



TESTIMONY

OF

MADHU GOTTUMUKKALA

ACTING DIRECTOR

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

BEFORE

THE

HOUSE APPROPRIATIONS COMMITTEE -  
SUBCOMMITTEE ON HOMELAND SECURITY  
UNITED STATES HOUSE OF REPRESENTATIVES

ON

*“Oversight Hearing – Potential DHS Shutdown Impacts”*

February 11, 2026  
Washington, D.C.

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

Since President Trump took office last year, and with strong support and guidance from Secretary Noem, CISA has been laser-focused on fulfilling the mission Congress gave us when the agency was first established by President Trump in 2018: to support, strengthen, and secure our nation's critical infrastructure. Today, our work is squarely aligned with the agency's original statutory purpose. That means working with government and private sector partners to ensure the digital and physical systems that our nation depends on remain resilient.

CISA is not a reactive agency that sits around waiting for the next cyberattack to happen. We are leading the fight against cyber threat actors. We have strengthened our operational capabilities to detect and to respond to cyber threats, deepened collaboration across government and industry, and continued to provide guidance to the critical infrastructure community to reduce vulnerabilities and systemic risk across our nation's most critical systems and functions as malicious actors seek to exploit our Nation's infrastructural vulnerabilities.

Under the Trump Administration, CISA is focused on our number one priority: protecting and defending the American people. CISA's work has reduced the impact of cyber incidents and helped to ensure that Americans continue to use the critical infrastructure functions that they rely on. The agency also continues to share threat and incident reports, coordinate intelligence across the Federal Government, and partner through structured meetings and threat briefings to strengthen resilience nationwide.

As the operational lead for federal cybersecurity, and as part of our mission to protect and defend federal civilian networks, CISA strengthened its coordination with each department and agency to promote the adoption of risk-based, common policies and best practices to effectively respond to the ever-evolving threat landscape.

Secretary Noem recognizes that cybersecurity is national security, and in 2025, under her leadership, CISA issued three emergency directives to protect federal networks from critical vulnerabilities and cyber threats. CISA also scaled its Endpoint Detection and Response (EDR) Technology, giving analysts near-real-time visibility to detect and stop advanced threats. Furthermore, during this Administration, we have added 257 Known Exploited Vulnerabilities (KEVs) to the list for stakeholders to understand what malicious actors are exploiting.

The Trump Administration recognizes that the Federal Government cannot fight our Nation's adversaries alone—we must empower our local partners. That is why CISA has worked alongside our state, local, tribal, and territorial (SLTT) governments to deliver security to our local partners. With a nationwide presence in 10 regions across the country, CISA delivered tailored resources, training, and technical assistance to help our partners anticipate, withstand, and recover from threats. We also recognize that many SLTT governments across the country are constrained by smaller, more limited operating budgets, and fewer IT staff than a similarly sized business. Secretary Noem and I recognize this challenge, and so to help support our SLTT partners last year, the Department of Homeland Security released Notice of Funding

Opportunities for the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP) –\$91.7 million to states and territories and \$12.1 million to Tribal Governments to assist with managing and reducing systemic cyber risk.

These efforts helped to ensure that Americans could continue relying on essential services. However, a lapse in funding for DHS would impede CISA’s ability to continue this good work. CISA currently plans to designate 888 of its 2,341 employees as excepted during a funding hiatus, and activities are strictly limited to those essential to protecting life and property. A shutdown forces many of our frontline security experts and threat hunters to work without pay—even as nation-states and criminal organizations intensify efforts to exploit critical systems that Americans rely on—placing an unprecedented strain on our national defenses.

It would delay deploying cybersecurity services and capabilities to federal agencies, leaving significant gaps in security programs. CISA’s capacity to provide timely and actionable guidance to help partners defend their networks would be degraded. Under the current DHS Lapse Plan, CISA can only sustain essential functions that are necessary to ensure the safety of human life or protection of property. Limited activities include responding to imminent threats, sharing timely vulnerability and incident information, maintaining our 24/7 operations center, and operating cybersecurity shared services. However, CISA would not perform any strategic planning, development of cybersecurity advice and guidance, or development of new technical capabilities. Since much of CISA’s key mission areas are centered around prevention and preparedness, it is harder to cleanly align an imminent threat to an excepted function. Should a DHS shutdown be ongoing, operations would become strained and service delivery delayed in core mission areas such as cyber response, security assessments, stakeholder engagements, training, exercises, and special event planning.

CISA is actively working to complete rulemaking on cyber incident reporting as required by the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). This work, along with upcoming efforts to obtain additional stakeholder feedback, would be paused and further delay our efforts to achieve a final rule.

Additionally, development and execution of binding operational directives (BODs) that protect federal networks from significant cyber threats could be delayed. For example, just last week, CISA issued a compulsory binding operational directive to federal agencies on *Mitigating Risk from End-of-Support Edge Devices*. Persistent cyber threat actors are increasingly exploiting unsupported edge devices—hardware and software that no longer receive vendor updates to firmware or other security patches. Positioned at the network perimeter, these devices are especially vulnerable to persistent cyber threat actors exploiting a new or known vulnerability. A delay in the issuance of these directives would be a boon to our adversaries.

President Trump, Secretary Noem, and I deeply value the dedication and professionalism of our workforce, whose tireless efforts ensure the safety and security of our nation's critical infrastructure. However, during a government shutdown, when many of our employees are required to work without pay, we recognize the significant challenges that this imposes on morale, financial stability, and overall well-being. A lapse in appropriations not only places undue financial stress on employees and their families but also introduces uncertainty into their

daily lives, making it harder to focus on the critical missions that we are tasked with accomplishing. The adverse effects of a shutdown are not just felt by our agency alone but also extend to the communities we serve, as delays or disruptions may impact our collective ability to protect and support national infrastructure security. Funding for DHS, and therefore CISA, is non-negotiable for safeguarding the nation's critical infrastructure.

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