an

efficient and cost-effective manner. There is much work to be done and I look forward to working with you during the FY 2024 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.