Testimony
of

Nick Andersen
Acting Director
Cybersecurity And Infrastructure Security Agency
U.S. Department Of Homeland Security

before the

U.S. House of Representatives
House Appropriations Committee
Subcommittee on Homeland Security

on

The Fiscal Year 2027 Budget for the Cybersecurity and Infrastructure Security Agency

April 16, 2026
Washington, D.C.

Chairman Amodei, Ranking Member Cuellar, and distinguished Members of the Subcommittee, thank you for the opportunity to testify regarding the Fiscal Year (FY) 2027 President's Budget for the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The FY 2027 President's Budget of $2.5 billion for CISA reflects our commitment to the DHS mission to safeguard our homeland, our values, and our way of life.

Under the Trump Administration, 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 resilience, and emergency communications. To accomplish this mission, we work across all levels of government and with industry stakeholders and international allies to defend against threats and build a more secure and resilient infrastructure for the future. The FY 2027 President's Budget provides the resources needed to continue efforts that protect the systems Americans rely on—strengthening federal networks, empowering State, Local, Tribal, and Territorial (SLTT) governments with cybersecurity and physical security, and securing critical infrastructure nationwide.

Securing our Nation's critical infrastructure is a shared responsibility requiring not only a whole-of-government, but also a whole-of-nation approach. CISA accomplishes our mission by building collaborative, trusted partnerships across all levels of government, the private sector, academia, and the international community.

The threat landscape today is more diverse and more rapidly evolving than when President Trump first established us. Today, cyber and physical systems are increasingly intertwined, and complex networks create persistent vulnerabilities that are difficult to mitigate. We continue to work 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 cyber and physical security vulnerabilities, as well as the intent and capabilities of adversaries targeting both digital and physical systems. These capabilities enable us to strengthen the resilience of U.S. critical infrastructure and ensure infrastructure and networks are prepared to withstand and respond when an adversary or natural disasters strike. This FY 2027 budget will help CISA continue to focus on executing our statutory mission and strategically align our staffing to ensure seamless continuity and maximum efficiency across all core mission areas.

As the federal operational lead for cybersecurity, CISA is tasked with protecting and defending federal networks. In FY 2026, we issued Binding Operational Directive 26-02: *Mitigating Risk from End-of-Support Edge Devices*, which specifically addresses insecure devices deployed on the "edge" of public-facing areas of federal networks, exposed to external environments such as the internet. We have issued three emergency directives since January 2025 aimed at identifying, updating, and assessing potential compromises to federal systems. CISA diligently works with its partners to scrutinize the threat landscape to identify and provide guidance to address significant threats targeting federal agencies.

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. Since January 2025, we have issued 42 joint cybersecurity advisories with law enforcement and international partners and provided threat intelligence guidance to combat evolving threats and protect critical infrastructure. We remain steadfast in our mission and focused on President Trump's policies for maximum security for all Americans.

The FY 2027 President's Budget includes $1.4 billion for the Cybersecurity Division to continue to build the national capacity to detect, defend against, and build resilience to cyberattacks to our critical infrastructure. CISA continues to engage with federal partners to bolster their cybersecurity and incident response postures and safeguard federal networks. We also coordinate with SLTT partners, international partners, and the private sector to promote the adoption of risk-based best practices and ensure the government and private sector can effectively respond to the ever-evolving threat landscape.

Over the last year, we have expanded the deployment to federal agencies of commercial endpoint detection and response technology that provides cyber analysts with real-time visibility to detect and stop advanced threats. During the second Trump Administration, we have added 292 known exploited vulnerabilities and recommended remediations to our catalog—bringing our total to more than 1,500 known exploited vulnerabilities—to help critical infrastructure and other stakeholders better manage vulnerabilities and keep pace with threat activity. Many intrusions are enabled by known exploited vulnerabilities.

Our Continuous Diagnostics and Mitigation (CDM) program remains an invaluable tool for rapidly deploying protection to federal agencies, resulting in increased operational visibility and an ability to defend against threats both at the agency and federal enterprise levels. The budget requests $410 million for this program, which provides CISA with invaluable operational visibility inside agency networks that helps drive targeted and enterprise-wide cybersecurity improvement actions. The CDM program enables agencies and CISA to respond to cyber threats in a coordinated and expedited fashion by sharing data between dedicated CDM Dashboards; and through CDM's implementation of government-wide threat detection through Endpoint Detection and Response (EDR) that facilitates an unsurpassed level of visibility into threats and incidents targeting federal networks, allowing faster detection and mitigation for CISA operators.

The budget additionally includes $178 million to deliver risk reduction services locally to CISA stakeholders in their community. 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 SLTT partners. Critical infrastructure located from America's largest metropolitan cities to the most rural communities faces determined adversaries and an ever-evolving threat landscape. To meet this challenge, 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. The budget includes funding to bolster cybersecurity across all 50 states

and major territories by deploying dedicated personnel to fortify local defenses, coordinate responses, and support recovery efforts against escalating cyber threats. Additionally, CISA's Integrated Operations Division provides intelligence context to support decision making, performs Agency-designated Emergency Support Functions, and monitors and disseminates cyber and physical risk and threat information to CISA stakeholders 24/7/365.

The budget includes $391 million for infrastructure security and resilience 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. CISA's Infrastructure Security Division is the operational lead and coordinates and executes national programs and policies on critical infrastructure security and resilience, including analyzing critical infrastructure and key dependencies, developing and conducting vulnerability assessments, and assisting state and local authorities in implementing and evaluating progress toward reducing risks and enhancing resilience.

The FY 2027 budget includes an increase of $5 million for the support of enhanced security for the 2028 Los Angeles Olympics, which is a National Special Security Event. The funds will support cyber and physical security exercises to evaluate the incident response plans and capabilities of Federal and SLTT Governments, as well as those of our venue security partners, to identify gaps before the games.

Over the last year, CISA has completed vulnerability physical and cyber assessments at ten World Cup host stadiums and at FIFA basecamps, team hotels, and supporting critical infrastructure. Since January 2025, CISA completed over 1,000 engagements, exercises, security assessments, and training activities for the World Cup. These activities provided risk reduction services supporting the agency's missions in cybersecurity, infrastructure protection, and emergency communications. In January 2026, CISA organized six exercises specifically aimed at the World Cup, involving nearly 200 federal partners and 2,000 participants from stadiums and host cities.

CISA also assesses and manages unmanned aircraft system threats, supports the Federal Aviation Administration efforts to establish flight restrictions to protect critical infrastructure, and increases public awareness of legal drone operations through CISA's Be Air Aware™ campaign. The breadth of CISA's involvement in strengthening the resilience of the Nation's critical infrastructure sectors is vast. In 2025, CISA delivered over 1,000 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 2026 host cities.

The budget includes $98 million for emergency communications to ensure interoperability and to assist federaland SLTT partners. CISA provides plans, resources, and training to public safety, national security, and emergency preparedness communities to ensure they can seamlessly and securely communicate during steady state and emergency operations in the event of natural disasters, acts of terrorism, and other hazards. 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 provides priority access capabilities for voice, video, data, and information services. ECD consults with SLTT partners to develop a National Emergency Communications Plan (NECP) for better emergency communications collaboration. The program fosters cooperation through SAFECOM for SLTT partners and the Emergency Communications Preparedness Center (ECPC) for federal partners to improve resiliency, interoperability, and security. It offers priority telecommunications services over various networks to ensure communication during National Security and Emergency Preparedness (NS/EP) events. The program provides strategic planning, grant guidance, and common investment and infrastructure planning to enhance emergency communications efficiencies.

The budget includes $31 million for activities focused on executing CISA's role as the national coordinator and as the Sector Risk Management Agency for eight of the Nation's sixteen critical infrastructure sectors. CISA will continue to lead and coordinate the implementation of the critical infrastructure partnership framework recommendations provided to the President pursuant to Section 9002 of the FY 2021 National Defense Authorization Act, as well as any subsequent national-level policy regarding critical infrastructure security and resilience.

Effectively and efficiently executing CISA's mission requires expertise and data on the Nation's critical infrastructure and the complex and dynamic risk environment it faces. The budget includes $42 million in funding for the National Risk Management Center (NRMC) to support the identification and prioritization of critical infrastructure and the analysis and assessment of physical and cyber risks. Such risk assessments support key White House priorities such as the development of a National Risk Register, as well as homeland defense efforts by the Department of War. These data sets, expertise, analyses, and assessments ensure that precious federal resources are laser-focused where they can have the greatest risk-reduction value for the American people. In addition, the NRMC provides specialized risk analysis and risk management planning and coordination in known areas of cross-sector infrastructure risks such as space systems and undersea cables.

As the longest shutdown in history continues, CISA implores the House to pass the Senate DHS funding bill and work expeditiously to enact a second reconciliation measure by June 1st to provide sustained funding to ICE and Border Patrol.

The President, his Administration, and I fully recognize the importance of CISA and its mission. We will continue to operate with the fiscal discipline and operational resilience the American people expect.

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