TESTIMONY OF

Ha McNeill

Senior Official Performing the Duties of the Administrator

Transportation Security Administration

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

Good morning, Chairman Garbarino, Ranking Member Thompson, and distinguished Members of the Committee. Thank you for the invitation to testify before you today on behalf of the Transportation Security Administration (TSA). I am honored to be here and grateful for the longstanding and productive partnership TSA shares with this Committee.

I would like to start by thanking TSA's employees for their unrelenting efforts day in and day out to secure the Nation's transportation systems. TSA is an agile security agency, embodied by a dedicated and professional workforce that works tirelessly to outmatch an increasingly sophisticated and dynamic threat.

Under the Trump Administration and Department of Homeland Security (DHS) Secretary Kristi Noem, TSA is laser-focused on delivering for the American people, fortifying travel security, renewing its commitment to the traveler experience, and serving as a responsible steward of the American tax dollar. This starts with deploying upgraded, state-of-the-art technology to airports nationwide, renewing our commitment to the American taxpayer, returning to our core mission, leveraging public-private partnerships, and enhancing hospitality and the passenger experience.

TSA Priorities

With the transportation sector remaining a top target for malign actors, and passenger volumes at airports reaching record highs in 2025—including eight out of the top ten busiest travel days on record—it is more critical than ever to have a technologically advanced, seamless, and secure aviation security system. In 2025 alone, TSA screened 906.7 million passengers, 480 million checked bags, and 2.1 billion carry-on bags.

The upcoming 2026 World Cup, America250 events, and 2028 Summer Olympics present an enormous opportunity to boldly transform transportation security in the United States. Through new policies, legislation, and private-sector partnerships that support technological innovation and modernizing the screening process, we can usher in President Trump's vision for a new Golden Age of American travel.

Leveraging Public-Private Partnerships to Advance the Mission

TSA's mission is supported by critical public-private partnerships, and the Trump Administration, DHS, and TSA are strongly committed to working more collaboratively with industry stakeholders than ever before, utilizing their expertise and efficiency, to strengthen aviation security and improve the passenger experience. On that note, I would like to thank this Committee for ensuring TSA and our critical interagency, state, local, and private sector partners have the resources needed to mitigate the evolving threat landscape, which includes the proliferating cybersecurity and Counter-Unmanned Aircraft Systems (C-UAS) threats.

Screening Partnership Program

Under the Screening Partnership Program (SPP), TSA contracts with qualified private companies to provide personnel to perform security screening operations at commercial airports. TSA is working closely with Congressional and industry partners to modernize SPP to incentivize airports and industry to invest in more tailored and innovative solutions faster, to optimize security operations, while maintaining the Agency's rigorous regulatory oversight and outcome-based security standards.

One-Stop Security

In close partnership with the Department of State, industry, and international partners, TSA is advancing the One-Stop Security (OSS) pilot program. OSS improves international aviation security, streamlines the transfer process for passengers inbound to the United States with connecting flights, and eliminates the need for passengers and their bags to go through screening again. Last summer, TSA launched its first OSS pilot location at London-Heathrow Airport (LHR), demonstrating an immediate success for all stakeholders. Currently, there are seven OSS flights per day from LHR into Hartsfield-Jackson International Airport (ATL) and Dallas–Fort Worth International Airport (DFW), saving each OSS passenger up to two hours that he or she can now use to relax, shop, and dine at the airport.

Reimbursable Screening Services Program

Another critical pilot program that Congress has afforded us to explore with industry partners is the Reimbursable Screening Services Program (RSSP). RSSP enables TSA to work with industry to screen passengers in a location separate from the checkpoint, such as an off-airport cruise or VIP terminal. RSSP is an innovative public-private partnership to alleviate congestion at the checkpoint and offset TSA costs. Permanently authorizing RSSP, which is set to expire on January 30 of this year, will provide certainty and unlock innovation, further increasing industry interest and participation.

Investing in Modernizing Security Technology

Starting in 2004, Congress authorized the first $250 million in revenue collected each year from the Passenger Security Fee to go to the Aviation Security Capital Fund (ASCF), to be used for checked baggage technology. Along with amounts provided in annual appropriations, amounts in the ASCF were meant to recapitalize and modernize TSA screening technology, but unfortunately this level of investment has not kept pace with changing technology and the evolution of the threat landscape.

Over the past several years, Congress has diverted approximately $1.6 billion in TSA Passenger Security Fee revenue each year for deficit reduction purposes. The President's FY 2026 Budget proposes to eliminate the deficit reduction contributions and instead direct Passenger Security Fee amounts to their intended purpose of bolstering TSA aviation screening operations. The FY

2026 Budget also includes proposed additional investments in aviation screening technology, such as Computed Tomography (CT) technology, that can supplement ASCF amounts to make improvements to both security and the passenger experience at the checkpoints. TSA encourages Congress to act on the President's FY 2026 Budget request so that the ASCF is not the only source of funding for modernizing TSA security technology.

Renewing Focus on Core Mission and Serving the American Taxpayer

REAL ID

Under the leadership of Secretary Noem, since May 2025, TSA is fully enforcing its statutory requirements under the *REAL ID Act of 2005*. The legislation was enacted in response to the 9/11 Commission Report recommendations aimed at combatting fraudulent identity documents (IDs) and ensuring passengers are who they say they are. As the 9/11 Commission Report stated, "For terrorists, travel documents are as important as weapons." This Administration acted swiftly to enforce the law to ensure TSA maintains the highest standards of aviation security for the American taxpayer and traveler.

Currently, most travelers (about 94 percent) present either a REAL ID-compliant or another acceptable form of ID. However, we must ensure that everyone who flies is who they say they are. TSA ConfirmID is a new modernized alternative identity verification system to enhance and streamline identity verification for travelers that do not have an acceptable form of ID.

Starting February 1, 2026, travelers who do not present an acceptable form of ID at TSA checkpoints and still want to fly, have the option of paying a $45 fee and undergoing the TSA ConfirmID process. The fee ensures that the cost to cover verification of an unacceptable ID will be borne by the non-compliant traveler, not the American taxpayer, and prevents malign actors from getting on a plane. TSA will continue working closely with all states to increase adoption of REAL IDs and urges all travelers to obtain a REAL ID, or other acceptable form of ID, as soon as possible to avoid delays and potentially missing flights.

Improving the Travel Experience for Our Military and American Families

TSA is committed to making the airport experience as smooth and stress free for active-duty military personnel and their families, and American families traveling with children. To honor those who protect our Nation and to recognize their service and sacrifices, TSA has established the "Serve with Honor, Travel with Ease" program, which provides dedicated screening lanes for active-duty military personnel and their families at airports near the Nation's largest military bases. Similarly, the Agency is actively working to create a welcoming environment for families with children. TSA's new "Families on the Fly" program provides dedicated lanes for families at select airports to create a welcoming environment and ease stress for families traveling with children.

Conclusion

Today, TSA is at a strategic crossroads. With continued support from Congress and industry partners, a screening process that is more efficient, technologically integrated, secure, and affordable to the American taxpayer, is within our grasp. Chairman Garbarino, Ranking Member Thompson, and distinguished members of the Committee, it is a privilege to testify before you today.

I thank you for your support of TSA and look forward to your questions.

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.

TESTIMONY OF

Pedro M. Allende

Under Secretary

Science and Technology Directorate

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 distinguished Members of the Committee, thank you for the opportunity to testify before you today. I am honored to have the confidence of President Trump and Secretary Noem to serve as the Under Secretary for Science and Technology (S&T) at the Department of Homeland Security (DHS). I look forward to executing the Trump Administration priorities to make the nation safer through advancement and application of science and technology.

I appreciate the Committee's continued engagement with the DHS S&T Directorate, and I look forward to our work together during my tenure as Under Secretary.

The S&T Directorate plays a unique role within DHS. We are responsible for understanding emerging threats and opportunities, and for ensuring the Department has access to timely, effective, and responsible technology solutions to meet its evolving mission needs. As threats to the homeland become more complex, adaptive, and technology-enabled, S&T's mission is to help DHS stay ahead of those challenges.

S&T works closely with DHS operational components, the private sector, academia, international and interagency partners to deliver solutions that enhance security, improve efficiency, and strengthen operational effectiveness. Our success is measured not by research alone, but by outcomes delivered to operators and the American people.

In my short time in this role, I have been energized by seeing S&T in action and witnessing firsthand the critical role technology plays in keeping our nation safe.

Just last week, I had the opportunity to meet with our partners at operational sites on the West Coast, including our DHS colleagues in the Transportation Security Administration (TSA), the U.S. Customs and Border Protection (CBP), and the U.S. Coast Guard, as well as our local law enforcement partners. At Los Angeles International Airport (LAX), I observed TSA security operations and gained valuable insight into how emerging technologies can create new opportunities for enhanced safety and security. At SoFi Stadium, I engaged with security teams to discuss how innovative solutions can strengthen our defenses as we prepare to host the FIFA World Cup in the summer of 2026.

I toured the complex operations and technology required for cargo operations and screening by CBP as they ensure the safety of two of the largest U.S. seaports in Los Angeles and Long Beach, California, to cargo operations and screening. At the Air and Marine Operations Center, I met with partners to discuss collaborative activities, such as the Kestrel system which enhances their ability to determine highest-priority threats and make real-time operational decisions and explore enhancements to achieve full domain awareness across our borders and airspace.

My experiences this past week have crystalized for me the importance of advancing the Administration's priorities and my commitment to ensuring S&T remains focused on the needs of our operational components while staying ahead of our adversaries. Our organization is also taking on broader challenges, including leading efforts in areas such as Counter-Unmanned Aircraft Systems. Secretary Noem recently announced the establishment of the Program Executive Office for Unmanned Aircraft Systems and Counter-Unmanned Aircraft Systems, investing to rapidly procure and deploy advanced counter-drone technologies. As Secretary Noem noted, these are critical investments to protect our borders and to keep Americans safe and secure during America 250 celebrations and at 2026 FIFA World Cup venues.

My recent trip also enabled me to engage with private sector partners, which will be a key theme of my service as Under Secretary. Not only does the private sector operate much of the critical infrastructure upon which our nation relies, but they are a major source of technological innovation necessary to protect the homeland. One of my guiding principles will be to seek out and adopt private sector solutions whenever possible. Leveraging existing or adaptable technologies will allow DHS to accelerate delivery to the field.

I look forward to working with Congress on key legislative priorities including the restoration of Other Transaction Authority (OTA). OTA is a critical tool used to partner with nontraditional small- and medium-sized businesses and organizations on innovations that enhance our national security. The expiration of the authority on September 30, 2024, brought to a halt various efforts at S&T to develop solutions across several mission areas.

Chairman Garbarino, Ranking Member Thompson, and Members of the Committee, S&T is committed to delivering innovative, responsible, and operationally relevant solutions that strengthen the security of the homeland.

We look forward to continuing our close collaboration with Congress, across DHS components and partner agencies, and our external partners as we work to execute Administration priorities, understand emerging threats, and leverage private sector innovation to make the nation safer.

Thank you for the opportunity to testify. I look forward to your questions.