TESTIMONY

OF

Bridget Bean
Senior Official Performing the Duties of the 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

"*Oversight Hearing – The Cybersecurity and Infrastructure Security Agency"*

May 8, 2025
Washington, D.C.

Chairman Amodei, Acting Ranking Member Underwood, and Members of the Subcommittee: Thank you for the opportunity to testify regarding the accomplishments and priorities or the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

I am honored to appear before this Subcommittee and I look forward to discussing the state of our Agency and our ongoing efforts to ensure we make the most efficient and effective use of the resources Congress provides to CISA to carry out our commitment to the DHS mission to safeguard our homeland, our values, and our way of life.

As the Nation'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 that necessitates a whole-of-government and a whole-of-nation approach. CISA's mission can only be accomplished by fostering collaborative, trusted partnerships across all levels of government, the private sector, academia, and the international community.

CISA, will continue focus on strengthening our Nation's cyber and physical defenses. CISA plays two key roles in this mission. First, we are the operational lead for federal cybersecurity, charged with protecting and defending federal networks in coordination with the Office of Management and Budget, the Office of the National Cyber Director, and each agency. CISA also leads asset response to significant cyber incidents in partnership with the Federal Bureau of Investigation and the Intelligence Community for threat response and intelligence support, respectively.

Every day, CISA works with government partners such as the FBI and sector risk management agencies to identify and notify victims of cyber intrusions. Specifically, CISA identified that actors known as Volt Typhoon and Salt Typhoon compromised multiple critical infrastructure organizations—primarily in Communications, Energy, Transportation Systems, and Water and Wastewater Sectors—in the United States and its territories, including Guam. It's been assessed with high confidence that Volt Typhoon actors have been pre-positioning themselves for potential disruptive effects in the event of potential geopolitical tensions and/or military conflicts. Salt Typhoon actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals involved in government or political activity, and the copying of certain information subject to U.S. law enforcement requests pursuant to court orders. This ongoing threat from Volt Typhoon and Salt Typhoon underscores the urgent need for our continued vigilance and collaboration.

CISA continues to aid in incident response and proactive risk reduction in the wake of recent cybersecurity operational activities and incidents, to include Volt Typhoon and Salt Typhoon. In these instances, cyber threat actors have employed advanced tactics for pre-positioning in critical infrastructure allowing them to maintain undetected persistent access for a prolonged and sustained period. We continue to work with Federal and Critical Infrastructure partners to

detect and eradicate these actors from critical systems, including through our CyberSentry threat detection capability. As of the first Quarter of FY 2025, CISA has established operational partnership with 44 critical asset owners across 7 sectors, with additional partnerships planned.

Threat actors continue to gain initial access to critical networks by leveraging Known Exploited Vulnerabilities (KEV). Since January 21, 2025, CISA has worked urgently, adding 73 KEVs to the KEV Catalog, enabling network defenders across the nation to prioritize their mitigations. Further, CISA is fully committed to sustaining and improving the Common Vulnerabilities and Exposures program, a critical part of cyber infrastructure. Additionally, we continue to expand the deployment of protective and detection technologies across the Federal Civilian Executive Branch, increasing our CISA-led Endpoint Detection and Response capability to more than 415,000 endpoints. We also continue to block connections to malicious domains through our Protective Domain Name System service. In the first quarter of calendar year 2025, we blocked more than 700 million malicious connections across the federal civilian enterprise and 60 million malicious connections across Critical Infrastructure, preventing countless cyber incidents.

Since January 21, 2025, CISA has advanced its mission to safeguard the Nation's critical infrastructure through a range of cybersecurity, physical security, and emergency preparedness efforts. As part of its ongoing cyber defense operations, CISA has consistently issued detailed advisories addressing a wide range of cybersecurity threats. These advisories include comprehensive analyses of threat actor tactics, techniques, and procedures; indicators of compromise that network defenders can use to protect their systems; and recommended mitigations—underscoring CISA's unwavering commitment to enhancing the security, resilience, and reliability of the Nation's cyber infrastructure.

Looking ahead, CISA will work with federal partners to mature their cybersecurity and incident response postures and safeguard federal networks. CISA will also partner with the private sector and state, local, tribal, and territorial (SLTT) governments to detect and mitigate cyber threats and vulnerabilities to our Nation's critical infrastructure before they are exploited. We will enhance critical infrastructure protection by enabling risk-informed decision-making by owners and operators of critical infrastructure, as well as federal and SLTT partners.

In parallel with its cybersecurity mission, CISA has maintained a strong focus on physical security and special event support.

Since January 2025, CISA delivered 269 terrorism and criminal threat mitigation training courses to over 5,100 participants across all 10 regions. Additionally, CISA conducted 68 exercises—48 focused on cybersecurity and 20 on physical security

In April, CISA provided on-the-ground support for the 129th Boston Marathon by assessing risks to critical infrastructure, staffing multiple command posts, and training nearly 60 law enforcement and security personnel through surveillance detection courses. For the 250th Celebration of the Battles of Lexington and Concord, CISA conducted physical security assessments, delivered vehicle ramming prevention training, and supported operational coordination through staffing of the Unified Coordination Center.

CISA also provided 14 Active Shooter Preparedness trainings to more than 4,000 registrants, equipping security professionals with actionable guidance to strengthen emergency action plans. Furthermore, CISA advanced school safety by training more than 2,800 stakeholders on responding to anonymous threats of violence.

This year, CISA expanded our unmanned aircraft systems (UAS) security guidance, in collaboration with federal and private sector critical infrastructure partners, to address key capability gaps in UAS threat recognition, response, and detection. Additionally, CISA works closely with stadium owners, law enforcement, and the Federal Aviation Administration to coordinate UAS temporary flight restrictions for the 2025 FIFA Club World Cup, which will support 60 matches across 12 stadiums in 10 states.

On April 23, CISA conducted a full-scale exercise at Lincoln Financial Field in Philadelphia, bringing together more than 800 government and private sector partners to simulate emergency response scenarios for a FIFA World Cup 2026 match. The exercise enhanced coordination and tested procedures for information sharing, tactical communication, family reunification, and public messaging, strengthening interagency relationships ahead of the World Cup.

I am honored to represent CISA's work supporting our mission to understand, manage, and reduce risk to our nation's cyber and physical infrastructure. The risks we face are complex, geographically dispersed, and affect a diverse array of our stakeholders and, ultimately, the American people.

In closing, I would like to take a moment to recognize this Committee's strong support for CISA. We will continue to operate efficiently and cost-effectively. 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 for the opportunity to appear before you today, and I look forward to your questions.