TESTIMONY

OF

HA MCNEILL

SENIOR OFFICIAL PERFORMING THE DUTIES OF THE ADMINISTRATOR
TRANSPORTATION SECURITY ADMINISTRATION
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE

THE

HOUSE COMMITTEE ON HOMELAND SECURITY

ON

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

March 25, 2026
Washington, D.C.

Introduction

Chairman Garbarino, Ranking Member Thompson, and 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.

TSA was created on the heels of 9/11 to help the United States stay a step ahead of terrorists and bad actors, and we are nearing our twenty-fifth anniversary later this year. We have entered each fiscal year of this agency's existence under a Continuing Resolution, and we have been shut down for 50% of this fiscal year. However, the transportation sector remains a top target for our enemies and terrorists, all while passenger volumes are reaching record highs. A lack of funding and predictability of resourcing poses significant challenges to our ability to deliver transportation security with the level of excellence we expect, and Americans deserve. We need Congress to pass the Department of Homeland Security's (DHS) budget for Fiscal Year (FY) 2026 and fund TSA.

Shutdown Impacts: TSA Workforce

TSA's greatest asset is its people, and I want to thank them for their unrelenting efforts day in and day out to secure the Nation's transportation systems. TSA's national security mission does not stop during a shutdown, and the Agency continues to screen around three million passengers on peak days. Around 95%, or more than 61,000, of TSA employees are deemed essential and must continue working to protect the traveling public during a shutdown, while not getting paid. Congress must fund DHS and pay our talented and dedicated TSA workforce.

Missed Paychecks

TSA employees work at over 430 commercial airports, living within your communities, not getting paid for performing incredibly challenging and taxing jobs. Many Transportation Security Officers (TSOs) work paycheck to paycheck trying to support themselves and their families. During a shutdown, the ability to pay for rent, bills, groceries, childcare, and gas becomes very challenging. TSA employees have already worked 87 days without getting paid in FY 2026, and by this Friday, March 27, we will be at nearly $1 billion in payroll that has not been paid in a timely manner. The dedicated public servants that work within DHS and TSA deserve better and to be paid.

We have heard reports of some airports asking the public to donate grocery store and gas gift cards in amounts of $10 or $20 to support officers. Officers are reportedly sleeping in their cars at airports to save gas money, selling their blood and plasma, and taking on second and third jobs to make ends meet, all while expected to perform at the highest level when in uniform to protect the traveling public. Many have received eviction notices, lost their childcare, missed bill payments and been charged late fees, damaged their credit, defaulted on loans, and have been unable to even qualify for a loan to help ease the financial burden during the shutdown.

Recruitment, Retention, Attrition, and Morale

Shutdowns and funding uncertainties have real and measurable impacts on recruitment, retention, and employee morale. TSA employees are dedicated public servants that want to continue to keep the traveling public safe and secure, but they are running out of options to keep a roof over their head and put food on the table.

During the 43-day government shutdown in October and November 2025, around 1,110 TSOs separated from TSA, representing a 25% increase in TSO separations from the same time in 2024. Since the government funding lapsed in February, and the cost of coming to work is becoming more untenable for the workforce, as of Tuesday, March 24, TSA has already lost around 460 officers and daily call out rates at airport checkpoints have increased from 4% (pre-shutdown) to 11% nationwide, with multiple airports experiencing greater than 40% and 50% call out rates. TSA is currently grappling with the Spring Break travel surge and experiencing about 5% higher travel volume than last year, all with fewer TSOs working at the checkpoints to screen the higher number of passengers. This is reducing the Agency's operational capacity at airports, increasing wait times to over four and half hours at certain airports, raising major security risks and missed flights for passengers.

To maintain the security of our transportation systems at the level American's deserve, TSA needs to be able to retain its employees. Losing employees creates tremendous staffing, readiness, and operational challenges. The hiring and rigorous onboarding process for TSOs includes assessments, interviews, background checks, and a comprehensive four to six months training program to ensure candidates are fully qualified to perform the screening duties at checkpoints.

Shutdown Impact: FIFA World Cup

TSA does not have the luxury of time. The FIFA World Cup is kicking off on June 11 – less than three months away. We are anticipating a significant influx in passenger volume as fans travel through our airports to see the games. Even if TSA were to hire new officers upon conclusion of the DHS shutdown, those officers would not be able to work on the checkpoint until well after the World Cup has concluded.

Conclusion

The safety and security of Americans and the traveling public must not continue to be threatened by budget uncertainties. On behalf of TSA, I respectfully urge Congress to provide full-year funding for DHS without delay. Chairman Garbarino, Ranking Member Thompson, and distinguished members of the Committee, I thank you for your support of TSA and look forward to your questions.

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.

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave SE
Washington, DC 20593-7000
Staff Symbol: CG-0921
Phone: 202 372-4411
Fax: 202 372-8300

TESTIMONY OF
ADMIRAL THOMAS ALLAN
VICE COMMANDANT, U.S. COAST GUARD

ON
"FUNDING LAPSE AND SECURITY GAPS: ASSESSING THE HARMFUL IMPACTS OF THE DHS SHUTDOWN ON AMERICANS"

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY

MARCH 25, 2026

Chairman Garbarino, Ranking Member Thompson, and distinguished Members of the Committee, thank you for inviting me to testify on the severe impacts the current government shutdown is having on the United States Coast Guard. As of today, we are 39 days into the current lapse in appropriations. For the Coast Guard, this marks the third shutdown of this fiscal year. In total, for 85 of the last 176 days—for nearly half the year our Service has been without the funding necessary to operate and pay our people.

As a vital instrument of national power, the Coast Guard controls, secures, and defends the U.S. border and maritime approaches, facilitates the safe and secure flow of commerce that is vital to economic prosperity, and responds to crises that may come without warning. As a proud member of the Department of Homeland Security and the only Armed Force within the Department, every action the Coast Guard takes is dedicated to protecting our Nation. The American people depend on the Coast Guard, and the Service provides a remarkable return on investment—but only with consistent and predictable appropriations.

Under the lapse in appropriations, the Coast Guard suspended all missions except those for national security or the protection of life and property. While missions including law enforcement, national defense, and emergency response continue, this funding lapse is causing severe and lasting consequences for the Coast Guard's workforce, operational readiness, and long-term capabilities.

Most importantly, this lapse is creating profound and unacceptable financial strain for our people. While our military members, thankfully, received their pay up to this point, we are operating under the grim uncertainty of whether we can make the next payroll. The reality of missing paychecks creates significant financial hardship for service members and their families and erodes the sacred trust our men and women have in the Nation they serve.

For our dedicated civilian workforce, the shutdown creates an immediate and devastating impact. Our civilian personnel already missed several paychecks, leaving them without the resources needed to pay bills and support their families. This includes the nearly 75% of our civilian specialists—experts in finance, contracting, and information technology—who are furloughed. Their skills are critical and cannot be backfilled by our military crews. For our entire workforce,

this financial strain and uncertainty cripples morale and directly harms our ability to recruit and retain the talented Americans we need to meet growing demands.

The work our Coast Guard crews perform every day is dangerous and challenging. They deserve the certainty that they and their families will be cared for. A Gunner's Mate pursuing a drug smuggling vessel should not have to wonder if their family will be able to pay rent in the midst of a dangerous interdiction. The Aviation Survival Technician deploying from a helicopter into treacherous seas should not have to worry if their family can buy groceries that week. These jobs require dedication, focus, and attention to detail, and any distraction puts the member, mission, crew, and unit at risk. While military pay continued thus far, this shutdown creates other severe financial burdens. Our deployed crews are accumulating thousands of dollars in official expenses on their government travel cards with no way to be reimbursed. This mounting, personal debt is an unacceptable burden, and no service member should be forced to finance government operations out of their own pocket.

This shutdown is also eroding mission readiness by crippling our ability to meet our contractual obligations. We are unable to pay our contractors and vendors—including the many small businesses that rely on timely payment to survive. This failure creates a series of escalating risks to our operations. Each day the shutdown continues, we move closer to a tipping point. We face the imminent danger of widespread utility shutoffs at our bases and the refusal of fuel deliveries, which would sideline our cutters and aircraft from executing critical national security missions. The suspension of payments for cloud and satellite communications services threatens to sever vital command-and-control links. At our maintenance depot locations, the inability to pay for parts and services risks triggering stop-work orders from our shipyard partners, which would exacerbate our existing significant maintenance backlog. As we approach the April 1 start date for a new base security contract period, we face the possibility that vendors will be unwilling to commit to securing our facilities without a funded contract, leaving our installations vulnerable.

We ceased activities that do not protect the safety of human life or property from imminent danger, including routine patrols, fisheries enforcement, maintenance of aids to navigation, and commercial vessel safety inspections. The National Maritime Center remains closed, halting the issuance of credentials for our nation's merchant mariners. As of today, we project that over 15,000 Merchant Mariner Credential applications are stalled in processing—a backlog that grows by approximately 350 applications every single day this shutdown continues. The ripple effects are causing delays in vessel inspections and financing that cost the U.S. economy billions of dollars each week and increase costs for all Americans.

The Coast Guard will continue to serve, because that is what our people have sworn to do. But our crews should never question whether the nation they protect will stand behind them and their families. Ensuring stable funding for the Department of Homeland Security is not simply a budgetary matter, it is a matter of trust, readiness, and national security. Our service members will keep their watch. We ask only that Congress ensure they are supported while they do so. Thank you, and *Semper Paratus.*