TESTIMONY

OF

NICK ANDERSEN

ACTING DIRECTOR
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE

THE

COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

ON

"*Funding Lapse and Security Gaps: Assessing the Harmful Impacts of the DHS Shutdown on Americans"*

March 25, 2026
Washington, D.C.

Chairman Garbarino, Ranking Member Thompson, and distinguished Members of the Committee: thank you for the opportunity to testify on the impacts of the shutdown to the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Under President Trump's leadership, CISA remains laser-focused on fulfilling the mission Congress authorized when the agency was first established by President Trump in 2018: to lead the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. This work spans three primary areas: cybersecurity, infrastructure security, and emergency communications. To accomplish this mission, we work across all levels of government, industry and with international allies to defend against today's threats and to build a more secure and resilient infrastructure for the future.

The threat landscape is diverse and rapidly evolving. CISA works diligently to protect the American people, critical infrastructure, and our way of life from both cyber and physical threats. We maintain a deep understanding of network and physical security vulnerabilities, as well as the intent and capabilities of adversaries targeting both digital and physical systems. This knowledge enables us to strengthen the resilience of U.S. critical infrastructure and ensure systems and networks are prepared to withstand and respond when an adversary strikes.

As the operational lead for federal cybersecurity, CISA is tasked with protecting and defending federal networks. We coordinate across federal agencies, as well as with state, local, tribal, and territorial partners, and the private sector, to promote the adoption of risk-based best practices and ensure the government can effectively respond to the ever-evolving threat landscape.

Cyberspace remains uniquely challenging to secure. Today, malicious actors can operate from anywhere around the world, cyber and physical systems are increasingly intertwined, and complex networks create persistent vulnerabilities that are difficult to mitigate. Under normal operating conditions, CISA provides a wide range of cybersecurity resources and services that strengthen operational resilience, enhance cybersecurity practices, support organizational management of external dependencies, and reinforce the foundational elements of a robust and resilient cyber framework.

However, the shutdown prevents us from operating under normal conditions. Our ability to carry out our mission has been significantly constrained, and we are limited to supporting only excepted functions. This means we can generally sustain only the most essential functions needed to protect life and property or to prevent a significant national security risk. Many of our proactive services, planning, and industry and stakeholder engagements are paused or significantly scaled back due to the limited number of people allowed to work – without pay – during the shutdown. Planned engagements with critical partners are on hold, and our ability to respond to emerging cyber incidents may be reduced due to these shutdown limitations, increasing risk not only across the federal enterprise, but across all critical infrastructure sectors.

As we have said before, CISA is shutdown, but our adversaries are not.

CISA possesses operational capabilities to detect and respond to cyber and physical threats, and plan against risks across government, industry, and the faith-based community, just to name a few. We also issue guidance to federal agencies and the broader critical infrastructure community to help reduce vulnerabilities and systemic risk across the Nation's most essential systems and functions. Together, these efforts form the backbone of a more secure and resilient national infrastructure.

To further illustrate the breadth of our work and the impact of our efforts, in 2025, CISA issued three emergency directives to protect federal networks from critical vulnerabilities known to be targeted and exploited by nation-state adversaries. Additionally, in 2025, CISA expanded the deployment to federal agencies of its endpoint detection and response technology that provides cyber analysts with real-time visibility to detect and stop advanced threats—a capability that continues, but becomes operationally challenging during a shutdown, as response actions are more limited. During the Trump Administration, we have added to our catalog 292 known exploited vulnerabilities for critical infrastructure stakeholders to understand what malicious actors are actively exploiting.

CISA's strategic role in maintaining cybersecurity across federal networks and critical infrastructure has been impacted by this shutdown. Efforts to finalize the rulemaking process for the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), intended to foster timely reporting of cyber incidents, and ransom payments, have been paused. This shutdown has cancelled all seven previously scheduled town halls dedicated to stakeholder collaboration on CIRCIA. The suspension of these efforts impact progress on the CIRCIA rulemaking, thus delaying critical policy frameworks and adding vulnerability to national security. Additionally, the rulemaking delay threatens the advancement of coordinated responses and resolutions to cyber threats targeting the nation's critical infastructure.

During this shutdown, with the limited number of employees legally allowed to work without pay, we are not providing the full range of support as robustly as our stakeholders request. CISA currently has approximately 40% of its workforce as excepted during the funding hiatus, and activities are generally limited to protecting life and property, or functions that are otherwise excepted or exempted. For instance, development and execution of binding operational directives that protect federal networks from significant cyber threats could be delayed. A delay in the issuance of these directives would be a boon to our adversaries.

The Trump Administration understands that critical infrastructure security and cybersecurity is national security – and every facet of government must support and defend our nation and our way of life. This means the Federal Government cannot fight our adversaries alone, and we must empower our state, local, tribal, and territorial (SLTT) partners. Critical infrastructure sectors from America's largest metropolitan cities to the most rural communities face the same adversaries and threat landscape. To meet this challenge, when fully funded, CISA maintains a nationwide presence in 10 regions across the country to deliver tailored resources, training, and technical assistance to help our partners anticipate, withstand, and recover from threats.

Since 2025, to support these communities across the nation, CISA also delivered over one thousand counter-improvised explosive device trainings, added 102 new resources to the School

Safety Clearinghouse, completed 58 active shooter preparedness workshops with over 14,000 registrants, and executed 149 cyber and physical security exercises, to include exercises with FIFA World Cup host cities. These activities are somewhat constrained by the current shutdown.

CISA's support also incorporates critical elements of physical infrastructure security mentioned above, with many programs and services aimed at enhancing preparedness and resilience. CISA plays a vital role in securing the nation's physical infrastructure—providing critical assessments, facilitating resilience planning, and offering robust chemical and infrastructure security measures. These efforts are indispensable to safeguarding facilities, systems, and sectors vital to U.S. economic stability and public safety. In times of restricted operations, the impact on these preparedness and outreach initiatives compounds the challenges communities and stakeholders face in addressing vulnerabilities effectively.

The lapse in appropriations for DHS has significantly impeded CISA's ability to proactively mitigate cyber risks and physical security resilience at a time when there are numerous large-scale events, including the America 250 celebration and the FIFA World Cup, that require heighted preparedness. During a shutdown, CISA is limited to performing only essential functions necessary to protect human life and safeguard property, or functions that are otherwise excepted or exempted. These activities include responding to imminent threats, sharing timely vulnerability and incident information, maintaining our 24/7 operations center, and provision of cybersecurity shared services.

CISA's holistic approach seamlessly integrates cybersecurity and infrastructure security to fortify the nation's resilience against evolving threats. However, limitations on proactive functions, strategic planning, stakeholder engagement including with prioritized international counterparts, and the timely delivery of essential services diminish the overall preparedness and safety posture of our critical infrastructure. Operations in several mission areas, such as, incident response, security assessments, training, exercises, and special event planning, have been delayed due to operational constraints. The inability to fully support physical infrastructure assessments and resilience services limits the proactive measures that help mitigate risks. These services are vital to sectors vulnerable to physical threats, including those posed by natural disasters, terrorism, and attacks on critical facilities.

During my time at CISA, I have been impressed by not only the expertise and professionalism of our workforce, but also by their dedication to our agency's mission. Our workforce remained committed to the mission during the 43-day shutdown last fall and are continuing to demonstrate the same commitment to mission during this shutdown. The lapse in appropriations forces frontline security experts and threat hunters to work without pay, even as nation-state and criminal organizations intensify efforts to exploit critical infrastructure that Americans rely on – placing an unprecedented strain on our national defense. Employees have endured personal financial hardships. The shutdown affects morale, stability, and overall wellbeing. Quickly restoring funding for DHS remains essential to safeguarding the nation's critical infrastructure.

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