TESTIMONY OF

Dr. Madhu Gottumukkala

Acting Director

Cybersecurity and Infrastructure Security Agency

U.S. Department of Homeland Security

BEFORE

Committee on Homeland Security
U.S. House of Representatives

ON

"Oversight of the Department of Homeland Security: CISA, TSA, S&T"

January 21, 2026
Washington, D.C.

Introduction

Chairman Garbarino, Ranking Member Thompson, and Members of the Committee, thank you for the opportunity to appear before you today, and for the opportunity to discuss the Cybersecurity and Infrastructure Security Agency's priorities to protect the nation's critical infrastructure from cyber and physical threats.

I appreciate the Committee's continued support for the critical mission that CISA carries out on behalf of the American people. 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. Our work today is squarely aligned with the agency's original statutory purpose. That means working with government and private sector partners to protect our financial systems, safeguard our pipelines, and ensure the digital and physical systems our nation depends on to remain resilient against disruption from possible cyberattacks.

To do this, over the past year, CISA has focused its work on efforts aligned to the agency's statutory priorities, including:

- Reinforcing federal civilian network defense.
- Supporting critical infrastructure nationwide in defending against physical and cyber threats.
- Delivering security directly to state and local governments by offering an array of no-cost resources and tools, such as technical assistance, exercises, and cybersecurity assessments.
- Continuing to share threat information and mitigation guidance in a faster, more integrated way.

Through these efforts, we remain deeply committed to working side by side with organizations of every size, across every critical sector. Because no single entity — not even the Federal Government — can manage these risks alone.

Thanks to the leadership of President Trump and Secretary Noem, CISA is leading the fight against malign actors. We 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 malign actors seek to exploit our Nation's vulnerabilities.

CISA has continued to provide practical services and guidance to critical infrastructure owners and operators, helping them to improve their resilience, limit disruptions, and recover more quickly when incidents do occur.

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 could continue to use the critical infrastructure functions 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 work 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.

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 address cybersecurity risks.

CISA remains dedicated to supporting critical infrastructure owners and operators. Physical security, defending against physical threats, remains a no-fail mission for the agency. In FY 2025, CISA continued to train public and private sector stakeholders on counter-improvised explosive device (C-IED) and risk mitigation practices, enhancing threat awareness, preparedness, and capabilities across the critical infrastructure community.

We also continue to look ahead to preparing for major events in 2026 and beyond, including the FIFA World Cup, America 250, and the 2028 Olympics in Los Angeles. To give you just one example of this work, in April, CISA convened participants from more than 40 agencies at Lincoln Financial Field in Philadelphia, one of the 11 American Host cities, for a full-scale exercise ahead of the FIFA World Cup. The exercise produced areas for improvement and action recommendations to enhance coordination, communication, and public safety.

Continuing to look ahead as we begin 2026, CISA will reinvigorate its mission first approach. We will be launching targeted initiatives designed to close the most pressing risk gaps facing critical infrastructure – particularly where cyber threats intersect with real world consequences. These efforts are intentionally scoped, operationally focused, and aligned with the Trump Administration's broader goals and priorities of efficiency, accountability and impact. We are prioritizing what works from previous lessons learned, eliminating duplication, and ensuring

every new service or product we release directly advances CISA's statutory mission and responsibilities.

For example, CISA is currently reviewing public comments on the proposed rule for the Cyber Incident Reporting and Critical Infrastructure Act of 2022, or CIRCIA. CISA appreciates the input it received from Congress and the public about aligning with Congressional intent and streamlining the CIRCIA requirements. CISA is also cognizant of the concerns raised regarding the scope and burden of the rule and improving harmonization of CIRCIA with other federal cyber incident reporting requirements. CISA is considering this feedback as it works to issue a final rule. I look forward to continuing to engage with Congress on these efforts and providing updates as the final rule process nears its completion.

Mr. Chairman, I would like to take a moment to thank Congress, and particularly this Committee under your leadership, for their work on reauthorizing CISA 2015, which is mission-critical for CISA's work and information sharing with the private sector. The Secretary and I have been very clear that we fully support the reauthorization of this vital piece of legislation.

CISA remains steadfast on the agency's statutory intent, we also recognize that a disciplined mission requires the right workforce – not a larger one, but a more capable and technically skilled one. In 2026, CISA will continue to right-size and rebalance its workforce by prioritizing highly technical professionals in mission critical roles, including cybersecurity operators and infrastructure security experts. These targeted positions will support frontline critical infrastructure owners and operators across every region in the United States in reducing their long-term risks. We will execute our hiring authorities while remaining consistent with the Administration's efforts to streamline the government workforce, control cost, and maximize return.

Under President Trump's leadership and Secretary Noem's guidance, CISA remains committed to being a focused, efficient, and accountable agency – one that executes the mission Congress assigned, supports the Administration's priorities, and delivers real security outcomes for the American people. We look forward to continuing to work with this Committee to ensure that CISA has the tools and capabilities necessary to protect the nation's critical infrastructure.

Thank you again for your support and I look forward to your questions.