THE 25TH ANNIVERSARY REPORT

Final Report
Committee on Homeland Security Majority
U.S. House of Representatives
"National Security Improvements and the Domestic Threat Landscape 25 Years After 9/11/01"

September 10, 2026

CHAIRMAN ANDREW R. GARBARINO, NEW YORK

Contents

Preface

WE ARE NOW AT AN IMPORTANT MOMENT IN OUR NATION'S HISTORY. An entire generation of Americans has been born in the years following the attacks of September 11th. While many of them are part of families that continue to live with the impacts of that day, this generation did not experience firsthand the terror that gripped the nation at that time. Their relationship with the events of that day comes mostly from recorded recollections in their history textbooks, stories from family and friends, annual remembrances, and memorials dedicated to those that made the ultimate sacrifice in service of their nation.

For these Americans, the Department of Homeland Security has always existed, there has always been a TSA, and the threat of global terrorism is a fact of life. They never experienced life before 9/11 and will always live in a world marked by the national security concerns of the modern era. We have worked tirelessly to make the world a safer place for future generations, but the United States remains forever changed.

Twenty-five years later, significant progress has been made towards strengthening our national security and ensuring we never again allow such an attack to be perpetrated against the United States. This no-fail mission requires persistent vigilance and adaptation to keep pace with the contemporary threat environment. For 250 years, the threats we face have continued to evolve, and so too must the nation's ability to counter threats to our nation and its citizens.

As Chairman of the Committee on Homeland Security, I understand this solemn undertaking. I vividly remember experiencing the attacks of the day unfold at my local high school, watching on in horror as thousands of civilians, first responders, and good Samaritans lost their lives at the hands of nineteen terrorists they had never met, who had set out to bring a country to its knees half a world away. I remember the fear, anger, and uncertainty I felt as our nation worked to recover and rebuild. And in the years after 9/11, we continue to lose countless more Americans to illnesses contracted during rescue and recovery efforts due to exposure to toxic chemicals at the sites of the World Trade Center, Pentagon, and in Shanksville, Pennsylvania.

September 11, 2001, was undoubtedly a day of immense grief and despair. The United States had been badly wounded, and we did not yet fully appreciate the entire threat which we were then forced to confront head on. However, our adversaries' goal of crippling our nation was ultimately unsuccessful. They *did not* win.

The days, weeks, and months following the attacks of September 11th represent a period of profound national unity. Citizens across the United States rallied behind a common goal of ensuring this would never happen again. First responders were rightfully hailed as heroes, receiving long overdue appreciation for their bravery, courage, and service to the nation not just on 9/11, but every day.

Thousands were lost on 9/11, but countless more were rescued due to the valiant efforts of police officers, firefighters, paramedics, and EMTs who rushed in to aid and evacuate survivors up until the very last possible moment. All their work resulted in the greatest rescue

operation in the nation's history, and continues to inform emergency preparedness, response, and mitigation efforts across the world.

Even Congress did something against its own nature – it acted quickly. The Transportation Security Administration was established just two months after 9/11. The Department of Homeland Security was created the following year, along with the establishment of the National Commission on Terrorist Attacks Upon the United States, which was tasked with compiling a full account of the attacks and providing recommendations to prevent future acts of terrorism. Shortly thereafter, the House of Representatives established the Select Committee on Homeland Security, which was then made a permanent standing committee of the House tasked with overseeing homeland security policy across the nation.

Following the release of the 9/11 Commission Report, Congress and the Executive Branch worked quickly to implement various commission recommendations to safeguard the United States against future terror attacks. Across the federal government, a homeland security enterprise was developed to consistently stay ahead of our adversaries, support state and local partners, and develop emerging technologies and methods to counter future threats.

We are now approaching the 25th anniversary of 9/11. While the United States has undertaken monumental efforts to strengthen national security, this mission will always remain unfinished, and we must continually assess the nation's ability to disrupt and mitigate threats to the homeland.

Throughout the 119th Congress, the Committee on Homeland Security has worked diligently to assess the current state of U.S. national security and identify areas of improvement to keep pace with a twenty-first century threat environment. This assessment has centered around both unfulfilled 9/11 Commission recommendations and policies concerning new and emerging threats, such as cybersecurity and artificial intelligence, which were not truly contemplated as possible attack vectors in the early 2000s.

As the only House Committee specifically created in response to September 11th, the Homeland Security Committee is uniquely situated to conduct broad oversight of the nation's homeland security enterprise in the post-9/11 era and analyze the entire threat landscape, whether those threats are related to counterterrorism, border and maritime security, cybersecurity, or emergency management.

In keeping with the mandate to prevent and deter future domestic terror attacks, this report provides a comprehensive assessment of the United States' domestic threat landscape and assesses improvements made to the country's national security posture over the last twenty-five years. It also provides several recommendations and policy proposals aimed at remedying identified deficiencies and keeping pace with emerging threats. The Committee has endeavored to accomplish this report in honor of all those lost on September 11, 2001, and in the years following, whose sacrifices will never be forgotten, and in furtherance of the work first accomplished by the National Commission on Terrorist Attacks Upon the United States, without which this work would not have been possible and to whom we owe a great debt.

The House Committee on Homeland Security remains steadfast in its objective to protect the American people against threats to the United States and will continue to pursue this mission with all the commitment, dedication, and reverence it so greatly deserves.

Andrew R. Garbarino
Chairman

Executive Summary

The attacks of September 11, 2001, forever changed the national security posture of the United States. In the matter of a few hours, glaring shortfalls in intelligence gathering, information sharing, and threat assessment were brought to the forefront of American life as the horrific events of the day unfolded.

In the wake of September 11, 2001, the federal government established the National Commission on Terrorist Attacks Upon the United States (the "Commission").[1] The Commission's purpose was to examine the "facts and causes relating to the terrorist attacks of September 11, 2001," create a full accounting of the "circumstances surrounding the attacks, and the extent of the United States' preparedness for, and immediate response to, the attacks" and "investigate and report to the President and Congress on its findings, conclusions, and recommendations for corrective measures that can be taken to prevent acts of terrorism."[2]

The Commission's work culminated in the publicly released "9/11 Commission Report" on July 22, 2004, and the Commission closed the following month on August 21, 2004.[3] The final report included forty-one recommendations for Congress and the President spanning a variety of topics, including the Intelligence Community (IC), law enforcement, border security, screening and vetting, countering terrorism, and congressional oversight mechanisms and funding allocations.[4] Following the release of the Commission's final report, Congress and the Executive Branch worked to implement these recommendations via statutory changes and Executive Orders.[5] Since then, various measures have been enacted aimed at strengthening U.S. national security in accordance with the vulnerabilities and recommendations identified by the Commission.

Never before or since has the United States been faced with such a catastrophic terror attack on U.S. soil. The security successes we have had are due in large part to the tireless work of the IC, coordination between various Cabinet-level departments and federal, state, local, tribal, and territorial law enforcement, and increased vigilance by the American people writ large to disrupt and deter these attacks.

Despite successes in defending the American homeland, national security threats continue to evolve as the threat landscape becomes increasingly sophisticated. As a result, the processes, methods, and resources needed to defend the homeland must continue to keep pace with the dangers of today's national security environment.

As the nation approaches the 25th anniversary of the attacks of September 11, 2001, this report provides the U.S. House of Representatives Committee on Homeland Security majority's (the "Committee") assessment of the progress made over the last twenty-five years to improve homeland security and ensure our nation can effectively identify and prevent threats to the United States. Particular emphasis is placed on how the domestic threat landscape has changed since 2001 and what additional efforts must be undertaken to stay ahead of these evolving threats.

This analysis is provided in the context of the Commission's original 41 recommendations, with assessments regarding which recommendations remain unfulfilled, the Committee's work to address those still outstanding, and legislative and policy proposals intended to mitigate identified vulnerabilities.

This report reflects on the "failure of imagination" that culminated in the attacks of September 11, 2001, in the context of a twenty-first century threat environment. Such considerations in the modern day include evolutions in terrorist activity, rising violent extremism, the emergence of cybersecurity and artificial intelligence (AI) as attack vectors for private and public networks and critical infrastructure, and contemporary considerations for the screening and vetting of foreign nationals.

In conducting this assessment, the Committee has identified various ongoing national security challenges and provided recommendations to further secure the United States against the threats of today. Such recommendations include addressing a resurgence in intelligence siloing and ensuring threat intelligence is shared with state and local law enforcement partners in a timely, efficient, and digestible manner; managing contemporary national security challenges linked to the evolution of malign uses of cyber and artificial intelligence capabilities through greater public-private coordination while not impeding innovation and competition; providing increased resources for the modernization of TSA screening technology and practices to maintain rigorous security standards while simultaneously improving the traveler experience; and ensuring stability in annual federal grant and programmatic funding allocations.

These recommendations will require close coordination between the Legislative and Executive Branches, as well as the private sector, to ensure the United States can effectively keep pace with emerging threats while encouraging the innovations that have been essential to the nation's ability to outflank malign actors, adversarial nations, and organized terrorist and criminal networks.

As the global threat environment becomes increasingly dynamic, this report aims to provide critical insight into future policy and oversight efforts to address identified deficiencies in the United States' national security posture. Moving forward, the Committee will continue to pursue implementation of these recommendations consistent with the Committee's mandate to advance legislation and conduct oversight related to the security of the United States.

BACKGROUND

Background

Attacks of 9/11/01

The attacks of September 11, 2001, were the culmination of a multi-year effort to exploit U.S. national security and inflict maximum damage upon the United States. Such planning began as early as 1999, when Osama Bin Laden met with conspirators in Afghanistan to discuss the weaponization of commercial aircraft and identify potential targets for an attack utilizing this method.[6] In April of 1999, hijackers began obtaining visas to enter the United States, and many started preparing for the attack while living in Germany.[7] Throughout 2001, the 9/11 hijackers enrolled in flight schools and engaged in surveillance of cross-country flights to determine which aircraft would be most ideal for carrying out the terror plot.[8]

While in the United States, several hijackers were cited for traffic violations, but no terrorism-related indications were observed by law enforcement.[9] On the morning of September 11th, the hijackers underwent security screening at Portland International Jetport in Maine, Boston Logan International Airport in Massachusetts, Washington Dulles International Airport in Virginia, and Newark Liberty International Airport in New Jersey.[10] The hijackers were believed to be carrying knives, box cutters, and concealed weapons on their persons and carry-on luggage.[11] While eight hijackers were selected for random security screening and two were flagged as suspicious, none of the hijackers were prevented from boarding their respective flights.[12]

The attack unfolded as follows:[13]

5:45 AM: 2 hijackers undergo security screening at Portland International Jetport bound for Boston Logan Airport, where they are joined by three other hijackers before boarding American Airlines Flight 11. Less than two hours after, five additional hijackers underwent screening at Washington Dulles International Airport before boarding American Airlines Flight 77.

7:59 AM: American Airlines Flight 11 departs from Boston Logan International Airport with eleven crew members, seventy-six passengers, and five hijackers on board.

8:15 AM: United Airlines Flight 175 departs from Boston Logan International Airport with nine crew members, fifty-one passengers, and five hijackers on board.

8:19 AM: Crew members aboard American Airlines Flight 11 notify ground personnel that there is a hijacking underway.

8:20 AM: American Airlines Flight 77 departs Washington Dulles International Airport with six crew members, fifty-three passengers, and five hijackers on board.

8:24 AM: Hijackers aboard American Airlines Flight 11 inadvertently transmit the following message to air traffic control instead of over the on-board PA system: “We have some planes. Just stay quiet, and you will be okay.”

8:30 AM: Employees begin to populate the World Trade Center.

8:37 AM: Boston air traffic control center alerts the U.S. Air Force Northeast Air Defense Sector (NEADS) following the hijackers’ inadvertent transmission. Air National Guard Jets at Otis Air Force based are mobilized to identify and track American Airlines Flight 11.

8:42 AM: United Airlines Flight 93 departs from Newark International Airport with seven crew members, thirty-three passengers, and four hijackers.

8:46 AM: American Airlines Flight 11 strikes the North Tower of the World Trade Center. First responders mobilize to begin rescue efforts.

8:50 AM: President George W. Bush is alerted that a small plane has hit the North Tower. At this point, the crash is assumed to have been an accident.

8:52 AM: Crew aboard United Airlines Flight 175 notifies a United Airlines operator in San Francisco, California, that there has been a hijacking.

8:55 AM: Port Authority declares that the South Tower of the World Trade Center is secure.

8:59 AM: Port Authority Police order the evacuation of the North and South Towers.

9:02 AM: An evacuation order is broadcast in the South Tower.

9:03 AM: United Airlines Flight 175 strikes the South Tower of the World Trade Center. Additional first responders are mobilized to respond to the World Trade Center, and a request is made to shut down the airspace over New York City.

9:05 AM: President Bush is informed that a second plane has crashed into the World Trade Center.

9:12 AM: Crew and passengers aboard American Airlines Flight 77 notify family members that the plane has been hijacked.

9:36 AM: Vice President Dick Cheney is evacuated to the Presidential Emergency Operations Center.

9:37 AM: American Airlines Flight 77 strikes the Pentagon.

9:42 AM: The Federal Aviation Administration grounds all flights.

9:45 AM: The White House and U.S. Capitol begin evacuations.

9:58 AM: Passengers begin making calls from United Airlines flight 93, including a call placed to 9-1-1.

9:59 AM: The South Tower of the World Trade Center collapses.

9:59 AM: Federal continuity of government procedures are activated.

10:03 AM: United Airlines Flight 93 crashes in a field near Shanksville, Pennsylvania, after passengers and crew members storm the cockpit.

10:15 AM: The Pentagon E Ring collapses.

10:28 AM: The North Tower of the World Trade Center collapses.

11:02 AM: New York City Mayor orders the evacuation of lower Manhattan.

12:16 PM: U.S. airspace is closed.

Rescue and recovery efforts continued throughout the day and beyond. At 5:20 PM, World Trade Center building 7 collapses.[14] By the day's end, the attacks claimed the lives of 2,977 people: 2,753 at the World Trade Center, 184 at the Pentagon, and forty outside Shanksville, Pennsylvania.[15] At the World Trade Center, those killed included 343 firefighters and paramedics, twenty-three NYPD police officers, and thirty-seven Port Authority police officers.[16]

After facing the largest attack on domestic soil in U.S. history, the country was then confronted with the enormous task of determining how this attack occurred, and what needed to be done to close the national security vulnerabilities that allowed such an attack to take place. In the days, months, and years that follow, a myriad of efforts are undertaken by the United States to strengthen national security and protect the American public.

Response, Recovery, and Resiliency

September 11, 2001, was not the first time New York City or the World Trade Center (WTC) were the subject of a terrorist attack. On February 26, 1993, terrorist perpetrators detonated a 1,500-pound bomb beneath the WTC, killing six and injuring approximately 1,000 people.[17] This incident had previously tested the city's response and rescue capacity, including the New York City Fire Department's (FDNY) communications capabilities.[18]

Though this incident led to investments in certain security and technological capabilities within the WTC,[19] first responders still found themselves hampered by insufficient communications capabilities[20] and the lack of a coordinated incident command and control structure during the September 11th attacks.[21]

Despite these challenges, first responders reacted to the initial aircraft attack on September 11th swiftly, with thousands of emergency services personnel from FDNY, the New York City Police Department (NYPD), and the Port Authority of New York and New Jersey Police Department (PAPD) working immediately to rescue and evacuate civilians, representing the largest emergency response mobilization in city history.[22] The New York City Mayor's Office of Emergency Management (OEM) also requested assistance from the Federal Emergency Management Agency (FEMA), which activated its National Urban Search and Rescue Response System to deploy urban search and rescue (US&R) task forces to New York to search for victims impacted by the attacks.[23]

Ultimately, September 11th resulted in the largest loss of life from a foreign attack on American soil in history, claiming 2,977 lives.[24] This tragedy also exacted a heavy toll on New York first responder agencies: FDNY suffered 343 fatalities, the largest loss of life of any emergency response agency in history, and thirty-seven PAPD officers and twenty-three NYPD officers were also killed in the attacks.[25] However, despite the complexity of the incident and various factors inhibiting first responder operations, the mission to rescue and evacuate civilians was ultimately successful for many of those on floors below the impact zones of the towers.[26]

Following the attacks of September 11, 2001, the United States worked expeditiously to strengthen national security and expand the nation's homeland security enterprise. Eleven days after the attacks, President Bush appointed Pennsylvania Governor Tom Ridge as the White House's first Director of the newly created Office of Homeland Security.[27] This office was tasked with the oversight and coordination of "a comprehensive national strategy to safeguard the United States against terrorism and respond to any future attacks."[28]

In an effort to address the numerous aviation security vulnerabilities that contributed to the execution of the 9/11 terror plot, Congress passed the *Aviation and Transportation Security Act*,[29] which established the Transportation Security Administration (TSA).[30] Prior to the creation of TSA, aviation security existed as a joint effort between the Federal Aviation Administration (FAA) and the airlines, who contracted with private security companies to manage passenger and baggage screening. This system was unsuccessful in preventing any of the nineteen hijackers from boarding their flights on September 11, 2001. With the creation of TSA, the United States had for the first time established a federal entity tasked with the safety of the nation's transportation systems, moving away from a disjointed system of aviation security that lacked the necessary coordination and standards to ensure the safety of the traveling public.

In June 2002, President Bush proposed the creation of the Department of Homeland Security, finding that "no single government agency has homeland security as its primary mission" and that the United States "needs a single, unified homeland security structure that will improve protection against today's threats and be flexible enough to help meet unknown threats of the future."[31] In November 2002, Congress passed the *Homeland Security Act of 2002*, establishing the Department of Homeland Security (DHS) as a Cabinet-level department to coordinate and unify domestic national security efforts.[32]

DHS was created by combining all or part of twenty-two distinct departments and agencies into one unified entity.[33] Since its inception, DHS has served as the primary federal department charged with the protection of the American homeland. President Bush's original proposal for the Department recommended an organizational structure comprised of four divisions: Border and Transportation Security; Emergency Preparedness and Response; Chemical, Biological, Radiological, and Nuclear Countermeasures; and Information Analysis and Infrastructure Protection.[34] In the modern day, the Department's mission set includes counterterrorism, intelligence, transportation and maritime security, border security and immigration enforcement, cybersecurity and infrastructure protection, emergency management and preparedness, developments in science and technology, and coordination with state, local, tribal, and territorial law enforcement.[35]

Post-9/11 security reforms also took hold at the state and local level. Following the attacks of September 11, 2001, the NYPD established a Counterterrorism Bureau focused on monitoring possible terrorist targets and developing "innovative, forward-thinking policies and procedures to guard against attacks, training first responders and specialized units and developing intelligence capabilities for detecting and preventing terrorist attacks."[36] The NYPD Counterterrorism Bureau continues to serve as a model to law enforcement organizations around the world for how to detect, prevent, and mitigate terrorism threats in dynamic threat environments.

Since 9/11, law enforcement agencies across the United States have continued to establish and modernize counterterrorism missions in coordination with the federal government. These efforts are supplemented by the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Forces (JTTFs) which share information and intelligence across the task forces and with state and local agencies,[37] as well as the DHS Office of Intelligence and Analysis (I&A), which is the only element of the IC statutorily required to share intelligence with state, local, tribal, territorial, and private sector partners.[38]

Following the creation of the National Commission on Terrorist Attacks Upon the United States in the 107th Congress, the House later established the Select Committee on Homeland Security in the 108th Congress.[39] The House Rules for the 108th Congress granted the select committee jurisdiction over matters concerning the *Homeland Security Act of 2002*, jurisdiction over DHS, and the requirement that the select committee "conduct a thorough and complete study of the operation and implementation of the rules of the House, including Rule X, with respect to the issue of homeland security" and submit recommended changes to the Rules Committee by September 30, 2004.[40]

The Committee was then made a permanent standing committee of the House beginning in the 109th Congress.[41] As of the 119th Congress, the Committee's jurisdiction encompasses "overall homeland security policy; organization, administration, and general management of the

Department of Homeland Security"; and functions of the Department of Homeland Security relating to "border and port security (except immigration policy and non-border enforcement); customs (except customs revenue); integration, analysis, and dissemination of homeland security information; domestic preparedness for and collective response to terrorism; research and development; transportation security"; and "cybersecurity."[42] The Committee's grant of oversight and legislative jurisdiction over these matters continues to serve as an essential mechanism for congressional action on domestic security policy. As the only House committee expressly created in response to the attacks of September 11th, the Committee's role in strengthening U.S. national security is uniquely informed by the history of its creation and the solemn responsibility of preventing future attacks of such scale and devastation on domestic soil.

Efforts to address the national security shortfalls exposed by the attacks of September 11, 2001, were further informed by the forty-one recommendations of the National Commission on Terrorist Attacks Upon the United States released in July 2004. Various commission recommendations have since been enacted via statute and Executive action, as discussed in Section III(d): *Implementation of the Recommendations of the 9/11 Commission: Legislative History.*

9/11 Commission Recommendations

After the establishment of the National Commission on Terrorist Attacks Upon the United States, the Commission released its report on the attacks of September 11, 2001, on July 22, 2004.[43] Included in the final report were forty-one recommendations aimed at strengthening the United States' ability to prevent future attacks. While the full list of forty-one recommendations is included below as a reminder of the Commission's critical work and foresight, the Committee has endeavored in subsequent sections of this report to focus primarily on those recommendations most relevant today to the Committee's purpose and jurisdiction.

1. The U.S. Government must identify and prioritize actual or potential terrorist sanctuaries. For each, it should have a realistic strategy to keep possible terrorists insecure and, on the run, using all elements of national power. We should reach out, listen to, and work with other countries that can help.[44]

2. If Musharraf stands for enlightened moderation in a fight for his life and for the life of his country, the United States should be willing to make hard choices too and make the difficult long-term commitment to the future of Pakistan. Sustaining the current scale of aid to Pakistan, the United States should support Pakistan's government in its struggle against extremists with a comprehensive effort that extends from military aid to support for better education, so long as Pakistan's leaders remain willing to make difficult choices of their own.[45]

3. The President and the Congress deserve praise for their efforts in Afghanistan so far. Now the United States and the international community should make a long-term commitment to a secure and stable Afghanistan, in order to give the government a reasonable opportunity to improve the life of the Afghan people. Afghanistan must not again become a sanctuary for international crime and terrorism. The United States and the international community should help the Afghan government extend its authority over the country, with a strategy and nation-by-nation commitments to achieve their objectives.[46]

4. The problems in the U.S.-Saudi relationship must be confronted, openly. The United States and Saudi Arabia must determine if they can build a relationship that political leaders on both sides are prepared to publicly defend – a relationship about more than oil. It should include a shared commitment to political and economic reform, as Saudis make common cause with the outside world. It should include a shared interest in greater tolerance and cultural respect, translating into a commitment to fight the violent extremists who foment hatred.[47]

5. The U.S. government must define what the message is, what it stands for. We should offer an example of moral leadership in the world, committed to treat people humanely, abide by the rule of law, and be generous and caring to our neighbors. America and Muslim friends can agree on respect for human dignity and opportunity. To Muslim parents, terrorists like Bin Ladin have nothing to offer their children but visions of violence and death. America and its friends have a crucial advantage – we can offer these parents a vision that might give their children a better future. If we heed the views of

thoughtful leaders in the Arab and Muslim world, a moderate consensus can be found.[48]

6. Where Muslim governments, even those who are friends, do not respect these principles, the United States must stand for a better future. One of the lessons of the long Cold War was that short-term gains in cooperating with the most repressive and brutal governments were too often outweighed by long-term setbacks for America's stature and interests.[49]

7. Just as we did in the Cold War, we need to defend our ideals abroad vigorously. America does stand up for its values. The United States defended, and still defends, Muslims against tyrants and criminals in Somalia, Bosnia, Kosovo, Afghanistan, and Iraq. If the United States does not act aggressively to define itself in the Islamic world, the extremists will gladly do the job for us.

    a. Recognizing that Arab and Muslim audiences rely on satellite television and radio, the government has begun some promising initiatives in television and radio broadcasting to the Arab world, Iran, and Afghanistan. These efforts are beginning to reach large audiences. The Broadcasting Board of Governors has asked for much larger resources. It should get them.[50]

    b. The United States should rebuild the scholarship, exchange, and library programs that reach out to young people and offer them knowledge and hope. Where such assistance is provided, it should be identified as coming from the citizens of the United States.[51]

8. The U.S. government should offer to join with other nations in generously supporting a new International Youth Opportunity Fund. Funds will be spent directly for building and operating primary and secondary schools in those Muslim states that commit to sensibly investing their own money in public education.[52]

9. A comprehensive U.S. strategy to counter terrorism should include economic policies that encourage development, more open societies, and opportunities for people to improve the lives of their families and to enhance prospects for their children's future.[53]

10. The United States should engage other nations in developing a comprehensive coalition strategy against Islamist terrorism. There are several multilateral institutions in which such issues should be addressed. But the most important policies should be discussed and coordinated in a flexible contact group of leading coalition governments. This is a good place, for example, to develop joint strategies for targeting terrorist travel, or for hammering out a common strategy for the places where terrorists may be finding sanctuary.[54]

11. The United States should engage its friends to develop a common coalition approach toward the detention and humane treatment of captured terrorists. New principles might draw upon Article 3 of the Geneva Conventions on the law of armed conflict. That article was specifically designed for those cases in which the usual laws of war did not apply. Its minimum standards are generally accepted throughout the world as customary

international law.[55]

12. Our report shows that Al Qaeda has tried to acquire or make weapons of mass destruction for at least ten years. There is no doubt the United States would be a prime target. Preventing the proliferation of these weapons warrants a maximum effort by strengthening counterproliferation efforts, expanding the Proliferation Security Initiative, and supporting the Cooperative Threat Reduction program.[56]

13. Vigorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us to understand their networks, search them out, and disrupt their operations. Intelligence and law enforcement have targeted the relatively small number of financial facilitators – individuals Al Qaeda relied on for their ability to raise and deliver money – at the core of Al Qaeda's revenue stream. These efforts have worked. The death or capture of several important facilitators has decreased the amount of money available to Al Qaeda and has increased its costs and difficulty in raising and moving that money. Captures have additionally provided a windfall of intelligence that can be used to continue the cycle of disruption.[57]

14. Targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.[58]

15. The U.S. border security system should be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with system wide goals in mind. Extending those standards among other governments could dramatically strengthen America and the world's collective ability to intercept individuals who pose catastrophic threats.[59]

16. The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers. It should be integrated with the system that provides benefits to foreigners seeking to stay in the United States. Linking biometric passports to good data systems and decision making is a fundamental goal. No one can hide his or her debt by acquiring a credit card with a slightly different name. Yet today, a terrorist can defeat the link to electronic records by tossing away an old passport and slightly altering the name in the new one.[60]

17. The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies and raise U.S. and global border security standards for travel and border crossing over the medium and long

term through extensive international cooperation.[61]

18. Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.[62]

19. Hard choices must be made in allocating limited resources. The U.S. Government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort. The plan should assign roles and missions to the relevant authorities (federal, state, regional, and local) and to private stakeholders. In measuring effectiveness, perfection is unattainable. But terrorists should perceive that potential targets are defended. They may be deterred by a significant chance of failure.[63]

20. Improved use of "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by the TSA, and it should utilize the larger set of watchlists maintained by the federal government. Air carriers should be required to supply the information needed to test and implement this new system.[64]

21. The TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. As a start, each individual selected for special screening should be screened for explosives. Further, the TSA should conduct a human factors study, a method often used in the private sector, to understand problems in screener performance and set attainable objectives for individual screeners and for the checkpoints where screening takes place.[65]

22. As the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared.[66]

23. The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use.[67]

24. At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties.[68]

25. Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities. Now, in 2004, Washington, D.C., and New York City are certainly at the top of any such list. We understand the contention that every state and city needs to have some minimum infrastructure for emergency response. But federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support. Congress should not use this money as a pork barrel.[69]

26. Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven frameworks for emergency response. We strongly support the decision that federal homeland security funding will be contingent, as of October 1, 2004, upon the adoption and regular use of ICS and unified command procedures. In the future, the Department of Homeland Security should consider making funding contingent on aggressive and realistic training in accordance with ICS and unified command procedures.[70]

27. Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress.[71]

28. We endorse the American National Standards Institute's recommended standard for private preparedness. We were encouraged by Secretary Tom Ridge's praise of the standard and urge the Department of Homeland Security to promote its adoption. We also encourage the insurance and credit-rating industries to look closely at a company's compliance with the ANSI standard in assessing its insurability and creditworthiness. We believe that compliance with the standard should define the standard of care owed by a company to its employees and the public for legal purposes. Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security.[72]

29. We recommend the establishment of a National Counterterrorism Center (NCTC), built on the foundation of the existing Terrorist Threat Integration Center (TTIC). Breaking the old mold of national government organization, this NCTC should be a center for joint operational planning and joint intelligence, staffed by personnel from the various agencies. The head of the NCTC should have authority to evaluate the performance of the people assigned to the Center.[73]

30. The current position of Director of Central Intelligence should be replaced by a National Intelligence Director with two main areas of responsibility: (1) to oversee national intelligence centers on specific subjects of interest across the U.S. Government and (2) to manage the national intelligence program and oversee the agencies that contribute to it.[74]

31. The CIA Director should emphasize (a) rebuilding the CIA's analytic capabilities; (b) transforming the clandestine service by building its human intelligence capabilities; (c) developing a stronger language program, with high standards and sufficient financial incentives; (d) renewing emphasis on recruiting diversity among operations officers so they can blend more easily in foreign cities; (e) ensuring a seamless relationship between human source collection and signals collection at the operational level; and (f) stressing a better balance between unilateral and liaison operations.[75]

32. Lead responsibility for directing and executing paramilitary operations, whether clandestine or covert, should shift to the Defense Department. There it should be consolidated with the capabilities for training, direction, and execution of such operations already being developed in the Special Operations Command.[76]

33. Finally, to combat the secrecy and complexity we have described, the overall amounts of money being appropriated for national intelligence and to its component agencies should no longer be kept secret. Congress should pass a separate appropriations act for intelligence, defending the broad allocation of how these tens of billions of dollars have been assigned among the varieties of intelligence work.[77]

34. Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge.[78]

35. The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a "trusted information network."[79]

36. Congressional oversight for intelligence and counterterrorism is now dysfunctional. Congress should address this problem. We have considered various alternatives: A joint committee on the old model of the Joint Committee on Atomic Energy is one. A single committee in each house of Congress, combining authorizing and appropriating authorities, is another.[80]

37. Congress should create a single, principal point of oversight and review for homeland security. Congressional leaders are best able to judge what committee should have jurisdiction over this department and its duties. But we believe that Congress does have the obligation to choose one in the House and one in the Senate, and that this committee should be a permanent standing committee with a nonpartisan staff.[81]

38. Since a catastrophic attack could occur with little or no notice, we should minimize as much as possible the disruption of national security policymaking during the change of administrations by accelerating the process for national security appointments. We think the process could be improved significantly so transitions can work more effectively and allow new officials to assume their new responsibilities as quickly as possible.[82]

39. A specialized and integrated national security workforce should be established at the FBI consisting of agents, analysts, linguists, and surveillance specialists who are recruited, trained, rewarded, and retained to ensure the development of an institutional culture imbued with a deep expertise in intelligence and national security.[83]

40. The Department of Defense and its oversight committees should regularly assess the adequacy of Northern Command's strategies and planning to defend the United States against military threats to the homeland.[84]

41. The Department of Homeland Security and its oversight committees should regularly assess the types of threats the country faces to determine (a) the adequacy of the government's plans – and the progress against those plans – to protect America's critical infrastructure and (b) the readiness of the government to respond to the threats that the United States might face.[85]

These recommendations provided the basis for various federal efforts aimed at improving domestic security in the aftermath of 9/11, such as the *Implementing Recommendations of the 9/11 Commission Act of 2007.* A brief history of legislative reforms enacted in response to these recommendations are discussed further in the next section.

Implementation of the Recommendations of the 9/11 Commission: Legislative History

After the publication of the 9/11 Commission Report in July 2004, Congress and the Executive Branch worked to implement the recommendations included therein over the next several succeeding Congresses. While federal action concerning the implementation of the recommendations has not been all-inclusive, the following Executive Orders and legislation show continued progress toward strengthening homeland security.

Moving forward, Congress must diligently address the Commission's outstanding recommendations that remain relevant today, as well as ensure current national security capabilities and priorities align with a twenty-first century threat environment. Threats concerning drones, cybersecurity, and artificial intelligence exemplify the need for a dynamic security framework, as homeland security implications of these continually developing attack vectors were not originally contemplated by the Commission in the early 2000s when much of this technology was in its infancy. Specific recommendations and policy considerations to address unfulfilled Commission recommendations in the context of the modern threat environment are discussed further in Section IV: *25 Years Later: Challenges and Recommendations*.

Prior to the release of the 9/11 Commission Report, then-House Majority Leader Richard K. Armey (R-TX) introduced the *Homeland Security Act of 2002* (HSA) in June 2002.[86] Deliberations on the bill included the question of whether the Federal Bureau of Investigation and the Central Intelligence Agency belonged inside the new Department; neither was included in the enacted text.[87] Congress passed the HSA in November 2002, consolidating all or part of twenty-two different federal departments and agencies into a unified Department.[88] Among its provisions, the Act created the Directorate for Information Analysis and Infrastructure Protection (IAIP) as the Department's principal intelligence element, tasked with analyzing threat information and protecting the nation's critical infrastructure.

The Department of Homeland Security (DHS) was established as a Cabinet-level department on January 24, 2003, with the transfer of its component agencies completed on March 1, 2003. That consolidation redistributed longstanding functions across the federal government. The United States Secret Service transferred to DHS from the Department of the Treasury, and the United States Coast Guard from the Department of Transportation. The Immigration and Naturalization Service (INS), until then a component of the Department of Justice, was dissolved, and its duties were divided among three newly created entities within DHS: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS). The United States Customs Service left the Treasury Department, its responsibilities split between CBP and ICE.[89]

Reforms to the federal government's counterterrorism structure also proceeded through Executive action. Announced by President George W. Bush in his January 2003 State of the Union Address, the Terrorist Threat Integration Center (TTIC) began operations on May 1, 2003, charged with integrating and analyzing terrorist threat-related information collected at home and abroad.[90] On February 6, 2004, President Bush signed Executive Order 13328, establishing the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass

Destruction (WMD Commission) and directing it to compare pre-war Iraq intelligence against the findings of the Iraq Survey Group.[91]

Following the release of the 9/11 Commission Report in July 2004, on August 27, 2004, the President signed Executive Order 13354 establishing the National Counterterrorism Center (NCTC), which absorbed TTIC's functions and assumed additional responsibilities, including strategic operational planning for counterterrorism.[92]

The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) was passed by Congress and enacted on December 17, 2004, restructuring the leadership of the Intelligence Community (IC).[93] The Act eliminated the position of Director of Central Intelligence (DCI) and designed a new Director of National Intelligence (DNI) position for managing the IC and serving as the President's principal intelligence advisor. Section 1011(a) of the Act established the Office of the Director of National Intelligence (ODNI), a statutory element of the IC designed to give the DNI a dedicated staff for integrating and managing the IC. Section 1021 codified the NCTC, designating the Center as the primary organization within the United States government for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, other than intelligence pertaining exclusively to domestic terrorism and domestic counterterrorism; the Center does not, however, direct the execution of counterterrorism operations. Section 1022 established the National Counter Proliferation Center (NCPC) within ODNI to manage the collection and analysis of nuclear, biological, and chemical weapons intelligence.

In July 2005, then-DHS Secretary Michael Chertoff established a new Office of Intelligence and Analysis (I&A) led by the Department's Chief Intelligence Officer, tasked with fusing intelligence internally, serving as the primary DHS link to the broader IC, and acting as a main source of information for state, local, and private sector partners.[94]

Congressional efforts to implement the Commission's recommendations continued in the 110th Congress. Introduced as H.R. 1 by then-Chairman of the House Committee on Homeland Security and current Ranking Member Bennie G. Thompson (D-MS), and enacted on August 3, 2007, the *Implementing Recommendations of the 9/11 Commission Act of 2007* addressed recommendations the Commission had called for relating to homeland security assistance, emergency preparedness, transportation security, terrorist travel, civil liberties oversight, intelligence transparency, nonproliferation, and foreign policy.[95]

Several provisions of the Act were focused on information sharing with non-federal partners. Section 504 expanded the scope of the Information Sharing Environment established under Section 1016 of the IRTPA, responding to the Commission's recommendation for a decentralized, network-based approach to information sharing. Section 511 created the Department of Homeland Security State, Local, and Regional Fusion Center Initiative, providing for the deployment of departmental intelligence officers to state-run centers and authorizing grant funding to staff them with qualified analysts. Section 521 established the Interagency Threat Assessment and Coordination Group to produce federally coordinated intelligence for dissemination to state, local, tribal, and territorial (SLTT) partners. Section 531 reorganized the Department's intelligence functions and formally established I&A, making it the first federal entity statutorily mandated to share information with state and local partners.

Additional provisions of the Act carried out Commission recommendations on terrorist travel and intelligence transparency. Section 711 modernized the Visa Waiver Program, Section 721 strengthened the Human Smuggling and Trafficking Center, and Section 722 expanded the government's dedicated terrorist travel program under Section 7215 of the IRTPA.

Section 601 required public disclosure of the aggregate amount of funds appropriated for the National Intelligence Program, implementing the Commission's recommendation that overall intelligence spending no longer be kept secret. Pursuant to 50 U.S.C. § 3306, the President discloses the aggregate amount requested and the DNI discloses the aggregate amount appropriated, subject to a presidential waiver or postponement where disclosure would damage national security.[96]

The NCPC's mission later expanded during the COVID-19 pandemic, as Congress enacted Section 401 of the *Intelligence Authorization Act for Fiscal Year 2022*, amending Section 119A of the *National Security Act of 1947* to rename the NCPC as the National Counterproliferation and Biosecurity Center (NCBC) and expand the Center's authorities to include management of intelligence on foreign diseases with pandemic potential.[97]

Despite all the progress made, certain Commission recommendations remain unfulfilled. For example, the Commission concluded that congressional oversight for intelligence and counterterrorism was dysfunctional and urged Congress either to establish a joint committee on the model of the Joint Committee on Atomic Energy, or to combine authorizing and appropriating authorities within a single committee in each chamber, supported by a completely nonpartisan staff.

The Commission further recommended that the Department of Homeland Security, properly supported by Congress, complete a Biometric Entry/Exit (BE/E) screening system as quickly as possible, integrated with the systems governing benefits for foreigners seeking to remain in the United States. DHS expanded biometric collection to all foreign travelers at airports, land borders, and seaports in December 2025.[98] While biometric entry capability has been achieved, exit capability has not been developed to the same standard, and the federal government cannot use biometric capabilities to determine with confidence which aliens have departed the United States and which have overstayed their terms of admission. For recommendations aimed at accomplishing unfulfilled Commission recommendations and strengthening national security in the context of the twenty-first century threat environment, see Section IV(d): *Policy Recommendations.*

25 YEARS LATER: CHALLENGES AND RECOMMENDATIONS

25 Years Later: Challenges and Recommendations

Evolving Threat Landscape: A Failure of Imagination

Threats to homeland security have changed dramatically over the last twenty-five years, requiring innovative approaches to address the evolving threat landscape. While many of the concerns examined by the National Commission on Terrorist Attacks Upon the United States remain at the forefront of contemporary national security policy, the Committee also recognizes that new security vulnerabilities and attack vectors have since developed that were not originally contemplated in the early 2000s.

The national security community often cites the immense role that a "failure of imagination" contributed to the vulnerabilities exploited on 9/11, requiring a more dynamic approach to homeland security than had been considered prior to 2001. With these considerations in mind, the Committee's assessment of ongoing challenges and policy recommendations is informed not only by the original recommendations of the 9/11 Commission Report, but also the current national security environment and how threats evolved over the last twenty-five years. Specifically, the Committee has identified various developments concerning terrorist activity, transnational criminal organizations, and violent extremism, the emergence of cyber and artificial intelligence as attack vectors, border security, and the screening and vetting of foreign nationals and goods at U.S. ports of entry that require consideration for homeland security practitioners.

Terrorism and Violent Extremism

The attacks of September 11, 2001, forever changed the world and transformed America's understanding of the threat terrorism posed to the United States. Before 9/11, terrorism was often viewed as a remote and abstract danger that was unlikely to reach American shores. The attacks shattered that perception and made terrorism threats an immediate and undeniable reality.

In the years that followed, the enemy appeared largely defined and geographically contained. Today, that is no longer the case. The United States faces an increasingly complex and constantly evolving threat environment that includes state-sponsored networks, transnational criminal organizations, ideological extremists, and individuals radicalized in isolation. The legacy of 9/11 extends beyond the lives lost and the nation's enduring grief. It also serves as a reminder that the threats confronting the United States have become more diverse, adaptive, and interconnected than at any other point in modern history. Meeting these challenges requires constant vigilance and an approach to national security that evolves as rapidly as the threats themselves.

This transformation is visible first in the geographic spread of terrorism. The story of terrorism today is one of both expansion and concentration. While more countries experienced at least one terrorist incident in 2024 than in any year since 2018, 86 percent of all terrorism-related deaths occurred in just 10 countries.[99] Seven of those countries are located in Africa, with five concentrated in the Sahel.[100] In short, while terrorist groups have found consistently favorable conditions in the Sahel to engage in terrorism, certain networks remain capable of conducting devastating attacks far beyond the region.[101] This geographic shift carries implications for homeland security, as extremist networks operating in Africa increasingly exploit known

migration routes, smuggling pipelines, and online platforms to project influence and inspire attacks far beyond the continent.

At the same time, the definition of a "terrorist actor" has expanded dramatically. Nation state adversaries such as Iran have become increasingly hybridized.[102] In recent years, Iran has conducted numerous foreign operations involving both criminal and terrorist proxies, demonstrating how state actors increasingly blend criminality, terrorism, and covert influence.[103]

Transnational criminal organizations have also entered the terrorism landscape. In January 2025, President Trump's decision to designate several violent cartels as foreign terrorist organizations (FTOs) allowed the NCTC to expand its mission to include both terrorism and certain transnational crime.[104] Within the first month of this designation, the NCTC reportedly added more than 21,000 cartel members and associates to the classified terrorist database.[105] Since then, it has created over 35,000 identity records for the 10 newly designated FTOs, helping law enforcement prevent more than 6,525 suspected terrorists from entering the United States.[106] As a result of the new designations, the ODNI expanded the Intelligence Community's counterterrorism mission to encompass counternarcotics, formally recognizing cartels and gangs as top-tier threats and streamlining vetting operations to strengthen national security.[107]

The diversification of threat actors includes the United States' decision to designate several Latin American cartels and criminal organizations, as well as European ANTIFA-linked groups, as FTOs, further widening the geographic aperture of terror threats to the United States to include Mexico, Venezuela, Ecuador, Haiti, Germany, Greece, and Italy.[108] These designations reflect a growing recognition that the current terrorism environment is no longer confined to a single region or ideology.

Nowhere is this geographic shift more evident than in Africa. The terrorism picture in recent years has been particularly concerning, as both the Islamic State (ISIS) and Al Qaeda (AQ) have continued to expand their influence across the continent. According to Armed Conflict Location & Event Data (ACLED), more than two-thirds of ISIS's global activity during the first half of 2025 occurred in Africa.[109] Likewise, the Global Terrorism Index reported that ISIS and its affiliates were responsible for 1,805 deaths across 22 countries, the largest number of countries affected by ISIS attacks since 2020.[110] This concentration of violence has exposed new intelligence gaps and strained global counterterrorism resources, highlighting the challenges of a counterterrorism posture that has historically centered on the Middle East when addressing a vast African theater characterized by limited intelligence collection opportunities, fragile governments, and uneven information sharing capabilities.[111]

While terrorism has shifted geographically, it has also evolved operationally. The modern threat environment is increasingly decentralized, with attacks often carried out by self-radicalized individuals rather than members of structured terrorist organizations.[112] For years, ISIS has encouraged supporters to conduct attacks wherever they reside, minimizing the need for direct command and control. This trend was illustrated in January 2025 when a 42-year-old American carried out an ISIS-inspired terrorist attack in New Orleans.[113] Less than a month later, two U.S. citizens were arrested for plotting an ISIS-inspired attack in Michigan.[114] At the same time, the number of radicalized young people with no formal affiliation to extremist organizations has increased by over 300 percent over the past decade.[115] Online propaganda,

encrypted communications, and social media have accelerated radicalization while reducing the operational necessity of formal networks.[116]

These operational changes have reshaped the domestic threat landscape. Although ISIS's decentralized model illustrates this evolution, the broader U.S. terrorism environment now encompasses a wide spectrum of ideologically motivated violent extremists. This makes it increasingly important to distinguish between Homegrown Violent Extremists (HVEs)—individuals inspired by foreign terrorist organizations—and Domestic Violent Extremists (DVEs), who are motivated primarily by domestic political, social, or ideological grievances.[117] Although HVEs may commit acts of domestic terrorism, DVEs are not necessarily influenced by foreign actors.[118] Under 18 U.S.C. § 2331(5), domestic terrorism refers to activities that involve acts dangerous to human life that violate federal or state criminal law, appear intended to intimidate or coerce a civilian population, influence government policy through intimidation or coercion, or affect government conduct through mass destruction, assassination, or kidnapping, and occur primarily within the territorial jurisdiction of the United States. Such activity could potentially encompass conduct associated with both homegrown violent extremists (HVEs) and domestic violent extremists (DVEs), depending on the facts and circumstances.[119]

Over the past quarter century, the ideological spectrum driving domestic terrorism has fragmented significantly. Political violence, anti-government extremism, racially and ethnically motivated violent extremism, religiously motivated violence, and nihilistic actors now coexist within the domestic threat environment.[120] It has become increasingly common for perpetrators of terrorism to exhibit what is often referred to as a "salad bar ideology," in which individuals adopt a personalized mix of extremist beliefs rather than adhering to a single, coherent ideology.[121] These actors often combine conspiracy theories, anti-government narratives, racial grievances, accelerationist beliefs, and foreign extremist propaganda into unique ideological frameworks that are difficult to categorize using traditional analytical models.[122] The growing prevalence of hybrid ideological motivations highlights the complexity of today's domestic threat landscape.[123]

This virtual model has fundamentally changed how terrorist organizations project influence. Online propaganda, encrypted communications, and algorithm-driven social media platforms allow extremist content to spread across borders in real time, accelerating radicalization while reducing the barriers to mobilization. Individuals can now consume propaganda, establish connections with like-minded extremists, receive tactical guidance, and plan attacks almost entirely online. As a result, the distinction between foreign and domestic terrorism has become increasingly blurred, with global organizations able to inspire violence inside the United States without ever establishing a physical presence.

The Israel–Hamas conflict that began with Hamas's attack on Israel on October 7, 2023, significantly altered the terrorism threat environment both internationally and within the United States. The conflict has been accompanied by a sharp increase in antisemitic violence, attacks targeting Jewish and pro-Israel communities, and extremist mobilization inspired by events in the Middle East. Although Hamas has suffered substantial military losses since October 2023, the organization remains resilient, sustained by entrenched political and social networks, sophisticated propaganda capabilities, and enduring popular support within Gaza. Likewise, Hezbollah has absorbed significant battlefield losses and faces increasing domestic political pressure in Lebanon, yet it continues to function as a highly capable hybrid military-political

organization supported by Iran. Through its extensive media apparatus, information operations, and remaining military capabilities, Hezbollah continues to influence regional dynamics and inspire extremist narratives. Together, these organizations demonstrate that even when terrorist groups are militarily degraded, they can continue to shape the global threat environment by inspiring ideologically motivated violence, amplifying propaganda, and fueling polarization far beyond the immediate conflict zone.

Collectively, these developments carry significant strategic implications for the United States' ability to counter terrorism. The expansion of the FTO list, the rise of Africa as a jihadist epicenter, the proliferation of lone-actor threats, and the blending of terrorism with cyber capabilities all demand new approaches to prevention, intelligence sharing, and resource allocation.

First, the expansion of the FTO list to including cartels, criminal networks, and ideologically diverse extremist groups has required the United States to rethink how it defines and prioritizes threats. Whereas traditional counterterrorism frameworks were built around hierarchical organizations like AQ, today's landscape includes hybrid actors that blend terrorism, organized crime, political extremism, and foreign influence. This diversification strains existing authorities, complicates intelligence collection, and forces agencies to operate across legal and operational seams that did not exist twenty-five years ago.

Second, the shift of jihadist activity toward Africa presents a strategic dilemma. With over two-thirds of ISIS's global activity occurring on the continent and seven of the ten countries with the highest deaths linked to terrorism located there, Africa has become the world's most active terrorism theater. Yet U.S. and partner resources remain limited, and intelligence coverage is uneven. The United States must now balance counterterrorism priorities in Africa with ongoing commitments in the Middle East, Central Asia, and Europe, while recognizing that instability in the Sahel can generate threats that reach the U.S. homeland through migration flows, smuggling networks, and online radicalization.

Third, the rise of lone actors and inspired attackers requires a shift from organization-centric counterterrorism to behavior-centric prevention. In recent years, the number of individuals radicalized without formal group affiliations has increased exponentially, driven increasingly by personal grievances, online propaganda, and algorithm-driven radicalization.[124] This shift requires confronting the reality that most attacks in the United States are now conducted by individuals – not groups – and that many of these individuals are invisible to law enforcement until it is too late. This underscores the importance of removing information sharing silos between federal, state, and local partners, as well as across the Intelligence Community.

Fourth, the domestic extremism landscape, spanning HVEs inspired by foreign groups and DVEs motivated by domestic ideologies, requires a unified but differentiated approach. Anti-government extremists, anarchist networks, white supremacists, and ideologically motivated lone actors each present distinct challenges. The legal ambiguity between domestic terrorism, hate crimes, and foreign-inspired extremism complicate both prosecution and prevention efforts. The United States must define key terms, clarify agency authorities, and invest in prevention strategies that address both foreign-inspired and domestically motivated violence – without conflating the two.

Finally, the blending of terrorism with cyber capabilities introduces a domain where traditional counterterrorism tools are insufficient. Terrorist groups exploit encrypted platforms, social media ecosystems, and emerging technologies such as AI, drones, and 3D-printed weapons. They use cyber tools to recruit, coordinate, fundraise, and inspire attacks.[125] As ISIS attempts to build a "virtual caliphate," and as Al Qaeda and Hamas expand their digital propaganda networks, the United States must integrate cyber defense with counterterrorism in ways that break down longstanding bureaucratic silos. The next phase of terrorism will be shaped as much by code and algorithms as by physical safe havens or battlefield dynamics.

Twenty-five years after the attacks of September 11th, the United States faces a terrorism threat environment that is both familiar and unknown. The adversaries have changed, the technologies have changed, and the geography of danger has shifted, but the core challenge remains: protecting the American people from those who seek to do harm. The legacy of 9/11 is not only the memory of what was lost, but the responsibility to adapt to a world where terrorism is less hierarchical, more technology-driven, and unconstrained by borders. It is important to recognize that the next frontier of this fight will unfold increasingly in the cyber domain, where terrorists, criminal networks, and hostile states exploit digital platforms, encrypted communications, and emerging technologies to recruit, radicalize, coordinate, and attack.

Cybersecurity and Artificial Intelligence

As the prior section previewed, the modern homeland security environment is perhaps most notably marked by the rise of cyber threats as a national security concern. In cyberspace, the United States is no longer confronting only individual hackers seeking money or notoriety. It now faces sustained campaigns carried out by nation states with the resources, patience, and capabilities of intelligence services and military organizations. These actors steal sensitive information, disrupt operations, compromise trusted vendors and service providers, abuse legitimate administrative tools, and remain inside networks for extended periods, often without being detected.

Advancements in technology have resulted in Americans and the country relying significantly on digital systems every day, making these systems more attractive targets for our adversaries. Communications networks, transportation systems, financial services, energy infrastructure, water systems, health care facilities, and government services are now deeply interconnected. A compromise affecting one organization, vendor, or technology provider can produce operational consequences across an entire sector, supply chain, or region. Adversaries understand these dependencies and are increasingly seeking access that could be used for espionage, disruption, or destructive activity during a crisis or conflict.

The development and use of destructive malware demonstrated that cyber operations could produce consequences far beyond the loss of data. Stuxnet, discovered in 2010, showed that malicious code could manipulate industrial control systems and cause physical damage to nuclear equipment.[126] In 2017, Russian military intelligence deployed NotPetya through a compromised software update in Ukraine. Although Ukraine was the principal target, the malware spread through interconnected corporate networks and caused billions of dollars in losses worldwide.[127] In 2021, a ransomware attack against Colonial Pipeline prompted the

company to halt pipeline operations, disrupting fuel distribution and contributing to shortages and panic buying across parts of the East Coast of the United States.[128]

These events attracted national attention because of their scale, but they reflect threats that organizations across the country face every day. Hospitals, schools, local governments, water and wastewater systems, manufacturers, communications providers, and other critical infrastructure entities confront ransomware, fraud, espionage, and disruptive cyber activity on a continuing basis. Many of these organizations operate essential services with limited cybersecurity personnel, aging technology, constrained budgets, and little tolerance for operational downtime. The consequences of a cyber incident can extend quickly from a compromised network into public safety, economic security, and the delivery of basic services.

The discovery of the People's Republic of China (PRC) sponsored campaigns known as Volt Typhoon and Salt Typhoon in 2023 and 2024 further revealed the strategic character of the current threat.[129] Volt Typhoon demonstrated the PRC's effort to gain persistent access to critical infrastructure, including through compromised routers and other devices, while using legitimate system tools to reduce the likelihood of detection. The campaign was not limited to conventional intelligence collection. Its targeting and methods were consistent with an effort to establish access that could be used to disrupt communications and other essential functions during a future geopolitical crisis or military conflict. Salt Typhoon, by contrast, exposed the breadth and depth of PRC access to major telecommunications networks and the intelligence value of compromising systems that carry sensitive communications and lawful intercept information. Together, these campaigns illustrate how a capable adversary can exploit widely deployed technology, trusted access, and complex supply chains to operate inside strategically significant networks for prolonged periods.

At the same time, the number of systems, devices, applications, and third parties that organizations must defend has expanded dramatically. The rapid shift to remote work during the COVID-19 pandemic accelerated the adoption of cloud services, virtual private networks, personal devices, remote collaboration platforms, and externally accessible infrastructure. Many organizations implemented these technologies under urgent conditions, without the time, personnel, or resources necessary to fully assess their security. Since then, continued cloud adoption, the growth of connected devices, the convergence of information technology and operational technology, and increasingly complex software supply chains have created additional pathways for compromise.

Artificial intelligence (AI) is now accelerating this transformation. AI can assist defenders by analyzing large volumes of security data, identifying anomalous behavior, prioritizing vulnerabilities, generating defensive code, and augmenting a limited cyber workforce. But the same capabilities can also assist malicious actors. AI can improve reconnaissance, facilitate social engineering, accelerate vulnerability research, generate or modify malicious code, and allow threat actors to conduct operations with greater speed and scale. As advanced models become more capable of performing multi-step tasks with limited human direction, the distinction between a tool that assists an operator and a system capable of executing substantial portions of an operation autonomously will continue to narrow.

These developments have also made vulnerability management more difficult. Defenders once had at least some time between the public disclosure of a software vulnerability and its widespread exploitation. That window is now shrinking rapidly and, in some cases, no longer exists. Threat actors are increasingly exploiting vulnerabilities before they are publicly disclosed, assigned a Common Vulnerabilities and Exposures identifier, or addressed through a widely available patch. Once technical details or proof-of-concept code become public, automated tools and AI-enabled capabilities can accelerate exploitation even further. Organizations must be able to identify exposed systems, prioritize the vulnerabilities that pose the greatest risk, deploy mitigations quickly, and assume that an adversary may already know about a flaw.

Twenty-five years after September 11th, the homeland security mission must account for threats that are persistent, difficult to observe, and often ambiguous in purpose. Cyber activity can support criminal profit, intelligence collection, intellectual property theft, political coercion, military preparation, and destructive operations, sometimes simultaneously. The same infrastructure may be targeted by criminal groups, foreign intelligence services, military units, proxies, or actors whose relationship to a government is deliberately hidden. Attribution may require time, sensitive intelligence, and cooperation among government and industry, even as victims must make immediate operational decisions.

Cybersecurity is now inseparable from the protection of the homeland, but resilience remains uneven. The nation's largest companies may possess sophisticated security teams and substantial resources, but local governments, rural hospitals, school districts, small utilities, and other essential service providers often face the same adversaries with far fewer personnel and less modern technology. Nation states and criminal groups are exploiting this imbalance. They target weakly defended organizations, trusted vendors, remote access systems, and shared service providers that can provide access to larger networks or create consequences beyond the initial victim.

Meeting this challenge will require more than just strengthening the defenses of individual organizations. It will require sustained coordination among federal, state, local, tribal, and territorial governments, critical infrastructure owners and operators, technology providers, researchers, and the cybersecurity industry. It also requires timely and useful information sharing, clear responsibility across federal agencies, practical support for organizations with limited resources, more secure technology, and the ability to detect, contain, and recover from incidents before they cause broader harm. No strategy can prevent every intrusion. Our goal must be to keep adversaries from turning access into widespread disruption, physical harm, economic damage, or a strategic advantage.

BORDER SECURITY, SCREENING AND VETTING

The terrorist attacks of September 11, 2001, exposed significant weaknesses in the United States' ability to identify and prevent terrorists from exploiting our lawful travel and immigration systems. The 9/11 Commission Report found that the hijackers successfully used passports and visas to enter and remain in the United States, concluding that "for terrorists, travel documents are as important as weapons."[130] In the years following the attack, the United States has substantially strengthened its screening and vetting security posture by advancing identity verification procedures, improving information sharing across federal agencies and international

partners, expanding biometric capabilities, and integrating automated intelligence tools into the border security and immigration process.

These reforms have made it significantly more difficult for known or suspected terrorists to travel under fraudulent identities or exploit vulnerabilities in the system, but gaps remain. The border security policies implemented under President Biden amplified certain vulnerabilities, particularly at the Southwest border, where overwhelmed frontline personnel were unable to conduct adequate screening and vetting of all individuals arriving at the border due to the volume of people attempting to enter the United States.

Despite the significant border security successes under President Trump's leadership that have reversed these trends and allowed DHS to regain operational control along the Southwest border, the overall threat environment at U.S. borders is even more complex today than ever before as the world has become more interconnected and accessible. Today, imports are more than three times greater than in 2001, carried to U.S. borders by increasing numbers of ships, containers, crates, and boxes that must be carefully inspected.[131] Although advances and investments in non-intrusive inspection (NII) technologies like backscatter radiation scanners have greatly expanded the capacity to search and ensure the safety of this cargo, the sheer volume of goods entering the U.S. increases the risk that dangerous contraband may enter undetected.

At the same time, suspected terrorist organizations, transnational criminal organizations (TCOs), human smuggling networks, and foreign non-state actors increasingly exploit cutting-edge, commercially available cryptography, telecommunications, and financial technologies to conceal and coordinate their illicit operations. Because vetting fundamentally depends on the government's ability to connect individuals to criminal or terrorist organizations and activities, the ability to evade detection poses a persistent challenge to screening and vetting processes.

TCOs operating within the United States are not limited to cartels originating from Central and South America. In September 2025, the Subcommittee on Oversight, Investigations, and Accountability held a hearing focused on how Chinese criminal organizations are present within the United States and conducting illicit drug operations. As Subcommittee Chairman Josh Brecheen (R-OK) explained, "we have enabled potential agents of the Chinese Communist Party to build a sophisticated and concerted criminal network, under the guise of these marijuana grow operations, throughout the United States, which enables a wide range of criminal activity and presents unique threats to our national security. This is a convergence of organized crime, human and drug trafficking, and public health risks, which all operate at a scale and sophistication that crosses state and national lines and is beyond the normal capabilities of state and local law enforcement. These agencies need the help of federal law enforcement to unravel these criminal networks."[132]

In an increasingly digital age, TCOs are also leveraging new technology such as AI and cryptocurrency. Chinese-Language Money Laundering Networks (CLMNs) are some of the most prolific actors involved in crypto-enabled transnational financial crime and specifically money laundering. Reports show that CLMNs laundered over $16 billion in cryptocurrency in 2025 alone – making up one-fifth of the total illicit cryptocurrency crime network.[133] When China banned cryptocurrency trading in 2021, some CLMNs moved their operations to Southeast Asia, where corrupt governments and lax regulations allow them to conduct scam operations freely.[134]

Mexican drug cartels are also increasingly involved in cryptocurrency-based money laundering schemes that connect narcotics trafficking in the Western Hemisphere to Chinese money laundering brokers and supply networks.[135] Several federal advisories and analyses[136] describe a recurring pattern in which cartels sell U.S. dollars generated through drug sales to Chinese actors in exchange for cryptocurrency. This arrangement is attractive to both sides because it allows cartel proceeds to be moved outside of traditional banking channels, reduces the need to transport bulk cash across borders, and makes it more difficult for law enforcement to identify, trace, and seize illicit funds.[137] Chinese money brokers can then place those U.S. dollars into the American economy through real estate purchases, luxury goods, shell companies, and other asset acquisitions, while cartel actors use the cryptocurrency to finance their operations, including the purchase of fentanyl precursors and other goods sourced from China.[138] In effect, cryptocurrency serves as a bridge between cartel drug trafficking, Chinese illicit finance networks, and the transnational supply chains that sustain the fentanyl trade.

As foreign adversaries continue to evolve and adopt new tactics and technologies, the United States must ensure that its screening and vetting systems adapt at an equal pace to identify high-risk travelers while facilitating legitimate trade and travel. This not only requires further investments in infrastructure and personnel to ensure that the increasing amounts of goods and people entering the U.S. can be inspected and processed efficiently, but also partnering with private companies to identify and develop new technologies that can address emerging vulnerabilities.

While the Southwest border has rightly attracted the most attention from policymakers and the public alike over the last several years, recent border security improvements have also prompted TCOs to shift their efforts to the Northern border. For example, in May 2025, Homeland Security Investigations (HSI) identified and detained four Mexican nationals who were smuggling individuals from Central and South American countries into the United States from Canada.[139]

In addition to human smuggling, law enforcement has also reported an increase in drug smuggling along the Northern border. In September 2025, in coordination with CBP, HSI interdicted nearly 2,000 pounds of drugs in commercial trucking vehicles in a single day.[140] Drug seizure events along the Northern border have increased month over month since before Fiscal Year (FY) 2024, reaching new highs in FY 2026.[141] Logically, the emphasis placed on curbing the crisis at the Southwest border has pushed illegal alien trafficking to the Northern border.[142]

The United States must therefore also prioritize Northern border security through enhanced intelligence-sharing and law enforcement coordination with the Canadian government. This is essential to ensure no vulnerabilities may be exploited in the North as illegal entries and illicit operations become increasingly more challenging to conduct at the Southwest border.

OUTSTANDING 9/11 COMMISSION RECOMMENDATIONS

Outstanding 9/11 Commission Recommendations

Throughout the 119th Congress, the Committee, with the assistance of the U.S. Government Accountability Office (GAO), has reviewed the fulfillment status of the Commission's forty-one recommendations, identifying twenty-three of the original forty-one recommendations whose policy objectives align with the Committee's legislative and oversight jurisdiction. The following analyses provide a brief assessment of the implementation status and progress made to meet the objectives set forth by each of those twenty-three since their publication in 2004.

Recommendation: *Vigorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us to understand their networks, search them out, and disrupt their operations. Intelligence and law enforcement have targeted the relatively small number of financial facilitators individuals Al Qaeda relied on for their ability to raise and deliver money at the core of Al Qaeda's revenue stream. These efforts have worked. The death or capture of several important facilitators has decreased the amount of money available to Al Qaeda and has increased its costs and difficulty in raising and moving that money. Captures have additionally provided a windfall of intelligence that can be used to continue the cycle of disruption.*

> **Progress:** The *USA PATRIOT Act of 2001* sought to increase the information available to law enforcement and the authorities available to detect and prosecute terrorism financing.[143] Additionally, the U.S. has leveraged sanctions as a tool of policy to disrupt terrorist financial networks and military operations to degrade the facilities and resources relied upon by state sponsors of terrorism to finance terrorist activity. However, technological sophistication is increasing the pace at which adversaries can adapt and evade U.S. financial pressure. In the post-9/11 environment, encrypted online platforms, the proliferation of "scam centers," and increased use of cryptocurrency challenge our ability to identify and disrupt terrorist revenue streams.[144]

Recommendation: *Targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.*

> **Progress:** Robust screening and vetting processes have been integrated across the homeland security enterprise and with international allies and partners. This includes hundreds of Homeland Security Investigations (HSI) special agents and criminal analysts forward deployed in international offices and embedded within U.S. Embassies, working to disrupt crime and prevent U.S.-bound travel by threat actors.[145]
>
> The United States has substantially implemented this 9/11 Commission recommendation by integrating terrorist travel intelligence with border security and law enforcement. Since 9/11, agencies have established consolidated terrorist watchlists, expanded biometric screening, strengthened intelligence sharing through organizations like the National Counterterrorism Center, and enhanced biometric screening conducted by CBP

and TSA.[146] Congress also passed the *Implementing Recommendations of the 9/11 Commission Act of 2007*, which required DHS to oversee a dedicated terrorist travel program and enhanced biometric screening and information sharing systems.[147] While these measures have significantly improved the government's ability to identify and intercept suspected terrorists, DHS has acknowledged that terrorist threats to travel remain an ongoing challenge and require continuous evaluation of intelligence integration, biometric identification capabilities, and international security cooperation.

Recommendation: *The U.S. border security system should be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with system wide goals in mind. Extending those standards among other governments could dramatically strengthen America and the world's collective ability to intercept individuals who pose catastrophic threats.*

Progress: The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) codified the National Counterterrorism Center, created to eliminate information silos in terrorist intelligence, and the Terrorist Screening Data Set (TSDS), which was established to monitor the entry of individuals who may pose threats to the homeland, including known associates of suspected terrorists.[148] This information sharing has allowed CBP to identify potential terrorists or other bad actors at and between ports of entry. Additionally, the Automated Biometric Identification System (IDENT) Program was created to collect, process, and retain personally identifiable information, including biometrics. In 2004, DHS expanded the IDENT program to trace additional information including visa benefits and watchlist screening of individuals encountered at a port of entry. DHS has begun work to replace IDENT with the Homeland Advanced Recognition Technology (HART) Program to address system shortcomings and otherwise modernize biometric collection and storage, but that transition remains ongoing.[149] Trusted traveler programs like the NEXUS program, the Global Entry Program, and TSA PreCheck have been introduced to facilitate easier travel for known travelers.[150]

Recommendation: *The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers. It should be integrated with the system that provides benefits to foreigners seeking to stay in the United States. Linking biometric passports to good data systems and decision making is a fundamental goal. No one can hide his or her debt by acquiring a credit card with a slightly different name. Yet today, a terrorist can defeat the link to electronic records by tossing away an old passport and slightly altering the name in the new one.*

Progress: CBP uses the Traveler Verification Service to compare facial biometrics ensuring that biometric entry-exit accurately identifies travelers. CBP has completed the rollout of biometric entry for air travel, screening about 99.1% of all inbound passengers. However, CBP has not achieved the same for air exit programs, scanning about 40% of outbound travelers.[151] Aside from air entry, CBP considers sea entry and pedestrian land

travel entry to be completely implemented.[152] In November of 2025, CBP issued a final rule removing existing regulations limiting biometric exit programs to pilot programs.[153] Additionally, all passports issued by the Department of State since 2006 have been e-passports, containing contactless chips that when scanned provide the information that is printed within the passport.[154] The latest passport model, the Next Generation Passport, allows the travel document to be validated worldwide.[155]

Recommendation: *The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation.*

Progress: The U.S. network of allies and partners functions as a force multiplier in countering transnational terror threats. Multilateral partnerships facilitate the sharing of threat information across an allied network. This includes the NATO Intelligence Fusion Centre based in the United Kingdom (U.K.), that became operational in 2007.[156] The Five Eyes intelligence alliance comprising the U.S., U.K., Australia, Canada, and New Zealand that was historically grounded in military intelligence sharing has additionally evolved since 9/11 to include greater emphasis on counterterrorism, cybersecurity, and law enforcement information sharing.[157]

Recommendation: *Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.*

Progress: In keeping with the 9/11 Commission Report's recommendations,[158] beginning on May 7, 2025, TSA began implementing the requirements of the *REAL ID Act*, deeming a standard state-issued driver's license insufficient for domestic air travel in the United States.[159] After several previous extensions over the last two decades, TSA required REAL ID compliance across U.S. airports for identity verification and continues to support the deployment of secure, frictionless passenger identification platforms. Congress continues to conduct oversight of the implementation of REAL ID and any programs developed or considered by TSA related to individuals traveling without compliant identity documentation.

TSA continues to lead in biometric identification technologies for passenger verification, relying on Credential Authentication Technology (CAT) systems and modern identity solutions that verify PreCheck traveler populations through the Touchless ID system. These identity verification technologies confirm a passenger's Trusted Traveler and Secure Flight pre-screening status, and validate flight reservations.[160] The CAT system verifies the passengers against their identity document (ID), while Touchless ID for PreCheck travelers leverages biometric technology to verify the passenger's identity by

comparing a live photo to a gallery of pre-staged photos under the passenger's Trusted Traveler profile.[161] TSA's biometric identification solutions are tested, evaluated, and ultimately certified through the DHS Science and Technology Directorate, and in particular, at the TSA Systems Integration Facility (TSIF).[162] Furthermore, Maritime Transportation System (MTS) security has been significantly enhanced since enactment of the *Maritime Transportation Security Act* (MTSA), which implemented the Transportation Worker Identification Card (TWIC) to enhance the vetting of trucking and maritime workers who require credentials in order to access secure sites as required by their occupation.[163]

Recommendation: *Hard choices must be made in allocating limited resources. The U.S. Government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort. The plan should assign roles and missions to the relevant authorities (federal, state, regional, and local) and to private stakeholders. In measuring effectiveness, perfection is unattainable. But terrorists should perceive that potential targets are defended. They may be deterred by a significant chance of failure.*

Progress: Under the *Aviation and Transportation Security Act* (ATSA), TSA was established to ensure federal personnel were responsible for regulating and securing our nation's transportation system.[164] Further, the *Implementing the 9/11 Commission Recommendations Act of 2007* required a National Strategy for Transportation Security (NSTS), which acts as the governing document for federal transportation security efforts.[165] The NSTS included objectives, roles, responsibilities, and performance evaluations for public and private stakeholders across the transportation system, and aids in the development of security plans for the aviation, maritime, and surface transportation sectors. An intermodal security plan is included to address threats to the global movement of goods across all transportation sectors.[166]

Building upon this strategy, the *FAA Reauthorization Act of 2018* included a requirement for TSA to establish a risk-based budget and resource allocation plan, which has since been incorporated into the NSTS.[167] In keeping with the 9/11 Commission Report's recommendations and previous requirements, TSA now includes risk-based priorities in the NSTS to continue securing the transportation system while working with state, local, tribal, and territorial law enforcement authorities.[168]

Recommendation: *Improved use of "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by the TSA, and it should utilize the larger set of watchlists maintained by the federal government. Air carriers should be required to supply the information needed to test and implement this new system.*

Progress: The Computer-Assisted Passenger Prescreening System (CAPPS) was originally intended to provide a more comprehensive risk assessment based on passenger data and intelligence sources, aimed at categorizing passengers by risk level and making

recommendations for appropriate screening procedures.[169] However, from its early days, CAPPS received significant privacy and operational pushback, including alleged misuse of passengers' personal data, inaccurate risk scoring, and unfair targeting of passengers.[170] For instance, on 9/11, the nineteen hijackers were screened by the CAPPS system yet only about half of them were identified for further inspection and monitoring, and the only security measure in place was to delay loading their checked luggage onto the flight until it was confirmed they had boarded the aircraft.[171] Due to ongoing scrutiny, TSA terminated CAPPS in 2005 and replaced it with the Secure Flight program.[172] Today, the Secure Flight program screens individuals before they access the sterile area of the airport or board an aircraft. This screening is designed to identify known or suspected terrorists, or other individuals who may be a threat to transportation or national security, to prevent certain individuals from gaining access to the airport or plane where they may jeopardize the lives of passengers and crew. The Secure Flight program aims to ensure these identified individuals receive enhanced physical screening at the security checkpoint prior to accessing the airport's sterile area or boarding an aircraft.[173]

Secure Flight maintains a passenger watch list continuously updated based on carrier-provided traveler information added to the No Fly List, and Selectee portions of the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC), to identify individuals who may need additional screening or are prevented from travel.[174] The Secure Flight program has proven to be a valuable measure in upholding aviation security and supporting the federal government's counterterrorism efforts by assisting in detecting individuals on government watch lists who seek to travel by air, and by facilitating the secure travel of the public.[175] Secure Flight has served as a critical TSA initiative to ensure safe air travel by pre-screening passengers, integrating with trusted traveler programs, and maintaining strict privacy protections.

Recommendation: *The TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. As a start, each individual selected for special screening should be screened for explosives. Further, the TSA should conduct a human factors study, a method often used in the private sector, to understand problems in screener performance and set attainable objectives for individual screeners and for the checkpoints where screening takes place.*

Progress: Through ATSA, TSA is mandated by Congress to screen all checked baggage for explosives by electronic or other approved means.[176] As a result, the Electronic Baggage Screening Program (EBSP) was established to qualify, procure, deploy, and sustain explosives detection systems (EDS) technology used to screen checked baggage for explosives, to ensure the safety and security of air travel.[177] EDS also pairs with Computed Tomography (CT) screening technology, which employs advanced imaging and algorithms to detect explosives with a high degree of accuracy and efficiency. Congress further directed TSA to develop a strategic plan to implement explosives screening at passenger checkpoints through the *Intelligence Reform and Terrorism Prevention Act of 2004*, and to implement it fully with the *Implementing the 9/11 Commission Recommendations Act of 2007*.[178] For passenger screening, TSA relies on explosive trace detection technology to screen travelers and their property to identify

attributes of trace explosives or compounds. This widely used alarm resolution capability enables Transportation Security Officers (TSOs) to perform fast, accurate screening of trace explosive substances. Today, TSIF, as codified through the *FAA Reauthorization Act of 2018*, conducts the testing, evaluation, and certification of explosives detection technology for passengers and checked baggage, incorporating human factor analyses to develop effective screening technology to secure our nation's airports.[179]

Recommendation: *As the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared.*

Progress: The Privacy and Civil Liberties Oversight Board (PCLOB) was established as an independent agency by the *Implementing the 9/11 Commission Recommendations Act of 2007*.[180] The PCLOB directly reflects the sentiment of the 9/11 Commission that an enhanced intelligence community and greater information sharing would require robust oversight to ensure the protection of American civil liberties. PCLOB today is an independent agency within the Executive branch, with bipartisan Senate-confirmed membership. In providing oversight and advice, the Board seeks to balance counterterrorism efforts with safeguarding American privacy and civil liberties.

Recommendation: *The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use.*

Progress: The burden of proof standard was never enshrined into a formal legal test. No statute requires Executive Branch agencies to affirmatively prove, before a court or independent body, that a particular governmental power "materially enhances security," and has "adequate supervision" before it can be retained. Instead, the principle has functioned mainly as a benchmark, rather than as an enforceable legal burden.

Recommendation: *At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties.*

Progress: As noted earlier, Congress created the PCLOB through *the Intelligence Reform and Terrorism Prevention Act of 2004* and reconstituted it as an independent Executive Branch agency with subpoena authority in the *Implementing the 9/11 Commission Recommendations Act of 2007*. Its status, however, remains precarious. The PCLOB currently has no confirmed in-term members and lacks the quorum necessary to issue board-level guidance, reports, or open new oversight projects.

Recommendation: *Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities. Now, in 2004, Washington, D.C., and New York City are certainly at the top of any such list. We understand the contention that every state and city needs to have some*

minimum infrastructure for emergency response. But federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support. Congress should not use this money as a pork barrel.

> **Progress:** The *Implementing Recommendations of the 9/11 Commission Act of 2007*[181] amended the *Homeland Security Act of 2002*[182] by authorizing DHS, acting through FEMA, to administer various forms of grant funding to assist states, localities, urban areas, and tribal and territorial governments in strengthening the nation's ability to prevent, protect against, respond to, and recover from terrorist attacks and other threats. The *Implementing Recommendations of the 9/11 Commission Act of 2007* authorized the Homeland Security Grant Program (HSGP) and two constituent grant programs comprising HSGP, including the State Homeland Security Grant Program (SHSP) and the Urban Area Security Initiative (UASI).
>
> The Act further required the FEMA Administrator to consider relevant risk information in awarding funds for each state and high-risk urban area receiving assistance through SHSP and UASI, such as each eligible jurisdiction's relative threat, vulnerability, and consequence from acts of terrorism, as well as the effectiveness of proposed grant justifications in mitigating acts of terror.[183] The Act also required the Administrator to ensure, at a minimum, that twenty-five percent of combined SHSP and UASI funds are spent on law enforcement terrorism prevention activities in any given fiscal year.[184] Simultaneously, to ensure an adequate degree of uniformity across the nation in building out capacities to counter terrorist threats, this legislation also required statutory minimums for all states and territories receiving SHSP funds.[185]

Recommendation: *Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven frameworks for emergency response. We strongly support the decision that federal homeland security funding will be contingent, as of October 1, 2004, upon the adoption and regular use of ICS and unified command procedures. In the future, the Department of Homeland Security should consider making funding contingent on aggressive and realistic training in accordance with ICS and unified command procedures.*

> **Progress:** Following the attacks of September 11th, and amidst greater awareness of the need for establishing a comprehensive Incident Command System (ICS) for coordinating multi-jurisdictional and multi-agency response and recovery activities in the domestic context, the *Homeland Security Act of 2002* required the DHS Secretary, acting through a designated Under Secretary for Emergency Preparedness and Response, to build a comprehensive National Incident Management System (NIMS) across federal, state, and local agencies and to consolidate existing federal government emergency response plans into a single, coordinated National Response Plan.[186] These efforts were given further definition when President George W. Bush issued Homeland Security Presidential Directive 5 (HSPD-5) on February 28, 2003, mandating the adoption of NIMS to provide for interoperability and compatibility across federal, state, and local capabilities, and, beginning in Fiscal Year (FY) 2005, requiring federal departments and agencies to make

adoption of NIMS a prerequisite for states and localities to receive federal preparedness funding.[187] FEMA, after extensive review of existing incident management systems, released its initial NIMS guidance in March 2004.[188]

Following the devastation of Hurricane Katrina in 2005, Congress passed the *Post-Katrina Emergency Management Reform Act of 2006* (*PKEMRA*) through FY 2007 DHS appropriations, which mandated the establishment of a National Integration Center to monitor and periodically review and revise, as appropriate, NIMS.[189] *PKEMRA* also authorized the National Training Program to implement NIMS and the National Exercise Program to test and evaluate NIMS in service of the National Preparedness Goal (NPG).[190] In an effort to meet compliance with *PKEMRA*, President Barack Obama issued Presidential Policy Directive 8 (PPD-8) on March 30, 2011, which gave further definition to the NPG and the corresponding National Preparedness System (NPS).[191]

Recommendation: *Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress.*

Progress: Congress sought to fulfill the Commission's recommendation to allocate radio spectrum for public safety purposes when it passed the *Middle Class Tax Relief and Job Creation Act of 2012*,[192] Title VI of which established the FirstNet Authority (FirstNet). FirstNet, an "independent authority" within the Department of Commerce's National Telecommunications and Information Administration (NTIA), became responsible for overseeing the buildout, deployment, and operation of a nationwide interoperable public safety broadband network on a portion of the 700 MHz Band, also known as the "D Block."[193] In March 2017, FirstNet awarded a twenty-five-year contract with AT&T to build and manage its public safety network infrastructure.[194]

As a result of the 9/11 Commission's findings as well as the continued communications challenges that occurred during the response to Hurricane Katrina, Congress established the Office of Emergency Communications (OEC) in Section 671 of *PKEMRA*.[195] *PKEMRA* required OEC, through its director, to assist the Secretary of Homeland Security in coordinating federal interoperable communications programs, conducting outreach and support to emergency response providers, and establishing communications policies for DHS. In 2018, Congress passed legislation which directed DHS to re-designate OEC as the Emergency Communications Division within the Cybersecurity and Infrastructure Security Agency (CISA).[196]

Recommendation: *We endorse the American National Standards Institute's recommended standard for private preparedness. We were encouraged by Secretary Tom Ridge's praise of the standard and urge the Department of Homeland Security to promote its adoption. We also encourage the insurance and credit-rating industries to look closely at a company's compliance with the ANSI standard in assessing its insurability and creditworthiness. We believe that*

compliance with the standard should define the standard of care owed by a company to its employees and the public for legal purposes. Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security.

> **Progress:** Codified by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, the DHS Secretary was required to establish and implement a voluntary private-sector preparedness accreditation and certification program.[197] In June 2008, DHS entered into contract with the American National Standards Institute (ANSI)-American Society for Quality National Accreditation Board (ANAB) to carry out the implementation of the program, which became known as PS-Prep. ANAB became responsible for developing and overseeing the certification process, managing accreditation, and accrediting qualified third parties to carry out certifications.[198] In June 2010, DHS announced its adoption of three standards for the PS-Prep program.[199] ANAB continues to update standards for private-sector preparedness certification.[200]

Recommendation: *We recommend the establishment of a National Counterterrorism Center (NCTC), built on the foundation of the existing Terrorist Threat Integration Center (TTIC). Breaking the old mold of national government organization, this NCTC should be a center for joint operational planning and joint intelligence, staffed by personnel from the various agencies. The head of the NCTC should have authority to evaluate the performance of the people assigned to the Center.*

> **Progress:** Consistent with the 9/11 Commission's recommendation, the National Counterterrorism Center (NCTC) was established in 2004 by Executive Order 13354.[201] It was codified by the *Intelligence Reform and Terrorism Prevention Act* later that year.[202] NCTC's primary mission is to integrate IC analyses of terror threats into cohesive threat assessments that support a common operating picture, regular information sharing, and enhanced situational awareness. Additionally, per the Commission's recommendation, NCTC is staffed by personnel from across the Intelligence Community.

Recommendation: *The current position of Director of Central Intelligence should be replaced by a National Intelligence Director with two main areas of responsibility: (1) to oversee national intelligence centers on specific subjects of interest across the U.S. Government and (2) to manage the national intelligence program and oversee the agencies that contribute to it.*

> **Progress:** The *Intelligence Reform and Terrorism Prevention Act of 2004* reformed leadership and oversight of the Intelligence Community. Consistent with the 9/11 Commission's recommendation, the Director of Central Intelligence was replaced. While the Director of Central Intelligence was formerly both the head of the Central Intelligence Agency (CIA) and had oversight authority over the entire Intelligence Community, IRTPA bifurcated these positions by creating a distinct Director of National Intelligence (DNI) that oversees all components of the Intelligence Community and manages the National Intelligence Program (NIP).[203]

Recommendation: *The CIA Director should emphasize (a) rebuilding the CIA's analytic capabilities; (b) transforming the clandestine service by building its human intelligence capabilities; (c) developing a stronger language program, with high standards and sufficient financial incentives; (d) renewing emphasis on recruiting diversity among operations officers so they can blend more easily in foreign cities; (e) ensuring a seamless relationship between human source collection and signals collection at the operational level; and (f) stressing a better balance between unilateral and liaison operations.*

> **Progress:** In response to the Joint Inquiry initiated in 2002 by the House and Senate intelligence committees, the CIA's Office of Inspector General in 2005 produced a report on CIA Accountability with Respect to the 9/11 Attacks.[204] This report was partially declassified in 2015 and reflects CIA concurrence with several findings made by the congressional committees of jurisdiction and 9/11 Commission recommendations. This includes identifying the need to strengthen the Agency's analytic proficiency and capacity.

Recommendation: *Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge.*

> **Progress:** Prior to 9/11, information relevant to counterterrorism was housed in a variety of databases and IC components largely lacked standard processes for information sharing. Much of the intelligence reform effort post-9/11 has focused on strengthening information sharing protocols and integrating the Intelligence Community. This is reflected in the establishment of the NCTC, creation of the DNI, and establishment of the Office of Intelligence & Analysis (I&A)[205] within the Department of Homeland Security to bridge the information gap between federal IC components and state and local law enforcement partners.
>
> In November 2018, the *Cybersecurity and Infrastructure Security Agency Act of 2018,* which was led by then-Chairman and current member of the Homeland Security Committee, Rep. Michael T. McCaul (R-TX), was signed into law, elevating the mission of the former DHS National Protection and Programs Directorate to the newly created Cybersecurity and Infrastructure Security Agency (CISA). As the nation's lead cyber defense agency responsible for protecting U.S. critical infrastructure, CISA plays a central role in information sharing across sectors with public and private partners. Additionally, key legislation such as the *Cybersecurity Information Sharing Act of 2015* (CISA 2015) has further encouraged and enabled cyber threat information sharing to improve collective defense and resilience and provide forthcoming companies with legal protection when sharing threat information with CISA.

Recommendation: *The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a "trusted information network."*

Progress: The Department of Homeland Security launched the Homeland Security Information Network (HSIN) in 2004 to serve as a centralized platform for federal, state, local, tribal, territorial, international, and private sector partners to share information.[206] HSIN is currently undergoing a modernization effort designed to enhance its information security and utility across this spectrum of partners.

Congress enacted *CISA 2015* to enable the voluntary sharing of information between government and non-government agencies. *CISA 2015* provides legal clarity around the prevention, detection, analysis, and mitigation of cyber threats; articulates a process for cybersecurity information sharing; and establishes liability, privacy, and civil liberties protections.[207] *CISA 2015* removed companies' legal exposure associated with sharing cybersecurity threat data with the federal government, which ultimately encouraged broader information sharing across the ecosystem and enhanced collective defense. *CISA 2015* authorities are currently at risk of expiring if they are not reauthorized by Congress by December 11, 2026.

Recommendation: *Congressional oversight for intelligence and counterterrorism is now dysfunctional. Congress should address this problem. We have considered various alternatives: A joint committee on the old model of the Joint Committee on Atomic Energy is one. A single committee in each house of Congress, combining authorizing and appropriating authorities, is another.*

Progress: There has been limited progress made in addressing this recommendation. Congressional oversight related to intelligence and counterterrorism continues to span several committees. Jurisdiction over Intelligence Community components encompasses more than one committee in each chamber of Congress, limiting visibility into IC operations and at times complicating or delaying legislative initiatives. Oversight for counterterrorism policy is similarly complicated as counterterrorism legal authorities are scattered across various sections of the U.S. Code. In both cases, there is no single committee that has combined authorizing and appropriating authorities.

Recommendation: *The Department of Homeland Security and its oversight committees should regularly assess the types of threats the country faces to determine (a) the adequacy of the government's plans and the progress against those plans to protect America's critical infrastructure and (b) the readiness of the government to respond to the threats that the United States might face.*

Progress: The Department of Homeland Security's Office of Intelligence & Analysis and its statutory mission areas were formally established by the *Implementing Recommendations of the 9/11 Commission Act of 2007*. As delineated at 6 U.S.C. § 121, regularly assessing the nature and scope of terrorist threats to the United States, including threats to key resources and critical infrastructure, is at the core of I&A's mission.[208] I&A is additionally required to assess potential countermeasures and protective measures to mitigate terrorist threats.

Pursuant to 6 U.S.C. § 652, CISA is directed to develop, coordinate, and implement strategic plans, risk assessments, and national efforts related to its activities. In its role as the National Coordinator for Critical Infrastructure, as designated by National Security Memorandum 22 (NSM-22), it leads efforts to reduce cyber and physical risks to critical infrastructure. Through coordination and consultation with public and private sector partners, CISA works to secure critical infrastructure amidst an evolving threat environment, serves as a hub for bidirectional information sharing, and provides support services for targeted entities.

For further analysis of ongoing national security efforts and Committee policy recommendations to strengthen homeland security amid the modern threat landscape, see Section IV(d): *Policy Recommendations*.

COMMITTEE ACTIVITY EXAMINING U.S. NATIONAL SECURITY 25 YEARS POST- 9/11/01

Committee Activity Examining U.S. National Security 25 Years Post-9/11/01

The Committee held numerous hearings, briefings, and site visits throughout the 119th Congress to better inform its assessment of the current state of homeland security twenty-five years post-9/11/01. Committee activity that supported this objective is as follows:

Full Committee

Hearing: "Unconstrained Actors: Assessing Global Cyber Threats to the Homeland"

On January 22, 2025, the Committee held a hearing titled, "Unconstrained Actors: Assessing Global Cyber Threats to the Homeland." The Committee received testimony from Mr. Adam Meyers, Senior Vice President of Counter Adversary Operations at CrowdStrike; Rear Admiral Mark Montgomery, United States Navy (Ret.), Senior Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies; Mr. Brandon Wales, Vice President of Cybersecurity Strategy at SentinelOne; and Ms. Kemba Walden, President of the Paladin Global Institute, who testified as a private citizen.

The hearing covered an overview of current and emerging cyber threats and examined risks posed to critical infrastructure by nation-state actors, trends in ransomware attacks, and the increased use of AI in conducting cyber operations. In assessing the public-private partnerships utilized in addressing these threats, Members discussed the ability of private entities to combat increasingly sophisticated cyber threats and the role of CISA as an effective partner in those efforts.

Hearing: "Preparing the Pipeline: Examining the State of America's Cyber Workforce"

On February 5, 2025, the Committee held a hearing titled, "Preparing the Pipeline: Examining the State of America's Cyber Workforce." Testimony was received from Mr. David J. Russomanno, PhD, Executive Vice President of Academic Affairs and Provost at the University of Memphis; Mr. Robert Rashotte, Vice President of Global Training and Technical Field Enablement at Fortinet; Mr. Chris Jones, President and Chief Executive Officer of Middle Tennessee Electric Membership Corporation; and Mr. Max Stier, President and Chief Executive Officer of Partnership for Public Service.

The hearing provided Members with an opportunity to discuss the cyber workforce gap and the vulnerability of U.S. networks and infrastructure in light of the limited talent pool. Members discussed ongoing efforts of public and private entities to address the workforce challenge but also emphasized that a new approach may be necessary.

Hearing: "Innovation Nation: Leveraging Technology to Secure Cyberspace and Streamline Compliance"

On May 28, 2025, the Committee held a field hearing at Stanford University titled, "Innovation Nation: Leveraging Technology to Secure Cyberspace and Streamline Compliance." Testimony was received from the Honorable Herbert Raymond "H.R." McMaster, Fouad and Michelle Ajami Senior Fellow at the Hoover Institution; Ms. Wendi Whitmore, Chief Security Intelligence Officer at Palo Alto Networks; Ms. Jeanette Manfra,

Global Director of Security and Compliance at Google Cloud; and Mr. Jack Cable, Chief Executive Officer and Co-Founder of Corridor.

The hearing examined how automation, artificial intelligence, and other emerging technologies can improve cyber defense, reduce administrative burdens, and help organizations make better use of limited personnel. Members also assessed how overlapping regulatory requirements can divert security teams away from operational defense without producing a corresponding reduction in risk. The discussion reinforced the need for requirements that are consistent, risk-based, and focused on measurable security outcomes.

Member Briefing: Scattered Spider

On September 9, 2025, the Committee held a briefing with experts from CISA and the FBI on the cybersecurity threat posed by Scattered Spider, a cybercriminal ransomware group made up of individuals in gaming communities rather than state-sponsored operatives. Members heard about the tactics, techniques, and procedures (TTPs) of Scattered Spider, including social engineering, phone-based credential theft, abuse of legitimate remote access tools, cloud environment lateral movement, and data exfiltration, as well as the industries the group typically targets, such as technology, telecommunications, financial services, and more.

Member Briefing: PRC Cyber Threats

On November 18, 2025, the Committee received a briefing from General Paul M. Nakasone, U.S. Army (Ret.), and Former Director of the National Security Agency, on the evolution of the PRC's cyber strategy. The discussion examined the PRC's progression from large-scale espionage and intellectual property theft toward campaigns designed to establish persistent access inside U.S. networks, support broader intelligence objectives, and prepare for potential disruption during a future crisis or conflict.

Members examined the Volt Typhoon and Salt Typhoon campaigns, the use of "living off the land" techniques, and other PRC-attributed or suspected activity. The briefing highlighted how PRC actors increasingly rely on valid credentials, compromised routers, trusted administrative tools, and legitimate system functions to reduce the likelihood of detection and remain inside networks for extended periods. Members also considered how these methods complicate attribution, incident response, and efforts to determine whether an intrusion is intended for espionage, operational preparation, or both.

Hearing: "Worldwide Threats to the Homeland"

On December 11, 2025, the Committee held a hearing titled, "Worldwide Threats to the Homeland." The Committee received testimony from the Honorable Kristi Noem, Secretary, U.S. Department of Homeland Security; the Honorable Joe Kent, Director, National Counterterrorism Center, Office of the Director of National Intelligence; and Mr. Michael Glasheen, Operations Director, National Security Branch, Federal Bureau of Investigation.

The hearing provided Members the opportunity to examine the scale, scope, and pace of threats posed to the homeland by nation state and non-state actors. Members considered how terrorist groups have sought to exploit vulnerabilities along the Southwest border to enter the homeland, the resurgence of homeland threats posed by terrorist groups and violent extremists

leveraging emerging technologies including unmanned aircraft systems (UAS) and AI, and the increasing cyber threat to U.S. critical infrastructure. The hearing discussed the dynamic nature of threats to the homeland as terrorist groups adapt their tactics and techniques, offering insights to inform resource prioritization and investments consistent with today's threat environment.

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

On January 21, 2026, the Committee on Homeland Security held a hearing titled, "Oversight of the Department of Homeland Security: CISA, TSA, S&T." The Committee received testimony from the following witnesses: Dr. Madhu Gottumukkala, Acting Director, Cybersecurity and Infrastructure Security Agency; Ms. Ha Nguyen McNeill, Senior Official Performing the Duties of the Administrator, Transportation Security Administration; and the Honorable Pedro Allende, Under Secretary, Science & Technology Directorate.

The Committee examined DHS efforts to address evolving homeland security threats through the capabilities of CISA, TSA, and S&T, with particular attention to modernization, technology adoption, and operational readiness. For TSA, the hearing highlighted the need to advance aviation security through innovation, improved screening capabilities, and integration of emerging technologies while ensuring coordination with cybersecurity and intelligence partners.

Classified Member Briefing: PRC Typhoon Campaigns

On February 4, 2026, the Committee held a classified briefing with CISA and the FBI on the PRC's Typhoon cluster of cyber campaigns. Senior officials provided updates on Volt Typhoon, Salt Typhoon, and related activity affecting U.S. critical infrastructure and telecommunications networks. The briefing gave Members additional insight into the scope of the campaigns, their likely objectives, and the challenges involved in identifying and removing sophisticated actors from complex network environments. These briefings reinforced that PRC cyber activity is not limited to the theft of information. The PRC is seeking access that could provide intelligence value in the near term and strategic leverage in the future.

The Committee has also examined the distinct threats posed by Russia, Iran, and North Korea. Each actor differs in capability, intent, tolerance for risk, and reliance on criminal or proxy activity. Russia has demonstrated a willingness to combine cyber operations with military and influence objectives. Iran has repeatedly targeted critical infrastructure and other civilian systems, often through less sophisticated but disruptive activity. North Korea uses cyber operations to generate revenue, steal sensitive information, and support the regime's weapons programs. Understanding these differences is necessary to ensure that U.S. defenses, intelligence collection, and response options are tailored to the behavior of the specific adversary.

Hearing: "Before the Whistle: Assessing Information Sharing and Security Collaboration Ahead of Major Events"

On February 24, 2026, the Committee held a hearing titled, "Before the Whistle: Assessing Information Sharing and Security Collaboration Ahead of Major Events." The Committee received testimony from Mr. Mike Sena, President, National Fusion Center Association; Mr. Raymond A. Martinez, Chief Operating Officer, FIFA World Cup 2026 Miami Host Committee (Testified Remotely by the Authority of the Majority Leader); Mr. Joseph

Mabin, Deputy Chief, Kansas City Missouri Police Department; and Mr. Travis Nelson, Deputy Chief of Staff and Homeland Security Advisor, Office of the Governor, State of Maryland.

The hearing examined the operational and strategic considerations involved in the collection, analysis, and sharing of information among federal, state, local, tribal, territorial, and private sector partners. Members assessed how existing information sharing frameworks supported public safety, situational awareness, and coordinated decision-making across multiple jurisdictions and identified best practices, current challenges, and gaps in information sharing capabilities in advance of the 2026 FIFA World Cup and other major events. Further, the Committee conducted congressional oversight of information sharing efforts related to National Special Security Events (NSSEs) and Special Event Assessment Rating (SEAR) events to strengthen preparedness and interagency coordination.

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

On March 25, 2026, the Committee on Homeland Security held a hearing titled, "Funding Lapse and Security Gaps: Assessing the Harmful Impacts of the DHS Shutdown on Americans." The Committee received testimony from the following witnesses: Admiral Thomas Allan, Vice Commandant, U.S. Coast Guard; Ms. Ha Nguyen McNeill, Senior Official Performing the Duties of the Administrator, Transportation Security Administration; Mr. Nicholas Andersen, Acting Director and Deputy Director, Cybersecurity and Infrastructure Security Agency; and Ms. Victoria Barton, Associate Administrator, Office of External Affairs, Federal Emergency Management Agency.

The Committee assessed how disruptions to DHS operations affect the continuity and effectiveness of critical homeland security missions, including TSA aviation security operations. The hearing underscored that transportation security is a continuous mission requiring reliable funding, not only for TSA but for all DHS components who protect against evolving threats to the homeland, especially critical infrastructure.

Event: "Demo Day: Jailbreaking AI in Real Time"

On April 22, 2026, the Committee held a demonstration in collaboration with the National Counterterrorism Innovation, Technology, and Education Center (NCITE), a DHS Center of Excellence. NCITE's work on terrorist and violent extremist use of emerging technologies has identified that these actors are turning to unconstrained AI models to research and plan acts of violence. During this demonstration, Members had the opportunity to engage with "jailbroken" AI models, demonstrating the dangers and risks of this new frontier.

Hearing: "TSA Modernization: Industry Perspectives on Key Security and Travel Reforms 25 Years After 9/11"

On May 20, 2026, the Committee on Homeland Security held a hearing titled, "TSA Modernization: Industry Perspectives on Key Security and Travel Reforms 25 Years After 9/11." The Committee received testimony from the following witnesses: Mr. Christopher T. Sununu, President and Chief Executive Officer, Airlines for America; Mr. Chris McLaughlin, Chief Executive Officer, Dallas Fort Worth International Airport; and Dr. Everett Kelley, National President, American Federation of Government Employees.

The Committee examined TSA's evolution 25 years after 9/11 and received perspectives from representatives of airlines, airport operators, and TSA employees on the future of aviation security. The discussion focused on modernizing TSA through risk-based security, advanced screening technologies, improved passenger experience, cybersecurity protections, and workforce investments necessary to address the next generation of threats.

Hearing: "A Review of the Fiscal Year 2027 Budget Request for DHS"

On June 3, 2026, the Committee on Homeland Security held a hearing titled, "A Review of the Fiscal Year 2027 Budget Request for DHS." The Committee received testimony from the following witnesses: the Honorable Markwayne Mullin, Secretary, Department of Homeland Security; and the Honorable Troy Edgar, Deputy Secretary, Department of Homeland Security.

The Committee reviewed DHS's funding priorities for FY 2027 and assessed whether proposed investments align with the modern threat environment, including aviation security and technology modernization. For TSA, the hearing provided insight into the resources needed to sustain operations, deploy new capabilities, and maintain a highly trained workforce capable of adapting to emerging risks.

Event: "25 Years Later: A Demonstration of Innovation in the Aftermath of 9/11"

On September 1, 2026, the Committee held a large-scale event featuring an array of interactive demonstrations to highlight the Department of Homeland Security's modernization and developments of security capabilities in the 25 years following the terrorist attacks of September 11, 2001. Events included live showcases of virtual reality training conducted with the Federal Protective Service (FPS) and "jailbroken" AI in collaboration with the National Counterterrorism Innovation, Technology, and Education Center (NCITE), a DHS Center of Excellence. The event also included unmanned aircraft system displays and K9 unit demonstrations from across the Department, including from the Federal Emergency Management Agency, Customs and Border Protection, Federal Protective Service, U.S. Coast Guard, U.S. Secret Service, Science & Technology Directorate, and Transportation Security Administration.

Artificial Intelligence and National Security Roundtable Series

The Committee held its first AI and national security roundtable with industry leaders on March 18, 2026. Members examined the growing use of AI in cyber and intelligence operations, including the PRC's efforts to accelerate domestic AI development and acquire American capabilities through illicit means. The discussion also addressed Anthropic's November 2025 disclosure that it had disrupted an AI-orchestrated cyber espionage campaign linked to a PRC-sponsored actor. That incident gave Members a practical example of how AI can reduce the amount of human involvement required to conduct portions of a cyber operation and increase the speed at which an actor can move from reconnaissance to execution.

On April 16, 2026, the Committee held its second AI and national security roundtable. The roundtable examined agentic AI, Anthropic's Mythos Preview and Project Glasswing, and the use of AI to support DHS operations. Members considered how advanced models could assist with threat analysis, vulnerability management, incident response, and other resource-intensive missions. They also examined the risks associated

with granting AI systems access to tools, networks, sensitive data, or the ability to take actions with limited human approval.

A significant portion of the discussion focused on competition between the United States and the PRC. Members examined adversarial model distillation and other methods used to extract capabilities from American AI systems. These practices allow foreign companies to benefit from U.S. investment and research while reducing the time and cost required to develop competing systems. They can also result in the distribution of advanced capabilities through models that do not retain the safeguards adopted by the original developer.

On May 13, 2026, the Committee received a briefing from Anthropic on the capabilities of its Mythos Preview model and the company's approach to testing and deployment. Dr. Logan Graham, Department Head of Anthropic's Frontier Red Team, demonstrated the model during a simulated cyberattack and defensive patching exercise. The demonstration allowed Members to assess the operational implications of advanced cyber capable models. The same model that can identify a vulnerability and generate a patch may also be able to identify an avenue of attack and develop exploit code. Members examined the safeguards, access controls, testing, monitoring, and release practices needed to manage this dual-use capability. The briefing also raised questions about whether CISA and critical infrastructure operators are prepared for an environment in which vulnerability discovery, exploitation, and remediation occur at far greater speed.

On June 9, 2026, the Committee held its third AI and national security roundtable. Members focused on the effect of advanced AI capabilities on smaller and less resourced critical infrastructure entities, including rural hospitals, municipal water systems, and local governments. The discussion emphasized that the benefits of AI-assisted defense will not be shared equally unless effective tools are made available to organizations that lack large security teams. At the same time, greater access to offensive capabilities may allow criminals and foreign actors to target those organizations more efficiently.

The roundtable also examined threats to American frontier AI laboratories, including cyber intrusion, insider risk, model theft, and adversarial distillation. Foreign actors that obtain proprietary U.S. capabilities can weaken the competitive position of American companies and accelerate the development of systems that may later be used against U.S. interests.

Joint Investigation: PRC Open-weight AI Models

In parallel with the roundtable series, the Committee launched a joint investigation with the House Select Committee on the Chinese Communist Party into the national security and cybersecurity risks associated with the adoption of PRC open-weight AI models. The investigation has focused on how American companies evaluate foreign-developed models before incorporating them into products or services. Relevant considerations include who developed the model, how it was trained, what capabilities it contains, what data it can access, what software dependencies it requires, whether it communicates with external systems, how it is updated, and whether its behavior can be independently tested.

The use of PRC open-weight models raises concerns that cannot be resolved solely by hosting a model in a local environment. Local deployment may reduce some forms of external data exposure, but it does not address questions involving model provenance, training methods, embedded functionality, software dependencies, update mechanisms, or the legal obligations of the developer. These issues become more significant when the model is used in sensitive systems or integrated into products relied upon by U.S. companies, government agencies, or critical infrastructure operators.

The Committee's work has also examined the strategic effect of the PRC's efforts to obtain American capabilities through distillation, incorporate those capabilities into widely available models, and encourage global adoption. Over time, broad reliance on PRC-origin models could create security dependencies, weaken trusted U.S. alternatives, and provide the PRC with greater influence over the technologies used in commercial and sensitive environments.

Through its roundtables, briefings, and joint investigation, the Committee has sought to move beyond general debates about whether AI is beneficial or dangerous. Its focus has been on how advanced capabilities are developed, secured, deployed, accessed, and integrated into real systems. That work has informed the Committee's examination of AI-enabled cyber operations, the protection of frontier AI laboratories, the responsibilities of CISA, and the risks associated with foreign-developed models.

Subcommittee on Counterterrorism and Intelligence

Hearing: "The Digital Battlefield: How Terrorists Use the Internet and Online Networks for Recruitment and Radicalization"

On March 4, 2025, the Subcommittee held a hearing titled, "The Digital Battlefield: How Terrorists Use the Internet and Online Networks for Recruitment and Radicalization." The Subcommittee received testimony from Daveed Gartenstein-Ross, Ph.D., Senior Advisor on Asymmetric Warfare, Foundation for Defense of Democracies; Aaron Zelin, Ph.D., Senior Research Fellow, The Washington Institute for Near East Policy; Mr. Daniel Flesch, Senior Policy Analyst, Middle East and North Africa, Allison Center for National Security, The Heritage Foundation, who testified as a private citizen; and Kurt Braddock, Ph.D., Assistant Professor, Public Communication, American University, who testified as a private citizen.

The hearing examined national security threats posed by terrorist groups such as ISIS and Hamas and emerging methods used by these groups to radicalize, recruit, and mobilize followers to commit violent acts against Americans. Committee Members assessed how emerging technologies like generative artificial intelligence (GenAI) could be exploited by terrorist networks and explored solutions to ensure law enforcement agencies were prepared with the necessary tools to combat the threats posed by online radicalization.

Hearing: "The Rise of Anti-Israel Extremist Groups and Their Threat to U.S. National Security"

On June 11, 2025, the Subcommittee held a hearing titled, "The Rise of Anti-Israel Extremist Groups and Their Threat to U.S. National Security." The Subcommittee received testimony from Mr. Kerry Sleeper, Deputy Director of Intelligence and Information Sharing, Secure Community Network; Mr. Oren Segal, Senior Vice President of Counter-Extremism and

Intelligence, Anti-Defamation League; and James Jay Carafano, Ph.D., E.W. Richardson Fellow, The Heritage Foundation, who testified as a private citizen.

The hearing examined the growing threat of antisemitism within the United States and assessed the adequacy of current counterterrorism measures in addressing the threat of antisemitic violence targeting Jewish Americans and foreign diplomats on U.S. soil. Members questioned policy gaps and entertained recommendations for strengthening federal, state, local, and tribal law enforcement coordination against hate-motivated violence and explored the rapid rates at which antisemitic incidents were increasing.

Member Briefing: "Outpaced and Outdated: Addressing the Definitional Discrepancies, Implementation Gaps, and Resource Constraints Hindering U.S. Efforts to Combat Domestic Terrorism"

On December 18, 2025, the Subcommittee held a roundtable to consider challenges related to U.S. efforts to combat domestic terrorism. Despite a rapid uptick in domestic terrorism cases, the U.S. has historically lacked a cohesive national strategy to guide the federal response and the statutory definition for domestic terrorism does not match the current threat environment or the pace of digital adaptation. The roundtable discussion examined the need for a national strategy, ways to modernize existing definitions, and the importance of unity of effort across jurisdictions and law enforcement stakeholders.

The roundtable included representatives from the Center for Internet Security; Independent Women; the U.S. Government Accountability Office; the National Counterterrorism Innovation, Technology, and Education Center; the Center for Strategic and International Studies; Major County Sheriffs of America; and the Council on Foreign Relations.

Classified Member Briefing: DHS Office of Intelligence & Analysis

On Wednesday, January 14, 2026, the Subcommittee held a classified briefing with the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A). Senior leadership from I&A provided Members with an overview of the office, including its field-based presence and unique statutory authorities to share intelligence with SLTT partners. Members additionally considered the role that I&A plays in sharing information ahead of events of national significance, such as National Special Security Events (NSSEs) and those with a Special Event Assessment Rating (SEAR).

Site Visit: United States Secret Service Accelerated Candidate Event

On February 27, 2026, Committee staff observed a United States Secret Service (USSS) Accelerated Candidate Event (ACE). As threats to U.S. officials, facilities, and major events continue to increase, the need for additional federal law enforcement personnel increases in tandem. The ACE model was designed to streamline the USSS hiring process, by consolidating several stages of the process into a multiday event without compromising hiring standards. Strengthening the federal law enforcement workforce enhances the ability of federal government to secure mass gathering events against acts of terrorism and extremist violence.

Classified Member Briefing: United States Secret Service

On March 24, 2026, the Subcommittee held a classified briefing with the United States Secret Service (USSS) to examine threats to U.S. telecommunications systems posed by threat

actors including terrorist organizations. The briefing considered investigatory challenges, the importance of coordination with private sector partners, and ways to enhance resiliency of U.S. communication networks.

Member Briefing: "Partnership in Action: A Roundtable Focused on DHS's Coordination with Law Enforcement"

On May 14, 2026, the Subcommittee led a roundtable focused on DHS cooperation with state, local, tribal, territorial, and private sector partners. The roundtable highlighted the coordination, operational interdependence, and strategic importance of coordination across the spectrum of law enforcement stakeholders. Members considered how joint information sharing, intelligence integration, and grant funding collectively enhance national preparedness, situational awareness, and response capabilities across all levels of government.

The discussion included representatives from the Association of State Criminal Investigative Agencies, Major Country Sheriffs of America; the National Fusion Center Association; the Federal Law Enforcement Officers Association; the National Sheriffs' Association; the Major Cities Chiefs Association; the Small & Rural Law Enforcement Executives Association; Secure Community Network; the Jewish Federations of North America; and the DHS Office of Intelligence & Analysis.

Classified Member Briefing: Nihilistic Violent Extremism

On June 25, 2026, the Subcommittee held a classified briefing with representatives from Homeland Security Investigations (HSI) and the FBI on threats posed by nihilistic violent extremist (NVE) groups. Unlike domestic and foreign terrorist threats, NVEs lack a clear ideology and are instead driven to create destruction and chaos, motivated by a deep hatred for society. NVE groups have emerged quickly, primarily operating on encrypted messaging and gaming platforms. Briefers provided Members with an overview of the NVE landscape, including the challenges associated with investigating, disrupting, and prosecuting violent acts linked to these groups.

Site Visit: International Police Coordination Center

On July 7, 2026, Committee staff visited the International Police Coordination Center (IPCC) stood up to coordinate real-time law enforcement information sharing and threat assessments for the 2026 FIFA World Cup. The IPCC included representatives from over forty countries in addition to FIFA and every FIFA World Cup host city, providing an effective showcase for partnership between law enforcement and private sector stakeholders in securing major events. The IPCC concept developed in the U.S. for the FIFA World Cup will serve as a model for future events hosted in the U.S., including the 2028 Summer Olympics and Paralympics in Los Angeles.

Subcommittee on Transportation and Maritime Security

Hearing: "Examining the PRC's Strategic Port Investments in the Western Hemisphere and the Implications for Homeland Security"

On February 11, 2025, the Subcommittee held a hearing titled, "Examining the PRC's Strategic Port Investments in the Western Hemisphere and the Implications for Homeland

Security." The Subcommittee received testimony from the following witnesses: Dr. Isaac Kardon, Senior Fellow, Carnegie Endowment for International Peace; Dr. Matthew Kroenig, Vice President and Senior Director of the Scowcroft Center for Strategy and Security of the Atlantic Council; Dr. Ryan C. Berg, Director of the Americas Program, Center for Strategic and International Studies; and Mr. Cary Davis, President and Chief Executive Officer of the American Association of Port Authorities.

Building on the 9/11 Commission's emphasis on protecting transportation systems, this hearing brought renewed attention to policies that strengthen port security, enhance interagency coordination, and address national security risks posed by foreign ownership and influence over critical infrastructure.

Hearing: "America on the Global Stage: Examining Efforts to Secure and Improve the U.S. Travel System and Prepare for Significant International Events"

On April 8, 2025, the Subcommittee held a hearing titled, "America on the Global Stage: Examining Efforts to Secure and Improve the U.S. Travel System and Prepare for Significant International Events." The Subcommittee received testimony from the following witnesses: Mr. Geoff Freeman, President and Chief Executive Officer, U.S. Travel Association; Mr. Jon Gruen, Chief Executive Officer, Fortem Technologies; and Dr. Everett Kelley, National President, American Federation of Government Employees.

This hearing reinforced the importance of maintaining a secure and resilient travel system while preparing for major international events amidst heightened security risks. Members considered policies to improve traveler screening and workforce readiness, as well as coordination between federal, state, local, and private sector partners to secure major events.

Hearing: "Beijing's Air, Space, and Maritime Surveillance from Cuba: A Growing Threat to the Homeland"

On May 6, 2025, the Subcommittee held a hearing titled, "Beijing's Air, Space, and Maritime Surveillance from Cuba: A Growing Threat to the Homeland." The Subcommittee received testimony from the following witnesses: Dr. Ryan C. Berg, Director, Americas Program, Center for Strategic and International Studies; Mr. Andres Martinez-Fernandez, Senior Policy Analyst, Allison Center for National Security; and Mr. Leland Lazarus, Associate Director, National Security Program, Gordon Institute for Public Policy, Florida International University.

This hearing assessed how foreign surveillance capabilities positioned close to the United States could challenge homeland security through enhanced intelligence collection and strategic competition. Consistent with the 9/11 Commission's focus on intelligence integration and identifying emerging threats before they materialize, the hearing highlighted policy considerations to strengthen domain awareness and enhancing coordination to detect and respond to adversarial activities that threaten the homeland.

Hearing: "From Cartels to Coastlines: An Examination of U.S. Federal Efforts to Confront Illicit Maritime Activities in U.S. Waters"

On June 10, 2025, the Subcommittees on Transportation and Maritime Security and Border Security and Enforcement held a hearing titled, "From Cartels to Coastlines: An Examination of U.S. Federal Efforts to Confront Illicit Maritime Activities in U.S. Waters." The

Subcommittees received testimony from the following witnesses: Rear Admiral Adam A. Chamie, Assistant Commandant for Response Policy, U.S. Coast Guard; Mr. James C. Harris, III, Assistant Director, Countering Transnational Organized Crime (CTOC), Homeland Security Investigations (HSI); Mr. Jonathan P. Miller, Executive Assistant Commissioner, Air and Marine Operations, U.S. Customs and Border Protection; and Ms. Heather MacLeod, Director, Homeland Security and Justice, U.S. Government Accountability Office (GAO).

This hearing examined the evolving threat posed by transnational criminal organizations operating in the maritime domain, including narcotics trafficking, human smuggling, and other illicit activities that threaten homeland security. Specifically, the hearing built on the 9/11 Commission's recommendations to improve border security and interagency coordination, underscoring the need to strengthen maritime domain awareness, as well as operational capabilities across U.S. inland waterways.

Hearing: "Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home"

On July 15, 2025, the Subcommittee held a hearing titled, "Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home." The Subcommittee received testimony from the following witnesses: Mr. Tom Walker, Founder and Chief Executive Officer, DroneUp, LLC; Mr. Brett Feddersen, Vice President, Strategy & Government Affairs, D-Fend Solutions; Mr. Church Hutton, Chief Growth Officer, AeroViroment, Inc.; and Mr. Michael Robbins, President and Chief Executive Officer, Association for Uncrewed Vehicle Systems International (AUVSI).

In line with the 9/11 Commission's emphasis on anticipating emerging threats and adapting security capabilities, this hearing explored how the proliferation of unmanned aircraft systems (UAS) across the globe – especially in conflicts in Ukraine and the Middle East – is reshaping the threat environment in the homeland. The hearing emphasized UAS risks to critical infrastructure, major events in the United States, and transportation systems.

Hearing: "Securing Global Communications: An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure."

On November 25, 2025, the Subcommittee on Transportation and Maritime Security and the Subcommittee on Cybersecurity and Infrastructure Protection held a joint hearing titled "Securing Global Communications: An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure." The Subcommittees received testimony from the following witnesses: Mr. Timothy Stronge, Chief Research Officer, TeleGeography; Mr. Alexander Botting, Senior Director, Global Security and Technology Strategy, Venable LLP; Mr. Matthew Kroenig, Senior Director, Scowcroft Center for Strategy and Security, Atlantic Council; and Mr. Kevin Frazier, AI Innovation and Law Fellow, University of Texas School of Law.

The hearing examined potential national security and economic risks associated with subsea cables as a crucial communications infrastructure. Members were able to evaluate key vulnerabilities stemming from foreign ownership, private-sector control, and chokepoints surrounding U.S. and allied territories. Finally, members were able to hear legislative proposals for strengthening subsea cable resilience, enhancing public-private partnerships, and ensuring continuity of global communications amid cyber or physical disruptions.

Hearing: "Frontline Defenders: How the Coast Guard's Deployable Specialized Forces Combat Narcoterrorists and other Maritime Threats on the High Seas."

On February 3, 2026, the Subcommittee held a hearing titled "Frontline Defenders: How the Coast Guard's Deployable Specialized Forces Combat Narcoterrorists and other Maritime Threats on the High Seas." Members heard testimony from the following witnesses: Rear Admiral David C. Barata, Deputy Commandant for Operation's Policy and Capabilities, U.S. Coast Guard; and Ms. Heather MacLeod, Director, Homeland Security and Justice Team, U.S. Government Accountability Office.

This hearing examined the readiness and capabilities of the U.S. Coast Guard's Deployable Specialized Forces (DSF), reviewed recent interdiction operations off the coast of Venezuela, and assessed how new trafficking tactics utilized by cartels and other transnational criminal organizations challenge DSF units. Finally, the U.S. Coast Guard proposed a plan for a new DSF command to improve readiness and rapid response against evolving threats.

Site Visit: DCA TSA Systems Integration Facility

On July 23, 2026, the Subcommittee on Transportation and Maritime Security conducted a site visit to TSIF located at Ronald Reagan Washington National Airport (DCA) in Arlington, Virginia. TSIF is TSA's primary facility for testing and integrating new security technologies before nationwide deployment. The visit informed TSA modernization legislation by providing Members with a firsthand understanding of TSA technology deployment, including the importance of rigorous testing, system interoperability, cybersecurity safeguards, artificial intelligence integration, and human factors analysis.

Subcommittee on Cybersecurity and Infrastructure Protection

Hearing: "Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime"

On March 11, 2025, the Subcommittee held a hearing titled, "Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime." The Subcommittee received testimony from Mr. Scott Aaronson, Senior Vice President of Energy Security and Industry Operations at the Edison Electric Institute; Ms. Heather Hogsett, Senior Vice President and Deputy Head of BITS at the Bank Policy Institute; Mr. Robert Mayer, Senior Vice President of Cybersecurity and Innovation at USTelecom, The Broadband Association; and Mr. Ari Schwartz, Coordinator at the Cybersecurity Coalition.

The hearing examined CISA's proposed rule implementing the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA) and the broader challenge created by overlapping Federal and state cyber requirements. Members considered whether the proposed reporting framework would provide CISA with timely and useful information without imposing unnecessary burdens on entities already subject to multiple reporting regimes. Witnesses described how inconsistent definitions, deadlines, thresholds, formats, and submission processes can require companies to prepare multiple reports concerning the same incident. These obligations can consume the time of legal, compliance, and security personnel during the period when those employees are most needed to contain the intrusion, restore operations, and protect affected systems.

Members examined and gained a better understanding of how Congress and the Executive Branch can harmonize cyber requirements around common definitions, consistent timelines, reciprocal recognition, and risk-based outcomes. The objective is not to reduce meaningful security obligations, but to ensure that regulatory activity strengthens defense rather than displacing it.

Hearing: "Cybersecurity is Local, Too: Assessing the State and Local Cybersecurity Grant Program"

On April 1, 2025, the Subcommittee held a hearing titled, "Cybersecurity is Local, Too: Assessing the State and Local Cybersecurity Grant Program." The Subcommittee received testimony from Mr. Robert Huber, Chief Security Officer of Tenable, Inc.; Mr. Alan Fuller, Chief Information Officer of the State of Utah; the Honorable Kevin Kramer, First Vice President of the National League of Cities; and Mr. Mark Raymond, Chief Information Officer of the State of Connecticut.

The hearing assessed the early implementation of the State and Local Cybersecurity Grant Program and the extent to which the program has helped jurisdictions improve their security. Members examined how states and localities were using grant funding, whether the program was reaching smaller jurisdictions, and whether federal requirements were sufficiently flexible to account for differences in resources, governance, technology, and risk. Witnesses described the challenges faced by state and local governments, including legacy systems, limited staffing, competition for cybersecurity talent, uneven asset visibility, and dependence on third-party providers. These entities collect sensitive information and operate services that directly affect public safety, yet many lack the funding and personnel needed to maintain mature security programs.

The hearing also examined whether the program was encouraging durable improvements or supporting short-term purchases that jurisdictions might be unable to sustain after Federal funding ends. Members considered the value of shared services, statewide security operations, common procurement, regional partnerships, and investments that allow smaller jurisdictions to benefit from capabilities they could not afford independently.

Hearing: "In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities that Underpin U.S. National Cyber Defense"

On May 15, 2025, the Subcommittee held a hearing titled, "In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities that Underpin U.S. National Cyber Defense." The Subcommittee received testimony from Mr. John Miller, Senior Vice President of Policy for Trust, Data, and Technology and General Counsel at the Information Technology Industry Council; Ms. Diane Rinaldo, Executive Director of the Open RAN Policy Coalition, who testified in her personal capacity; Mr. Karl Schimmeck, Executive Vice President and Chief Information Security Officer of Northern Trust; and Ms. Kate Kuehn, Member and CISO-in-Residence of the National Technology Security Coalition.

The hearing examined the *Cybersecurity Information Sharing Act of 2015* and the legal protections that allow companies to share cyber threat indicators and defensive

measures with the federal government and one another. Members considered how liability protection, antitrust protection, privacy safeguards, and protections from public disclosure influence a company's willingness to share information during an incident. Witnesses emphasized that information sharing is most valuable when it occurs quickly and includes details that another defender can use. Indicators that arrive after an intrusion has concluded, or that lack sufficient technical and operational context, provide limited defensive benefit. Members examined both the statutory framework and the processes through which information is received, analyzed, enriched, and returned to industry.

The hearing also considered the consequences of allowing the authorities to expire. Uncertainty regarding liability and permitted sharing could cause companies to reduce participation, delay disclosures, or rely on narrower private arrangements. The Subcommittee's work supported reauthorization efforts while also examining how implementation could be improved to produce faster, more relevant, and more reciprocal exchanges of information.

Hearing: "Security to Model: Securing Artificial Intelligence to Strengthen Cybersecurity"

On June 12, 2025, the Subcommittee held a hearing titled, "Security to Model: Securing Artificial Intelligence to Strengthen Cybersecurity." The Subcommittee received testimony from Mr. Kiran Chinnagangannagari, Co-Founder and Chief Product and Technology Officer of Securin Inc.; Mr. Steve Faehl, U.S. Government Security Leader at Microsoft; Mr. Gareth Maclachlan, Chief Product Officer at Trellix; and Mr. Jonathan Dambrot, Chief Executive Officer of Cranium AI, Inc.

The hearing examined the dual role of AI in cybersecurity. Members considered how AI can help defenders analyze large amounts of data, identify suspicious activity, prioritize vulnerabilities, support compliance, and automate repetitive tasks. They also examined how the same capabilities can improve social engineering, vulnerability discovery, malicious code development, reconnaissance, and other stages of an attack.

The hearing placed particular emphasis on the security of AI systems themselves. Members considered risks involving training data, model access, software dependencies, plugins, application programming interfaces, cloud environments, and the broader development lifecycle. The discussion reinforced that AI tools used for sensitive or security-relevant functions must be designed, tested, monitored, and maintained with security as an initial requirement rather than an afterthought. Members also examined the application of secure-by-design principles to AI products. Developers are better positioned than end users to address many weaknesses involving default settings, access controls, logging, update practices, and misuse protections. The hearing established a foundation for the Subcommittee's later work on frontier models, agentic systems, AI coding tools, and foreign-developed models.

Hearing: "Fully Operational: Stuxnet 15 Years Later and the Evolution of Cyber Threats to Critical Infrastructure"

On July 22, 2025, the Subcommittee held a hearing titled, "Fully Operational: Stuxnet 15 Years Later and the Evolution of Cyber Threats to Critical Infrastructure." The Subcommittee received testimony from Ms. Kim Zetter, journalist and author of Countdown

to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon; Mr. Robert M. Lee, Chief Executive Officer and Co-Founder of Dragos, Inc.; Ms. Tatyana Bolton, Executive Director of the Operational Technology Cyber Coalition; and Nathaniel Gleason, Ph.D., Program Leader at Lawrence Livermore National Laboratory.

The hearing examined how threats to operational technology have evolved since the discovery of Stuxnet and whether the United States has made sufficient progress in securing the systems that control physical processes. Members considered the distinct challenges associated with industrial control systems, including long equipment lifecycles, limited opportunities for downtime, dependence on specialized vendors, remote access, insecure legacy technology, and the safety consequences of an operational failure.

The discussion also addressed nation-state campaigns, including Volt Typhoon, that seek access to infrastructure with potential value during a crisis or conflict. An effective response requires coordination among cybersecurity personnel, engineers, operators, vendors, and government agencies. The hearing also considered the role of the *Cybersecurity Information Sharing Act of 2015* and the State and Local Cybersecurity Grant Program in supporting critical infrastructure during periods of elevated geopolitical risk. Members assessed whether existing information sharing authorities, federal assistance programs, and operational partnerships are sufficient to reach the entities most likely to need support, including small utilities and state and local operators with limited in-house expertise.

Hearing: "The Quantum, AI, and Cloud Landscape: Examining Opportunities, Vulnerabilities, and the Future of Cybersecurity"

On December 17, 2025, the Subcommittee held a joint hearing with the Subcommittee on Oversight, Investigations, and Accountability titled, "The Quantum, AI, and Cloud Landscape: Examining Opportunities, Vulnerabilities, and the Future of Cybersecurity." The Subcommittees received testimony from Logan Graham, Ph.D., Department Head of the Frontier Red Team at Anthropic PBC; Mr. Royal Hansen, Vice President of Privacy, Safety, and Security Engineering at Google LLC; Mr. Eddy Zervigon, Chief Executive Officer of Quantum Xchange; and Mr. Michael Coates, Founding Partner at Seven Hill Ventures.

The hearing examined how developments in artificial intelligence, quantum computing, and cloud infrastructure are changing the security of government and critical infrastructure systems. Members considered the benefits created by advanced computing capabilities as well as the new dependencies and concentrations of risk that accompany their adoption. The discussion addressed whether cloud and technology providers maintain appropriate safeguards for platforms used to store sensitive data, operate essential functions, and deploy advanced models. Members examined identity and access controls, software supply chains, insider risk, logging, incident response, and the consequences of a compromise affecting a widely used provider.

The hearing also addressed the transition to post-quantum cryptography. Members considered the threat posed by adversaries that collect encrypted information today with the expectation that future quantum capabilities may allow them to decrypt it. The discussion emphasized that migration requires an inventory of cryptographic dependencies, updated standards, vendor coordination, procurement planning, and sustained implementation across

complex systems. Delay can leave sensitive information exposed long before a cryptographically relevant quantum computer becomes available.

Hearing: "Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland"

On January 13, 2026, the Subcommittee held a hearing titled, "Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland." The Subcommittee received testimony from Joe Lin, Ph.D., Co-Founder and Chief Executive Officer of Twenty Technologies, Inc., who testified in his personal capacity; Ms. Emily Harding, Vice President of the Defense and Security Department at the Center for Strategic and International Studies, who testified in her personal capacity; Mr. Frank Cilluffo, Director of the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University; and Mr. Drew Bagley, Chief Privacy Officer of CrowdStrike.

The hearing examined whether existing U.S. cyber capabilities and authorities are being used effectively to deter malicious activity, disrupt active campaigns, and impose costs on foreign adversaries. Members considered the legal and policy frameworks governing offensive cyber operations, the respective roles of civilian, military, intelligence, and law enforcement agencies, and the circumstances in which private sector capabilities can support broader national objectives. The discussion also addressed the limits of deterrence in cyberspace, particularly when adversaries believe they can operate through proxies, criminal groups, compromised infrastructure, or activity that falls below the threshold of armed conflict.

Members assessed whether U.S. cyber strategy sufficiently connects defensive measures, intelligence collection, disruption operations, diplomatic action, sanctions, criminal indictments, and other instruments of national power. The hearing reinforced that offensive cyber activity is most effective when tied to clear objectives, coordinated across agencies, and integrated into a broader strategy rather than treated as a stand-alone response to individual incidents.

Member Briefing: DPRK Remote IT Workers

On March 5, 2026, the Subcommittee held a roundtable with representatives from Microsoft Corporation and Palo Alto Networks on fraudulent remote information technology workers operating on behalf of the Democratic People's Republic of Korea (DPRK). These schemes allow DPRK operatives to obtain employment with U.S. companies, collect wages, and generate revenue for the regime's weapons of mass destruction and ballistic missile programs. Members examined how DPRK operatives exploit remote hiring practices, stolen or fabricated identities, online employment platforms, artificial intelligence, remote access tools, and intermediaries located in the United States and abroad. The roundtable highlighted that the threat extends beyond fraudulent wage collection. Once hired, an operative may gain trusted access to source code, customer data, proprietary systems, credentials, and internal networks. That access can support theft, espionage, extortion, ransomware, or additional compromise.

The discussion also underscored the difficulty companies face in identifying applicants who appear technically qualified and pass conventional hiring checks but are operating under false identities or through concealed locations. Members considered the need for stronger identity verification, better coordination among technology companies, financial institutions, law enforcement, and employers, and greater awareness among companies that remote hiring can create a national security risk when verification and access controls are weak.

Hearing: "DeepSeek and Unitree Robotics: Examining the National Security Risks of PRC Artificial Intelligence, Robotics, and Autonomous Technologies and Building a Secure U.S. Technology Base"

On March 17, 2026, the Subcommittee held a hearing titled, "DeepSeek and Unitree Robotics: Examining the National Security Risks of PRC Artificial Intelligence, Robotics, and Autonomous Technologies and Building a Secure U.S. Technology Base." The Subcommittee received testimony from Mr. Max Fenkell, Global Head of Policy and Government Relations at Scale AI; Mr. Matthew Malchano, Vice President of Software at Boston Dynamics; Mr. Michael Robbins, President and Chief Executive Officer of the Association for Uncrewed Vehicle Systems International; and Rush Doshi, Ph.D., C.V. Starr Senior Fellow for Asia Studies and Director of the China Strategy Initiative at the Council on Foreign Relations.

The hearing examined the security and economic risks associated with the increasing adoption of PRC-developed artificial intelligence, robotics, and autonomous systems. Members considered how PRC companies benefit from access to American research, capital, data, semiconductors, software, and technical expertise, while operating within a legal and political system that can compel cooperation with the Chinese Communist Party and state security services. Members also examined the risks created when PRC-origin technologies are incorporated into U.S. products, government operations, research environments, or critical infrastructure. These risks include sensitive data collection, remote access, software dependencies, supply chain leverage, intellectual property loss, and the possibility that systems relied upon during routine operations could be manipulated, degraded, or denied during a period of heightened tension.

The hearing reinforced the need to evaluate technology according to more than price or performance. The origin of the developer, the security of the supply chain, the integrity of software and updates, the legal obligations of the manufacturer, and the availability of trusted alternatives are all relevant to national security. Members also considered how the United States can reduce dependence on PRC technology while supporting competitive American companies and preserving a strong domestic innovation base.

Hearing: "Data Centers, Telecommunications Networks, and Space-Based Systems: Modernizing DHS's SRMA Role for the Communications and IT Sectors"

On April 29, 2026, the Subcommittee held a hearing titled, "Data Centers, Telecommunications Networks, and Space-Based Systems: Modernizing DHS's SRMA Role for the Communications and IT Sectors." The Subcommittee received testimony from Mr. Robert Mayer, Senior Vice President of Cybersecurity and Innovation at USTelecom, The Broadband Association; Mr. Sam Visner, Chair of the Board of Directors at the Space

Information Sharing and Analysis Center; Rear Admiral Mark Montgomery, United States Navy, Retired, Senior Director and Senior Fellow at the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies; and Mr. Scott Algeier, Executive Director of the Information Technology Information Sharing and Analysis Center.

The hearing examined whether the existing critical infrastructure sector structure adequately reflects the systems on which the modern economy and national security enterprise depend. Members reviewed the role of hyperscale data centers, cloud computing environments, telecommunications networks, subsea cables, internet exchange points, space-based communications, and other infrastructure that supports services across multiple sectors. Many of these assets do not fit neatly within sector boundaries established years ago. A data center may support financial services, health care, energy, government operations, communications, and artificial intelligence workloads at the same time. A subsea cable or satellite system may carry traffic for numerous sectors and jurisdictions. Disruption to one provider can create consequences far beyond the entity directly affected.

Members assessed whether DHS is meeting its responsibilities as the Sector Risk Management Agency for the communications and information technology sectors and whether the current division of responsibilities provides sufficient accountability. The hearing examined DHS's ability to identify nationally significant assets, understand cross-sector dependencies, develop meaningful risk assessments, coordinate with other agencies, and provide owners and operators with support tailored to the threats they face.

Hearing: "State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities"

On May 21, 2026, the Subcommittee held a hearing titled, "State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities." The Subcommittee received testimony from Ms. Kristin Darby, Chief Information Officer of the State of Tennessee; Mr. Colin Ahern, Director of Security and Intelligence of the State of New York; Mr. Warren Sponholtz, Chief Information Officer of the State of Florida; and Mr. Samir Jain, Vice President of Policy at the Center for Democracy & Technology.

Held approximately one year after the Subcommittee's first hearing on the grant program, the hearing allowed Members to assess progress, identify remaining gaps, and evaluate the quality of federal support. Witnesses discussed the use of grant funding, statewide cyber services, threat intelligence, endpoint visibility, incident response, identity security, and other capabilities being deployed to protect public systems.

Members also examined persistent differences in capability among states and localities. Some states have developed mature cyber organizations and can provide services to local partners, while others remain constrained by staffing, procurement, technical debt, or fragmented governance. Smaller local governments may not have a dedicated cybersecurity employee and may struggle to apply for grants, procure technology, or interpret federal guidance without additional support. The hearing reinforced that federal assistance should be evaluated by whether it reduces risk and improves operational capacity. Funding alone is not sufficient if recipients cannot sustain the capability, integrate it into existing systems, hire personnel to operate it, or obtain useful assistance during an incident. The

Subcommittee's review focused on outcomes, including improved visibility, faster detection, stronger identity controls, greater regional coordination, and the ability to maintain essential services during a cyber event.

Hearing: "The AI Security Landscape: How Frontier Models, Agentic AI, and AI Coding Tools Are Reshaping Cybersecurity and Critical Infrastructure Resilience"

On June 4, 2026, the Subcommittee held a hearing titled, "The AI Security Landscape: How Frontier Models, Agentic AI, and AI Coding Tools Are Reshaping Cybersecurity and Critical Infrastructure Resilience." The Subcommittee received testimony from Ms. Sandra Joyce, Vice President of Google Threat Intelligence at Google LLC; Chris Meserole, Ph.D., Executive Director of the Frontier Model Forum; Mr. Jack Cable, Chief Executive Officer and Co-Founder of Corridor Security Inc.; and Matthew Guariglia, Ph.D., Senior Policy Analyst at the Electronic Frontier Foundation.

The hearing examined how increasingly capable models are changing the conduct of cyber operations. Members focused on agentic systems that can reason, develop plans, use tools, write and execute code, and take actions with limited human direction. These capabilities can assist defenders, but they can also reduce the expertise, time, and personnel required to conduct malicious activity. Members considered how AI coding tools affect vulnerability discovery, software development, patching, and exploit creation. The discussion addressed the possibility that advanced systems could compress the time between the identification of a flaw and its exploitation, placing greater pressure on vendors, CISA, and critical infrastructure operators to identify exposed systems and deploy mitigations quickly.

The hearing also examined the security implications of integrating PRC-origin open-weight models into American software, tools, and infrastructure. Members considered risks involving model provenance, supply chain integrity, capability theft, external dependencies, embedded behavior, and the strategic consequences of relying on technologies developed by companies subject to PRC law and state influence. The Subcommittee's work reflected the need for a risk-based approach that accounts for how a model is developed, what capabilities it possesses, the systems and data it can access, and the consequences if it is compromised or misused. The relevant question is not simply whether a model is open or closed, hosted locally or accessed through an external service. The more important question is whether the model and its supporting infrastructure can be trusted for the function in which they are used.

Subcommittee on Border Security and Enforcement

Hearing: "Exploring the Use of Unmanned Aircraft Systems Across the DHS Enterprise"

On April 1, 2025, the Subcommittees on Border Security and Enforcement and Emergency Management and Technology held a joint hearing titled, "Exploring the Use of Unmanned Aircraft Systems Across the DHS Enterprise." The Subcommittees received testimony from Mr. Bryan Farrell, Interim Director, Raspet Flight Research Laboratory, Mississippi State University; Mr. Mike Ledbetter, Executive Vice President and Chief Operating Officer, COLSA Corporation; Mr. Jerry Hendrix, Executive Director, Rotorcraft Systems Engineering and Simulation Center, the University of Alabama in Huntsville; and Mr. Kevin

Fetterman, Fire Division Chief, Division 4, Orange County Fire Authority, on behalf of the International Association of Fire Chiefs.

The hearing included discussion examining the Department of Homeland Security's use of unmanned aircraft systems (UAS) for border protection, drug interdiction, disaster mitigation, and emergency management. Specifically, witnesses described the use of UAS at the border for maintaining situational awareness, identifying potential threats approaching, and gathering intelligence to inform law enforcement action.

Member Briefing: Cartel Activity and Border Security

On May 20, 2025, the Subcommittee held a classified briefing with the U.S. Department of Homeland Security (DHS) Office of Intelligence & Analysis, U.S. Customs and Border Protection, the U.S. Coast Guard, U.S. Immigration and Customs Enforcement, and the Drug Enforcement Administration. Representatives from DHS and the Department of Justice (DOJ) briefed Members on the threats posed by cartels to U.S. border security.

"Case by Case: Returning Parole to its Proper Purpose"

On July 15, 2025, the Subcommittees on Oversight, Investigations, and Accountability and Border Security and Enforcement held a joint hearing titled, "Case by Case: Returning Parole to its Proper Purpose." The Subcommittees received testimony from the Honorable Ken Cuccinelli, Senior Fellow, Center for Renewing America; Mr. Steven Camarota, Director of Research, Center for Immigration Studies; Mr. David J. Bier, Director, Immigration Studies, CATO Institute; and written testimony from Mr. Charles Marino, Former Senior Law Enforcement Advisor to the Secretary of the Department of Homeland Security.

The hearing included discussion on the security risks associated with parole programs that rapidly admit aliens who may otherwise be inadmissible into the United States, bypassing traditional processes that give USCIS and the Department of State adequate time to screen and vet individuals and make the deliberate admissions of screened asylum seekers in accordance with the original congressional intent of parole.

Member Briefing: Industry Perspective on Biometric Entry-Exit Implementation

On January 21, 2026, the Subcommittee on Border Security and Enforcement and the Task Force on Enhancing Security for Special Events in the United States held a joint roundtable focused on CBP's implementation of the Biometric Entry-Exit Program. Members and participants discussed the importance of the biometric entry-exit program in screening passengers at airports to verify the identity of all travelers when entering or exiting the United States. Participants provided data supporting CBP statistics on the near completion of incoming passenger screening and the persistent challenges with implementing exiting passenger screening.

The discussion included representatives from the U.S. Travel Association; Dallas Fort Worth International Airport; Delta Air Lines; and iProov. Given the 9/11 Commission's explicit recommendation to establish a biometric entry-exit program, the Committee is particularly focused on its implementation.

Hearing: "Smarter Borders, Safer Nation: Expanding the Use of Non-Intrusive Inspection Technology"

On January 22, 2026, the Subcommittee held a hearing titled, "Smarter Borders, Safer Nation: Expanding the Use of Non-Intrusive Inspection Technology." The Subcommittee received testimony from Ms. Diane Sabatino, Acting Executive Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection; and Ms. Hilary Benedict, Director, Science, Technology Assessments, and Analytics, U.S. Government Accountability Office.

The hearing highlighted the progress that has been made and challenges that remain in fully implementing 100 percent Non-Intrusive Inspection (NII) scan rates at ports of entry as required in the *Securing America's Ports Act of 2021*. Members and witnesses also discussed the importance of NII in identifying potential threats at land, air, and maritime ports of entry.

Hearing: "Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans"

On April 21, 2026, the Subcommittee on Border Security and Enforcement and the Subcommittee on Cybersecurity and Infrastructure Protection held a joint hearing titled, "Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans." The Subcommittees received testimony from Ms. Cynthia Kaiser, Senior Vice President, Halcyon Ransomware Research Center; Mr. Ari Redbord, Global Head of Policy, TRM Labs; Mr. Joshua Bercu, Senior Vice President, Policy, USTelecom — The Broadband Association; and Ms. Megan Stifel, Chief Strategy Officer, Institute for Security and Technology.

The hearing included discussion on the emerging threat posed by transnational criminal organizations that are increasingly leveraging digital technologies, including cryptocurrency, online platforms, artificial intelligence, and global financial networks, to conduct fraud, launder illicit proceeds, and target American citizens, businesses, and critical infrastructure.

Hearing: "Northern Exposure: Assessing the Evolving Threat Landscape at America's Northern Border"

On June 30, 2026, the Subcommittee on Border Security and Enforcement and the Subcommittee on Counterterrorism and Intelligence held a joint hearing titled, "Northern Exposure: Assessing the Evolving Threat Landscape at America's Northern Border." The Subcommittees received testimony from Mr. Jason Schneider, Acting Deputy Chief, U.S. Border Patrol, U.S. Customs and Border Protection; Mr. Chris Holtzer, Executive Director of Operations, Office of Field Operations, U.S. Customs and Border Protection; Mr. Michael J. Krol, Assistant Director for Domestic Operations, Homeland Security Investigations, U.S. Immigration and Customs Enforcement; and Ms. Heather MacLeod, Director, Homeland Security and Justice, U.S. Government Accountability Office.

The hearing included discussion on the unique security challenges posed by the Northern border, including its vast geography, remote terrain, limited personnel, technology and infrastructure gaps, and policy differences between the United States and Canada related to visas, asylum, and border screening. The 9/11 Commission's emphasis on the importance of an

integrated border security network and maintaining control over border crossings is particularly relevant today with an increased focus on U.S. security posture along the Northern border.

Member Classified Briefing: Cyber Enabled Transnational Financial Crimes

On July 14, 2026, the Subcommittee on Border Security and Enforcement and the Subcommittee on Counterterrorism and Intelligence held a joint classified briefing with representatives from Homeland Security Investigations, the U.S. Secret Service, and the Federal Bureau of Investigation. Agency officials briefed Members on the threat of cyber-enabled transnational financial crimes.

SUBCOMMITTEE ON EMERGENCY MANAGEMENT AND TECHNOLOGY

Hearing: "Future of FEMA: Perspectives from the Emergency Management Community"

On March 4, 2025, the Subcommittee held a hearing titled, "Future of FEMA: Perspectives from the Emergency Management Community." The Subcommittee received testimony from Mr. Jeff Smitherman, Director, Alabama Emergency Management Agency, State of Alabama; the Honorable Daniel Kaniewski, Managing Director, Public Sector, Marsh McLennan; Ms. Carrie Speranza, CEM, President, U.S. Council of the International Association of Emergency Managers; and the Honorable Timothy Manning, Former Deputy Administrator for Protection and National Preparedness, Federal Emergency Management Agency, who testified as a private citizen.

Following the addition of the delivery of federal disaster assistance to the U.S. Government Accountability Office's (GAO) high-risk list in February 2025,[209] the hearing allowed Members the opportunity to assess the current role of FEMA, including its expanding mission sets, stewardship of taxpayer dollars, grant administration, and coordination with state and local governments in disaster recovery and response. Members also discussed President Trump's Executive Order convening a FEMA Review Council[210] and sought to identify any efficiencies or potential reforms needed within the agency.

Hearing: "Mass Gathering Events: Assessing Security Coordination and Preparedness"

On May 21, 2025, the Subcommittee held a hearing titled, "Mass Gathering Events: Assessing Security Coordination and Preparedness." The Subcommittee received testimony from the Honorable Donald Barnes, Sheriff-Coroner, Orange County Sheriff's Department, who testified on behalf of the Major County Sheriffs of America; Mr. John Junell, Chief Security Officer, Live Nation Entertainment; and Mr. Jeremy Hammond, Assistant Commissioner, Southeastern Conference.

The hearing allowed Members the opportunity to assess how state and local law enforcement, state governments, and the private sector coordinate with the federal government for mass gathering events. This hearing specifically sought to highlight security challenges associated with mass gathering events and provide recommendations to the Committee's Task Force on Enhancing Security for Special Events in the United States for further consideration.

Hearing: "Surveying the Threat of Agroterrorism: Perspectives on Food, Agriculture, and Veterinary Defense"

On September 16, 2025, the Subcommittee held a hearing titled, "Surveying the Threat of Agroterrorism: Perspectives on Food, Agriculture, and Veterinary Defense." The Subcommittee received testimony from Daniel K. Wims, Ph.D., President, Alabama A&M University; Cris Young, DVM, MPH, DACVPM, COL USA (Ret.), Professor of Practice, College of Veterinary Medicine, Auburn University; Marty Vanier, DVM, Director, National Agricultural Biosecurity Center and Associate Director, Biosecurity Research Institute, Kansas State University; and Asha M. George, DrPH, Executive Director, Bipartisan Commission on Biodefense.

In June 2025, the Department of Justice (DOJ) charged several Chinese nationals associated with the University of Michigan in connection with attempts to smuggle potentially dangerous biological agents into the country.[211] One of the identified biological agents, *fusarium graminearum*, was a fungus classified as a potential agroterrorist weapon known to cause "head blight," a disease of wheat, barley, maize, and rice, which is responsible for billions of dollars in economic losses worldwide each year.[212] Witnesses provided an in-depth overview of the magnitude of the threat that agroterrorism poses to the food and agriculture critical infrastructure sector of the United States and where federal operations to prevent, protect against, mitigate, respond to, and recover from acts of agroterrorism can be enhanced.

Member Classified Briefing: Chemical, Biological, Radiological, and Nuclear Threats

On January 13, 2026, the Subcommittee on Emergency Management and Technology and the Subcommittee on Counterterrorism and Intelligence held a joint classified briefing with representatives of the former DHS Countering Weapons of Mass Destruction Office (CWMD) and the DHS Office of Intelligence and Analysis (I&A) regarding threat assessments for current and future chemical, biological, radiological, and nuclear (CBRN) threats to the homeland and ongoing efforts of DHS and the federal government more broadly to deter those threats.

Hearing: "Surveying the Threat of Agroterrorism, Part II: Assessing Federal Government Efforts"

On February 11, 2026, the Subcommittee held a hearing titled, "Surveying the Threat of Agroterrorism, Part II: Assessing Federal Government Efforts." The Subcommittee received testimony from Ms. Suzette Kelly, Deputy Executive Director Performing the Duties of the Executive Director, Agriculture Programs and Trade Liaison, Office of Field Operations, U.S. Customs and Border Protection, U.S. Department of Homeland Security; Mr. Matt Allen, Director, Office of Homeland Security, U.S. Department of Agriculture; Mr. Jeff Cooper, Program Manager, Probabilistic Analysis for National Threats Hazards and Risks, Science and Technology Directorate, U.S. Department of Homeland Security; and Ashley Grant, Ph.D., MPH, Senior Health Security and Biodefense Advisor, Office of Health Security, U.S. Department of Homeland Security.

The hearing allowed Members to better understand the role the federal government plays in establishing national preparedness for threats to the food and agriculture critical infrastructure sector of the United States and assess the implementation of the National Farm Security Action Plan.[213] The discussion built upon testimony received during the Subcommittee's previous September 16, 2025, hearing to refine legislative solutions geared towards improving the mission sets and capabilities of the federal government, and specifically DHS, to counter agroterrorist threats.

Site Visit: Redstone Arsenal

On April 23, 2026, and April 24, 2026, the Subcommittee led a Member site visit to Redstone Arsenal in Huntsville, Alabama, to examine facilities and equities with relevance to the DHS mission set. Among other items, Members visited the Federal Bureau of Investigation's Terrorist Explosive Device Analytical Center (TEDAC), which coordinates bomb-related evidence and intelligence collection that supports FBI's science and technology partners, including the Transportation Security Laboratory, a national laboratory operated by the DHS Science and Technology Directorate (S&T). Members also visited the FBI's National Counter-Unmanned Aircraft Systems Training Center (NCUTC), modeled after the FBI's Hazardous Devices School, which serves as the sole hub for training and certifying law enforcement and security professionals to counter unmanned aircraft systems (UAS) threats, ensuring that all training recipients are instructed to the same standard.[214]

Site Visit: FEMA Headquarters

On June 4, 2026, the Subcommittee led a Member site visit to FEMA headquarters to examine the work of its National Response Coordination Center in preparation for the 2026 Atlantic hurricane season, as well as FEMA's Special Events Coordination Center in advance of the 2026 FIFA World Cup and America250 and Freedom250 events.[215]

POLICY RECOMMENDATIONS

Policy Recommendations

Informed by thorough assessment of ongoing national security considerations, the status of unfulfilled 9/11 Commission Report recommendations, and lessons learned from the Committee's relevant activities in the 119th Congress as listed above, the Committee has identified numerous proposals to continue this vital work and further improve homeland security in the United States. The Committee urges Congress and the Executive Branch to work quickly to implement the following proposals, and to do so in a bipartisan manner to ensure long-term certainty and stability across the homeland security enterprise.

COUNTERTERRORISM AND INTELLIGENCE

Challenge: A Fragmented Information Sharing Environment

Despite the creation of new offices and fusion centers, and a reorganization of the Intelligence Community in the years since 9/11, the information sharing challenges that contributed to intelligence blind spots twenty-five years ago continue to be pervasive.

Fusion centers emerged in the aftermath of 9/11 as policymakers understood the urgency of integrating and sharing information across SLTT and private sector partners. While fusion centers are locally owned and operated, they are supported by federal government agencies and have been described as force multipliers in counterterrorism efforts.[216] The National Network of Fusion Centers today consists of eighty sites, with at least one in every state. DHS, particularly the Office of Intelligence & Analysis, and the FBI serve as the lead federal partners in fusion centers, embedding intelligence analysts and special agents as liaisons to facilitate cross-jurisdictional information sharing and the seamless exchange of intelligence and investigative resources.

According to DHS, fusion centers enhance the Information Sharing Environment (ISE) by "receiving threat information from the federal government; analyzing that information in the context of their local environment, [and] disseminating that information to local agencies," while also connecting federal agencies with state and locally generated threat information and subject matter expertise.[217] A formalized ISE itself is a result of the *Intelligence Reform and Terrorism Prevention Act* (IRTPA). IRTPA became law in 2004 and served as a comprehensive reform of the Intelligence Community and terrorism prevention efforts.[218] Among other reforms, IRTPA established an ISE to serve as a framework for the sharing of terrorism information between federal and non-federal partners.[219] IRTPA additionally established the National Counterterrorism Center within the Office of the Director of National Intelligence to coordinate the same among federal agencies.[220]

While these were important strides, operational friction persists in several areas related to how information is shared amongst this spectrum of partners. This includes misalignment between National Incident Management System (NIMS) information sharing requirements. NIMS is intended to provide common vocabulary and processes for federal, SLTT, and private sector cooperation, but it is often overshadowed by varying state and local protocols that can impede timely dissemination of intelligence. Additionally, limitations in sharing law enforcement sensitive or classified information with all-hazards partners can restrict the full operational utility of available intelligence products. This is compounded by insufficient availability of secure facilities for the handling of classified information, which impedes timely

information flows to state and local partners.

A further challenge to effective information sharing is insufficient field-based presence of intelligence personnel. I&A was created to serve as an intelligence conduit between the IC and SLTT partners and is the only element of the IC statutorily required to share information with those partners. This is best accomplished through the presence of I&A personnel embedded in the field, in proximity to SLTT partners, to facilitate bi-directional information flows and to enhance regional coordination and situational awareness. Although I&A has this unique mandate within the IC, the scope of its mission has since expanded, contributing to a current organizational model that is headquarters-centric. As a result, I&A is unable to sustain the field-based presence that is necessary to ensure timely, coordinated flows of intelligence. For law enforcement partners, the result is intelligence that is delayed, incomplete, or delivered in a manner that is too complex or otherwise inaccessible to law enforcement partners – all of which contribute to intelligence gaps and unacceptable risk.

As it exists today, the information sharing environment is still fragmented – such that intelligence is often present but not integrated or shared with the appropriate partners to form a common threat picture. This may resemble the pre-9/11 environment as disparate jurisdictions and federal agencies operate in siloes and often on non-interoperable platforms. Addressing these gaps is essential to improving unity of effort and ensuring that critical information reaches the appropriate stakeholders in a timely and actionable manner.

Recommendation: Improve Information Sharing Processes Across Federal and SLTT Law Enforcement Through Enhanced Field Presence

The Committee strongly supports and encourages reforms to I&A designed to restore the Office to its foundational mission, to increase I&A's field-based presence, and enhance cohesion across the IC. As highlighted by Rep. Gabe Evans (R-CO), a former law enforcement officer, "there's nothing more critical to law enforcement operations than communication between local, state, and federal agencies. Information sharing between the men and women on the frontlines and federal intelligence counterparts allows for a smooth process when local law enforcement encounters threats on the streets that have national or global threat roots."[221]

Led by Rep. August Pfluger (R-TX), Chairman of the Subcommittee on Counterterrorism and Intelligence, the bipartisan *I&A Mission Reorientation Act* (H.R. 7443) accomplishes a strategic redirection of I&A to better align the Office with its founding operational mission.[222] The bill amends I&A's statutory authorization under 6 U.S.C. § 121 to clarify that I&A's operational mission is to provide timely and efficient intelligence support to SLTT partners by forward-deploying intelligence capabilities, facilitating two-way information flows, and engaging with fusion centers. This realignment would be further supported by Subcommittee Chairman Pfluger's *Field Integration of Homeland Intelligence Act* (H.R. 7773), which would transition I&A to a more decentralized, field-based organizational structure by requiring intelligence analysts and officers to be embedded within every fusion center – situating intelligence capabilities closer to the stakeholders and regions they support, rather than concentrating those functions in Washington, D.C.[223]

These reforms should be complemented by others that support essential training across I&A and the broader intelligence community. The bipartisan *Department of Homeland Security Intelligence and Analysis Training Act* (H.R. 7436), led by Rep. Seth Magaziner (D-RI), the

Ranking Member of the Subcommittee on Counterterrorism and Intelligence, would ensure that all I&A personnel receive uniform post-employment training focused on civil rights, civil liberties, and privacy rights.[224] Personnel would additionally receive training on I&A's mission to integrate and disseminate intelligence to SLTT partners and on intelligence community analytic and open-source collection standards. These trainings align directly with the 9/11 Commission's focus on ensuring that the privacy rights of Americans are protected as counterterrorism and intelligence capabilities improve.

Relatedly, the *DHS Intelligence Rotational Assignment Program and Law Enforcement Support Act* (H.R. 2212), introduced by Rep. Ryan Mackenzie (R-PA) and passed by the House, incorporates I&A personnel within IC joint duty programs, allowing I&A analysts to rotate through assignments to other IC components.[225] Together, these reforms strengthen I&A's workforce while ensuring consistency across Intelligence Community products and incentivizing interagency information sharing.

Additionally, Congress should work to alleviate the access challenges currently encountered by SLTT partners. This includes providing necessary funding to support the construction or modernization of secure facilities in each fusion center. Alongside investments in physical infrastructure, Congress should consider improvements to the classification environment, including ways to streamline what is often a multi-year security clearance process for fusion center personnel, to encourage the integration of platforms for building a common operating picture, and to expand training opportunities designed to enhance information fluency for small and rural law enforcement partners.

Challenge: Terrorism Definitions and Legal Standards Do Not Appropriately Reflect Today's Threat Environment

While the 9/11 attacks exposed the vulnerability of the homeland to foreign terrorist ideologies, today's threat environment is increasingly characterized by homegrown and domestic violent extremism. This is evidenced by the surge in political violence, recent lone wolf attacks driven by grievances related to international conflict, and activity fueled by online ecosystems that accelerate radicalization.

As a result, the nation's security, legal, and intelligence frameworks that were optimized post-9/11 to disrupt, prevent, and prosecute threats of terrorism with a foreign nexus may fail to fully capture domestic threats or those without a clear differentiation. The circumstances surrounding the alleged shooter in the November 2025 attack on two National Guardsmen in Washington, D.C. illustrate this dilemma. The suspect held legal asylum status in the U.S. and is believed to have been radicalized online after arrival – blurring the lines between foreign-inspired and domestic terrorism.[226]

A notable gap in this space is inconsistency in federal definitions for domestic terrorism. The FBI and DHS are the primary federal entities responsible for preventing and investigating terrorism, primarily through multi-agency Joint Terrorism Task Forces (JTTFs). Yet, these two lead agencies operate using different definitions. DHS uses the 6 U.S.C. §101 definition of terrorism, which encompasses acts dangerous to critical infrastructure and key resources.[227] In contrast, the FBI relies on the domestic terrorism definition at 18 U.S.C. § 2331, which does not include language related to key assets.[228] The Title 18 definition used by the FBI additionally requires conduct to occur primarily within the United States. These definitional discrepancies

hinder interagency efforts to counter domestic terrorism by inhibiting a common operational picture. As agencies lack consensus on what conduct meets the threshold of domestic terrorism, threat prioritization and intelligence sharing become disjointed. The fact that thirty-two states and the District of Columbia have distinct domestic terrorism statutes further complicates the investigation and prosecution of cases that cross jurisdictions.[229]

The rapid emergence of Nihilistic Violent Extremist (NVE) groups highlights the urgency in closing these gaps and demonstrates how the nature of terrorist threats has changed since 9/11. NVEs are distinct from other domestic extremist or foreign terrorist groups in that they lack a coherent ideology and are instead driven by a desire to create chaos and destruction. NVEs frequently operate on encrypted messaging and gaming platforms, grooming and coercing minors into engaging in violent conduct, self-mutilation, sexual acts involving minors, harm to animals, murder, and suicide.[230]

As of May 2026, the FBI announced that it had opened investigations involving 450 subjects tied to the NVE group 764 and other online criminal networks spanning all 56 FBI field offices.[231] Absent a unified federal definition or criminal charge for domestic terrorism, prosecutors have generally relied on underlying criminal offenses, including racketeering, to bring charges against suspected offenders.[232] Similarly, NVE cases often demonstrate a transnational nexus, including affiliate groups or U.S. citizens abroad who are complicit in conduct occurring within the United States.[233]

Recommendation: Create Uniformity Across Definitions and Update to Reflect Current Threats

To keep pace with the changing nature of terrorist threats to the homeland, the Committee recommends updating and creating uniformity in how federal agencies define acts of terrorism. This includes assessing the feasibility of a unified federal definition for domestic terrorism across all agencies, without geographic parameters on conduct, that encompasses conduct targeting critical infrastructure and strategic resources.

While aligning definitions to the current environment, the Committee supports the development of a national strategy to counter domestic terrorism. Such strategy should consider how the digital landscape, including social media and artificial intelligence, offers new means for NVE and FTO groups to reach and radicalize individuals in the homeland. Importantly, a national strategy should reflect input from both DHS and FBI, and properly resource JTTFs as the existing and effective model for investigating threats of terrorism. Further, recognizing that First Amendment protections often complicate efforts to address domestic terrorism, the Committee recommends that any strategy be ideology-neutral and focused on conduct.

Challenge: Staying Ahead of Terrorist Adaptation

Although immense national resources and attention have been dedicated to the counterterrorism mission over the past twenty-five years, terrorist group adaptation is an enduring strategic reality. At home and abroad, the U.S. is confronting terrorist groups that were not established on 9/11 and who are employing tools and techniques that likewise did not exist.

Artificial intelligence is the emerging capability with the highest potential for terrorist organizations to exploit. In the past year, research products and public reporting have suggested that terror groups are actively seeking to enhance their AI literacy and leverage AI to increase the

sophistication and effectiveness of planned attacks.[234] Additionally, as highlighted by Rep. Pfluger, terrorists are leveraging AI for "online radicalization by producing highly convincing propaganda videos to fabricate events and manipulate the perception of potential recruits. Known terrorist organizations such as ISIS and Al Qaeda have even gone as far as to have AI "workshops" to train members on its use."[235]

Earlier this year, the National Counterterrorism Innovation, Technology, and Education Center (NCITE) identified the heightened risks posed by the malign use of uncensored AI models by terror groups.[236] Uncensored models are those in which built-in safety mechanisms are weakened or removed, such that the model will not refuse to answer a prompt with violent or criminal consequences. If employed by terror groups, uncensored models may reduce barriers, such as low subject matter expertise, that currently act as inhibitors to attack planning.

Relatedly, as discussed in previous sections, the advent of social media and encrypted messaging platforms represents a new environment for terrorist recruitment and radicalization. As the U.S. confronts rising incidents of homegrown violent extremism, online radicalization is often a common thread. Recent examples include the January 2025 New Orleans truck attack that killed 14, and an Afghan national arrested for plotting an ISIS-inspired Election Day bombing.[237] These incidents highlight how FTOs can still inspire and enable violence on U.S. soil without direct contact.

Lastly, today's terror threat landscape increasingly transcends national boundaries as terror groups move, adapt, and attempt to evade detection by the U.S. and its network of allies and partners. To realize the full potential of U.S. allies and partners as force multipliers in countering threats of terrorism, the U.S. government must maintain robust and real-time awareness of where terror groups are operating.

Recommendation: Increase Awareness of Emerging Terrorist Threats, Tactics, and Organizations, and Support the DHS Research Enterprise

The no-fail mission of this Committee and the DHS enterprise requires persistent education, awareness, and innovation by lawmakers and national security professionals. Robust understanding of emerging threats is a prerequisite for crafting sound national policy and strategies to counter the risks posed by U.S. adversaries. To this end, the Committee supports the *Generative AI Terrorism Risk Assessment Act* (H.R. 1736), introduced by Rep. Pfluger, which would provide Congress, DHS, and the IC with regular assessments of terrorist threats to the U.S. posed by FTOs leveraging generative artificial intelligence, or GenAI.[238] This bill was passed by the House in November 2025.

Relatedly, the Committee also supports Rep. Pfluger's *Countering Online Radicalization and Terrorism Act* (H.R. 1212).[239] This bill would similarly increase the information available to Congress and the homeland security enterprise regarding recruitment, radicalization, and terror financing facilitated through cloud-based messaging platforms. As terrorist organizations seek to exploit new online forums and technologies to disseminate propaganda, streamline radicalization, and aid in planning attacks against the United States, strengthening whole-of-society countermeasures is a critical line of effort. This includes encouraging collaboration and enhanced partnerships with social media companies to mitigate terrorist and extremist content. Over the past year, the Committee has convened discussions with several major social media

companies to better understand how such content is identified and removed, and where enforcement gaps may remain.

The very first recommendation provided by the 9/11 Commission in its final report discusses the importance of denying terrorists access to safe havens, and this remains a critical component of U.S. counterterrorism efforts today, even as terrorist organizations constantly adapt.[240] To aid in these efforts, the Committee supports enactment of the *Major Non-NATO Ally Terror Threat Assessment Act* (H.R. 8168), introduced by Rep. Matt Van Epps (R-TN), which would regularly identify and assess the presence of, and threats posed by, foreign terrorist groups operating within countries designated as Major Non-NATO Allies, enhancing collective situational awareness for the U.S. and its partners.[241] This bill was passed by the House in July 2026.

The January 2025 New Orleans truck attack referenced above highlights a persistent tactical threat available to terrorists. While less sophisticated than other emerging technical capabilities, a vehicle ramming attack on a soft target, like a parade or other mass outdoor gathering, can still have devastating consequences. This was made clear to the global community on July 14, 2016, when a terrorist drove a truck through a crowd celebrating Bastille Day in Nice, France, killing eighty-six people and injuring more than 400, in attack claimed by ISIS.[242] In order to combat this threat, the Committee supports the *Department of Homeland Security Vehicular Terrorism Prevention and Mitigation Act of 2025* (H.R. 1608), introduced by Rep. Carlos Gimenez (R-FL), to enhance law enforcement collaboration on preventing these kinds of attacks.[243] This bill was passed by the House in November 2025.

As terrorist threats continue to evolve, it is critical that DHS and Congress maintain situational awareness on how these changes impact broader homeland security priorities. The Committee has advanced several initiatives to improve the information available to policymakers and homeland security practitioners in the field regarding some of the shifting terrorism trends discussed above, including the FTO designations for cartels and other transnational criminal organizations and how to balance a shift towards Africa without losing focus on traditional terrorist hotbeds in the Middle East. These Committee-supported efforts include the *Tren de Aragua Border Security Threat Assessment Act* (H.R. 4070),[244] introduced by Rep. Brad Knott (R-NC), and the *Syria Terrorism Threat Assessment Act* (H.R. 1327),[245] introduced by Rep. Morgan Luttrell (R-TX), which were both passed by the House in November 2025.

Another evolving tool that has become increasingly available to terrorists and other bad actors are unmanned aircraft systems, or drones, that can be weaponized and used for malicious purposes. As drones become more technologically advanced and more commercially accessible, DHS and Congress must continue to track these developments. Rep. Eli Crane (R-AZ), a member of the Transportation and Maritime Security Subcommittee, has advanced the Committee's efforts to better understand the implications of drone capability developments on the battlefield by introducing the *Detecting and Evaluating Foreign Exploitation of Novel Drones Act* (H.R. 6846), or *DEFEND Act*, which would require DHS to submit annual reports to Congress assessing how these emerging drone capabilities could be used by terrorists to target the United States.[246] The Committee supports this legislation and agrees with Rep. Crane that "as drone technology rapidly transforms the modern battlefield, Congress can't afford to be in the dark on these evolving threats."[247]

Additionally, the Committee supports consistent investments in the DHS research enterprise, including S&T Centers of Excellence like NCITE.[248] NCITE's research has been invaluable to this Committee's work and enhances collective understanding of the newest frontiers for threat actors, ensuring U.S. innovation stays a step ahead of our adversaries.

TRANSPORTATION AND MARITIME SECURITY

Challenge: Modernizing Aviation Security Technology and Screening Operations

The aviation threat landscape has evolved significantly since September 11, 2001, and terrorist tactics have become increasingly sophisticated amidst rapidly advancing technologies, cyber threats, and the proliferation of unmanned aircraft systems. At the same time, the need for a robust, federalized aviation security system remains unchanged. Ensuring TSA has the technology, resources, and operational flexibility necessary to identify and mitigate these threats before they can be exploited is essential to protecting the homeland.

In response to the September 11th terrorist attacks, Congress created the Passenger Security Fee in the *Aviation and Transportation Security Act* (ATSA).[249] This fee is mandatory, collected from airline passengers, to help fund aviation security activities carried out by TSA.[250] The fee is currently set at $5.60 per one-way flight that originates at an airport in the United States and does not exceed $11.20 for a roundtrip ticket.[251] At the time this law was enacted, Congress intended for this fee to offset some of the costs associated with providing aviation security. However, the *Bipartisan Budget Act of 2013* (P.L. 113-67) significantly altered the collection of the Passenger Security Fee by increasing the amount from $2.50 to $5.60 and directing approximately $1 billion annually in collected fees to be deposited in the General Fund of the Treasury for deficit reduction purposes.[252] The *Bipartisan Budget Act of 2013* specified the diversion amounts through FY 2023, and Congress extended the diversion of Passenger Security Fee revenues through FY 2027, requiring deposits of $1.6 billion in FY 2025, $1.64 billion in FY 2026, and $1.68 billion in FY 2027, with the diversion set to expire after FY 2027.[253] To date, approximately $15 billion in Passenger Security Fee revenue has been diverted from investments in passenger and baggage screening technology, among other critical aviation security capabilities, and redirected for deficit reduction purposes. This diversion has limited TSA's ability to make sustained investments in next-generation screening capabilities.

Furthermore, operational flexibility presents a related challenge. Airports experience significant variations in passenger volumes and security needs, but TSA must maintain consistent security standards while allocating personnel and resources across the aviation system. Without additional flexibility, airports can face congestion and delays even when additional screening resources could be deployed to address specific operational demands.

Recommendation: Restore the Passenger Security Fee to Serve its Intended Purpose

The Committee recognizes that the threat landscape has evolved to include more sophisticated terrorist tactics, rapidly advancing technologies, cyber threats, insider threats, and the increasing use of unmanned aircraft systems, while the need for robust aviation security remains unchanged. The 9/11 Commission emphasized that the United States must continually identify emerging vulnerabilities and invest in risk-based security measures. The Committee

recommends the collection of the Passenger Security Fee is restored to its purpose of funding aviation security technology that helps to prevent future attacks.

During the second session of the 119th Congress, the Committee advanced the *Spending Aviation Fees for Equipment, Guaranteeing Upgraded and Advanced Risk Detection and Safety Act of 2026* (H.R. 8770), or *SAFEGUARDS Act*, sponsored by the Committee's Emergency Management and Technology Subcommittee Chairman, Rep. Dale Strong (R-AL). This legislation would allow Passenger Security Fee revenues to be directed towards aviation security technology that strengthens TSA's ability to protect the United States against future attacks once the current diversion expires, preventing Congress from extending the deficit reduction diversion again. Specifically, this legislation would annually allocate the first $500 million in collected Passenger Security Fees for checked bag explosive detection systems, and the next $250 million for checkpoint technology upgrades beginning in FY 2028, following the end of Passenger Security Fee diversion. This bill was passed by the House in July 2026.[254]

Furthermore, the Committee also supports the *Reimbursable Screening Services Program* (RSSP) *Extension Act of 2026* (H.R. 9391), introduced by Chairman Andrew Garbarino (R-NY), which would extend TSA's RSSP partnerships through FY 2031 and increase the number of eligible entities from eight to fourteen. Established as a pilot program in the FY 2019 *Department of Homeland Security Appropriations Act*, RSSP allows TSA-regulated entities to enter into reimbursable agreements for additional screening services outside primary terminal screening areas.[255] Participating entities fully reimburse TSA for the personnel and non-personnel costs associated with these services. This bill was passed by the House in July 2026.[256]

Expanding RSSP participation would give TSA greater flexibility to adjust staffing and screening resources based on airport-specific operational needs while maintaining federal security standards. The program can also improve passenger throughput, reduce airport congestion, and provide airports with additional tools to address periods of elevated demand without negatively affecting security operations at primary TSA checkpoints.

Challenge: Improving Risk-Based Security & Facilitating International Travel

As reflected in the 9/11 Commission Report, effective aviation security requires TSA to focus its resources where they are most needed while maintaining rigorous screening standards. Risk-based security can reduce unnecessary duplication for lower-risk travelers, allowing security personnel and technology to be concentrated on identifying emerging threats and addressing higher-risk vulnerabilities. International travel presents a particular opportunity to apply this approach.

Under traditional screening processes, passengers arriving in the United States from international destinations undergo inspection by CBP, collect their checked baggage, and exit the sterile area of the airport. Passengers with onward connections must then re-check their baggage and undergo TSA security screening again. This process can create significant delays and duplicative screening requirements for travelers who have already been screened at trusted foreign airports thoroughly vetted by TSA. Trusted international partnerships can help address this challenge by allowing TSA to recognize security screening conducted at approved foreign airports while maintaining appropriate oversight and standards.

Recommendation: Extend TSA's One-Stop Pilot Program

The Committee supports the continuation of TSA's One-Stop Pilot Program[257] through enactment of the *One-Stop Pilot Program Extension Act* (H.R. 9388), introduced by Rep. Gimenez, who serves as the Committee's Transportation and Maritime Security Subcommittee Chairman. This legislation would extend the program for an additional four years beyond its original six-year pilot period and require last point of departure (LPD) participants, or TSA-approved foreign airports, to screen passengers and their checked baggage inbound to the United States using TSA-approved explosive detection systems (EDS).[258] By ensuring that participating foreign airports maintain security measures commensurate with TSA requirements, the legislation strengthens the United States' ability to identify and mitigate security vulnerabilities before passengers and baggage reach U.S. soil, enhancing aviation security while facilitating legitimate international travel. This bill was passed by the House in July 2026.

Challenge: Improving the Traveler Experience for Trusted Travelers While Maintaining Rigorous Security Standards

TSA must balance the need for rigorous screening with the practical realities of passenger travel. Lower-risk populations like military personnel and their families, as well as families traveling with young children, can benefit from targeted screening procedures that reduce unnecessary friction without compromising security requirements. A risk-based approach allows TSA to leverage verified information and known traveler characteristics to streamline screening for lower-risk populations. Doing so can improve passenger throughput while allowing TSA personnel and screening resources to remain focused on emerging threats and higher-risk travelers.

Recommendation: Implement Programs Aimed at Improving the Traveler Experience for Low-Risk Populations

The Committee supports the *Improving Travel for Military Members Act* (H.R. 9328), introduced by Rep. Sheri Biggs (R-SC), which would improve travel procedures for military personnel while preserving TSA's security requirements. By leveraging verified military status to facilitate screening for known, lower-risk travelers, the legislation would reduce unnecessary travel burdens for the military community while enabling TSA to focus resources on higher-risk passengers and emerging threats. This bill was passed by the House in July 2026.[259]

This legislation builds on TSA's "Serve with Honor, Travel with Ease" initiative, launched in July 2025, which provides free TSA PreCheck for Gold Star families, discounts for military spouses, and expedited screening lanes for service members. TSA has also established expedited screening lanes for service members and their families at select airports near large military installations.[260] The program is currently operational across 119 airports, including 33 large hub airports and 86 medium airports, with participating airports offering dedicated lanes, preferred lanes, or front-of-line screening procedures.[261]

The Committee also supports the *Improving Travel for American Families Act* (H.R. 8897), introduced by Rep. Mackenzie, which would facilitate screening for lower-risk populations such as families while allowing TSA to concentrate screening resources on higher-risk passengers.[262] The legislation builds on TSA's "Families on the Fly" initiative, announced in 2025, which provides dedicated screening lanes for families traveling with children under twelve

to improve passenger throughput and reduce the burden of traveling with young children.[263] This bill was passed by the House in July 2026.

Overall, the Committee supports a comprehensive approach to TSA modernization that combines investments in next-generation screening technology and continued support for the TSA workforce with greater operational flexibility, stronger international partnerships, and expanded risk-based screening programs to build on the aviation security imperative outlined by the 9/11 Commission. The *SAFEGUARDS Act* would responsibly restore dedicated aviation security resources over the coming years and help provide TSA with the technology needed to modernize passenger and checked baggage screening. The *RSSP Extension Act of 2026* would give airports greater flexibility to address unique passenger volumes and operational challenges through additional reimbursable screening resources. The *One-Stop Pilot Program Extension Act* would strengthen international screening partnerships while eliminating duplicative screening for eligible travelers. Finally, the *Improving Travel for Military Members Act* and *Improving Travel for American Families Act* would reduce travel burdens for trusted, lower-risk populations while preserving TSA's core security mission.

Taken together, these efforts reflect the 9/11 Commission's vision of an adaptive aviation security system that prioritizes risk, strengthens security, and facilitates legitimate travel.

CYBERSECURITY AND INFRASTRUCTURE PROTECTION

Challenge: Gaps in Information Sharing and Cross-Sector Coordination

The intelligence failures preceding September 11th demonstrated the consequences of fragmented information, unclear responsibilities, and institutional barriers to collaboration. In the years since, Congress and the Executive Branch have applied those lessons to cybersecurity by establishing CISA, creating federal incident coordination frameworks, strengthening public-private partnerships, and building sector-based mechanisms for sharing threat information and coordinating risk reduction.

Presidential Policy Directive 41 (PPD-41) and National Security Memorandum 22 (NSM-22) established frameworks for coordinating the federal government's response to significant cyber incidents and managing risks to critical infrastructure. Information Sharing and Analysis Centers (ISACs) provide forums for sector-specific exchange, while Sector Risk Management Agencies (SRMAs) serve as the federal government's primary points of coordination and assistance for their assigned sectors. CISA, in turn, is responsible for coordinating national cyber defense and, under NSM-22, serves as the National Coordinator for Critical Infrastructure Security and Resilience.

These structures have improved cooperation, but their effectiveness remains uneven. SRMAs differ considerably in staffing, technical expertise, authorities, resources, and the maturity of their relationships with industry. Some maintain experienced teams and well-developed partnerships, while others lack the personnel or institutional capacity to provide sustained support. These differences become especially consequential during incidents that affect more than one sector, where unclear lines of responsibility can delay information sharing, create conflicting requests, and make it difficult to develop a common understanding of the incident and its downstream consequences.

The growing interdependence of critical infrastructure further strains frameworks organized around individual sectors. A compromise affecting a cloud service provider, telecommunications carrier, software vendor, data center, or other widely relied upon entity can create consequences across several sectors at once. In such cases, no single SRMA may possess complete visibility into the affected systems, dependencies, and operational risks. Complex cyber campaigns also move faster than many existing coordination processes, increasing the need for information that is timely, specific, and useful to network defenders.

Although the federal government has taken meaningful steps to encourage collaboration, gaps remain in how information is collected, analyzed, shared, and converted into action. Information may be delayed, overclassified, incomplete, or distributed without sufficient context. Private entities may provide information to the government without receiving a timely assessment in return. Federal agencies may collect overlapping information through separate channels, while state and local partners may struggle to identify the appropriate point of contact. These weaknesses reduce the value of information sharing when it is most needed.

Recommendation: Modernize Information Sharing Authorities, Strengthen Coordination, and Equip CISA for the Current Threat Environment

Congress should preserve and modernize the statutory authorities that support voluntary cybersecurity information sharing. The *Cybersecurity Information Sharing Act of 2015* (CISA 2015) remains a core part of that framework. It provides legal clarity for sharing cyber threat indicators and defensive measures, includes protections concerning liability, antitrust law, and public disclosure, and establishes privacy and civil liberties safeguards.

Today, these authorities are set to expire on December 11, 2026, absent additional congressional action. Their expiration could create legal uncertainty, discourage participation, and weaken established channels for sharing information between and among private sector stakeholders and the federal government. Long-term reauthorization is critical to prevent a decline in voluntary information sharing and to ensure that defenders continue to receive information needed to identify and respond to malicious activity.

Chairman Garbarino's *Widespread Information Management for the Welfare of Infrastructure and Government Act* (H.R. 5079), or *WIMWIG Act*, would reauthorize and update these authorities to reflect changes in the cyber environment since 2015. That modernization would account for the expanding role of artificial intelligence, cloud infrastructure, managed service providers, operational technology, and other developments that affect how cyber threats are identified, shared, and mitigated.

Reauthorization should also be accompanied by improvements in implementation. Information sharing should be timely, reciprocal, and operationally useful. CISA should provide clear mechanisms for receiving information, combining it rapidly with relevant government and industry reporting, and returning actionable findings to affected organizations and sectors. The value of the framework should be measured not only by the volume of information submitted, but by whether it enables defenders to identify intrusions earlier, contain malicious activity, protect other potential victims, and prevent an adversary from expanding access.

Congress must also ensure that CISA has the personnel, authorities, technical capabilities, and resources necessary to act on the information it receives. Since the agency was established in

2018, its responsibilities have expanded to include defending federal civilian networks, coordinating national cyber defense, supporting critical infrastructure owners and operators, assisting state and local governments, managing significant incident coordination, addressing risks to operational technology, and preparing for threats arising from artificial intelligence and other emerging technologies. Those responsibilities cannot be carried out effectively without sustained operational capacity.

CISA should improve its ability to provide direct assistance during significant incidents. This should include deployable incident response personnel, specialized operational technology expertise, scalable threat hunting capabilities, secure mechanisms for exchanging sensitive technical information, and the capacity to support multiple victims during a widespread campaign. Assistance should be prioritized according to the risk presented, the potential consequences of disruption, the national significance of the affected systems, and the defensive capacity of the victim.

This capability is especially important when a campaign affects smaller or less mature organizations. A municipal utility, rural hospital, local government, or regional service provider may face attacks from the same foreign intelligence service or criminal group as a large corporation, but lack the personnel and technology needed to investigate the intrusion independently. CISA should be able to provide practical support quickly, while coordinating with the FBI, the Intelligence Community, law enforcement agencies, regulators, SRMAs, and private sector partners as appropriate.

CISA must also maintain the technical expertise needed to understand how foreign adversaries operate and how emerging technologies are changing their capabilities. The agency should be able to recruit and retain personnel with experience operating in complex technical environments and draw on private sector, laboratory, and academic expertise when specialized capabilities are required.

In 2023, when serving in his previous role as Chairman of the House Appropriations Subcommittee on Homeland Security, Rep. Dave Joyce (R-OH), who currently serves on the Homeland Security Committee's Oversight, Investigations, and Accountability Subcommittee, stated in a hearing on CISA's FY 2024 budget request, "Without the right people, CISA cannot fully carry out its mission... As the country faces continually evolving threats, our workforce too must evolve. Rapid technological developments will continue to dramatically change network security, and CISA will need personnel with the right tools, training, and tenacity to meet those critical networks."[264] CISA's skilled workforce remains as important today as it was then, and the Committee will continue to advocate for the resources required to ensure that CISA has the personnel necessary to meet its statutory mission.

Emerging technologies require a corresponding transformation in CISA's capabilities. Artificial intelligence may allow adversaries to identify vulnerabilities, conduct reconnaissance, develop malicious code, improve social engineering, and operate across networks more quickly. It may also give defenders new tools for identifying anomalous activity, analyzing malware, prioritizing vulnerabilities, accelerating remediation, and automating routine defensive tasks. CISA should securely evaluate and adopt technologies that improve its own operations, while helping federal agencies and critical infrastructure owners understand the risks associated with AI systems deployed in sensitive environments.

CISA should develop the capacity to evaluate threats involving AI models, autonomous agents, supporting infrastructure, and software supply chains. This should include risks arising from excessive system permissions, autonomous behavior, compromised model repositories, malicious manipulation, foreign-developed models, insecure third-party integrations, and the use of AI to target critical infrastructure. The agency should coordinate with other technically capable agencies and private sector experts, but it should not defer responsibility when those risks directly affect federal network security or critical infrastructure resilience.

CISA should also exercise a stronger coordinating role across the SRMA community. As the National Coordinator for Critical Infrastructure Security and Resilience, the agency should establish common expectations for SRMA capabilities, assist less mature agencies in strengthening their capacity, and improve coordination during incidents that affect multiple sectors. This should include standardized procedures for interagency and intergovernmental engagement, shared planning assumptions, clear escalation mechanisms, and a common operating picture that incorporates relevant information from SRMAs, the Department of War, the Intelligence Community, law enforcement agencies, regulators, and private sector partners.

CISA's coordinating role should not displace sector expertise or the statutory responsibilities of other departments and agencies. It should ensure that sector-specific knowledge is incorporated into a broader assessment of risk and that significant dependencies, affected entities, and jurisdictional boundaries are identified before they impede a response. Congress should also ensure that other SRMAs have sufficient resources and expertise to carry out their responsibilities and participate effectively in cross-sector planning and incident coordination.

Congress should provide CISA with predictable resources that support long-term workforce development, technology modernization, operational planning, and sustained partnerships. Abrupt changes in funding can impair hiring, contracting, procurement, and the development of capabilities that require several years to mature. Predictable funding is particularly important for specialized technical teams, secure information sharing systems, persistent threat hunting capabilities, and long-term modernization efforts.

Empowering CISA requires both resources and discipline. Funding should be tied to clearly defined missions, measurable outcomes, transparent budgeting, and rigorous congressional oversight. Additional resources alone will not resolve weaknesses in program execution, interagency coordination, or assistance to critical infrastructure. CISA should be required to demonstrate how its activities reduce risk, improve visibility, accelerate incident response, and deliver practical value to the organizations it serves.

Congress should require regular reporting on program performance, operational readiness, workforce needs, technology investments, assistance provided during significant incidents, and progress in addressing identified capability gaps. Performance should be evaluated according to whether CISA helps organizations detect threats earlier, contain incidents more quickly, sustain essential functions, and prevent localized compromises from producing wider consequences.

CISA should not attempt to operate or regulate every critical infrastructure system. Its greatest value lies in identifying shared risks, connecting information across agencies and sectors, coordinating federal support, providing technical assistance, and helping owners and

operators improve resilience. Congress should reinforce those functions, eliminate or narrow activities that do not advance them, and hold the agency accountable when its programs fail to produce practical results.

Clear roles, established procedures, recurring exercises, modern technical capabilities, and sufficient operational capacity are necessary so that federal coordination mechanisms function before, during, and after a significant cyber incident. CISA should be empowered to lead where Congress has assigned it responsibility, resourced at a level consistent with the scope and urgency of its mission, and held accountable for demonstrating that its work makes federal networks and critical infrastructure more difficult to compromise and more capable of sustaining essential functions when incidents do occur.

Challenge: A Fragmented Cybersecurity Regulatory Environment

Cyber incident reporting requirements can improve situational awareness, help identify campaigns affecting multiple victims, and inform government assistance. When properly designed, they provide valuable information about adversary behavior, exploited vulnerabilities, affected sectors, and recurring weaknesses. The benefits decline, however, when reporting obligations are duplicative, inconsistent, or disconnected from a clear operational purpose.

Today, organizations may be required to report the same incident to multiple federal and state authorities under different definitions, thresholds, deadlines, and formats. One agency may require notification within hours, another within several days, and another after a materiality determination. Agencies may request overlapping but nonidentical information, forcing legal, compliance, and cybersecurity personnel to prepare separate submissions while the organization is still investigating the incident and restoring operations.

Industry stakeholders and state and local partners have consistently raised concerns that these requirements can divert personnel from incident response to administrative compliance. The problem is especially acute for smaller organizations that lack dedicated regulatory teams and must rely on the same personnel to investigate the intrusion, communicate with government agencies, and maintain essential services.

A recent U.S. Government Accountability Office report requested by Chairman Garbarino and Senate Homeland Security and Governmental Affairs Committee Ranking Member Gary Peters (D-MI) documented the range of federal cyber incident reporting requirements that covered entities may be required to navigate.[265] The absence of common definitions, aligned timelines, and coordinated processes imposes unnecessary costs and can also reduce the quality of information reported. Organizations responding to several requests at once may submit incomplete or inconsistent information, while agencies may receive duplicative reports without an effective process for reconciling or sharing them.

This fragmentation can create a false choice between compliance and security. Reporting requirements should support incident response and collective defense, not require organizations to redirect limited cyber personnel away from those functions.

Recommendation: Harmonize Cyber Regulations Around Security Outcomes

The federal government should streamline cybersecurity requirements so that regulated entities can devote more personnel and resources to reducing risk. Harmonization should focus

on common definitions, consistent reporting thresholds, aligned timelines, standardized data fields, reciprocal recognition of reports, and secure mechanisms for submitting information once and making it available to authorized agencies.

This effort should preserve meaningful accountability. Harmonization does not require weaker requirements or lower standards. It requires agencies to identify what information they need, why they need it, when it is useful, and whether another agency is already collecting it. Agencies should avoid requesting information that has no clear operational, regulatory, or policy value.

Several federal initiatives have recognized the need for regulatory harmonization, including the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) and the Trump Administration's March 2026 cybersecurity strategy.[266] Progress, however, has been limited. A more disciplined process is needed in which regulators, CISA, SRMAs, state authorities, and affected industries identify specific conflicts and agree on concrete changes.

The final rule implementing *CIRCIA* will be an important test of this approach. If the rule reflects congressional intent, clearly identifies covered entities and reportable incidents, protects sensitive information, and integrates with existing reporting obligations, it can improve national visibility while reducing some duplication. If it adds another independent requirement without resolving overlap, it may compound the burden Congress sought to address.

Congress and the Executive Branch should evaluate cyber regulations according to their security value. Reporting obligations should help the government warn other potential victims, coordinate assistance, identify trends, and hold regulated entities accountable. Requirements that do not advance those outcomes should be revised, consolidated, or eliminated.

Challenge: Rapid AI Development Is Outpacing Policy and Institutional Readiness

Artificial intelligence capabilities are advancing faster than the policies, governance structures, and security practices needed to manage their use. Organizations are adopting AI across software development, cybersecurity, data analysis, customer service, internal operations, and other functions, often without a complete understanding of where the systems are deployed, what information they can access, or what actions they are authorized to take.

This challenge is becoming more serious as models move from generating content to planning and executing multi-step tasks. Agentic systems may be permitted to write and run code, call external tools, access files, interact with networks, or make changes to operational environments. In many organizations, these capabilities are being deployed before security teams have established clear inventories, approval processes, logging requirements, access controls, or incident response procedures.

The lack of visibility creates several risks. An organization may not know that an employee has connected an external model to sensitive data. A coding agent may introduce insecure dependencies or make changes that are not adequately reviewed. An autonomous system may exceed its intended permissions, interact with external infrastructure, or take actions that the organization cannot reconstruct after the fact. Where AI is connected to critical infrastructure or operational technology, failures could affect physical processes and essential services.

A recent incident involving an autonomous AI agent during an internal evaluation demonstrated the risks associated with models that are given tools, network access, and broad permissions.[267] The agent escaped its testing environment and exploited vulnerabilities in an external system. As we continue to learn more, the incident clearly showed that conventional testing assumptions may not be sufficient for systems capable of adapting their behavior, identifying unintended pathways, and acting with limited human direction.

Organizations are currently left to make their own judgments about acceptable model behavior, appropriate human oversight, and the controls needed for deployment. The result is inconsistency across sectors and significant variation in security maturity. Some organizations conduct rigorous testing and restrict model access, while others deploy advanced capabilities without formal policies or reliable monitoring.

The federal government also lacks a unified approach to foreign-developed AI models, particularly open-weight models originating in the People's Republic of China. Agencies and companies may assess these systems differently, even when the models are used in sensitive environments. Without a coordinated strategy, the United States risks developing technology dependencies before the associated national security, supply chain, and data risks are fully understood.

Recommendation: Establish Risk-Based AI Cybersecurity Standards for Critical Infrastructure and Strengthen National Coordination

Congress should establish a clear, risk-based cybersecurity framework for AI systems that are deployed on, integrated into, or granted meaningful access to critical infrastructure systems and whose compromise or misuse could reasonably produce material consequences. The framework should focus on the operational function of the system, the access and privileges it receives, the degree of autonomy it exercises, its exposure to untrusted data and external services, and the reasonably foreseeable consequences of compromise, manipulation, unavailability, or unauthorized behavior.

CISA should coordinate this effort as part of its national responsibility for critical infrastructure security and resilience, while preserving the role of each SRMA as the primary federal interface for its sector. CISA and the SRMAs should work with sector-specific regulators, owners and operators, AI developers and providers, cybersecurity companies, independent evaluators, standards bodies, and other technical experts so that common expectations reflect both cross-sector risk and the operational realities of individual sectors.

Minimum requirements should be performance-based, technology neutral, and proportionate to risk. They should distinguish lower consequence uses from systems capable of materially affecting safety, security, or essential services, and impose enhanced requirements only where the potential consequences justify them. Standards should build on existing cybersecurity and AI risk management frameworks, recognize materially equivalent federal or sector specific requirements, and account for legacy operational technology, maintenance windows, safety and reliability obligations, procurement cycles, and other constraints that make critical infrastructure different from ordinary enterprise computing.

Baseline controls should address threat modeling, identity and least privilege authorization, granular tool permissions for agentic systems, network segmentation, secure

configuration and change management, logging and auditability, monitoring for anomalous behavior, vulnerability management, security testing, incident response, recovery, human override or safe fallback mechanisms where appropriate, and supply chain risk management. Owners and operators should be able to identify what an AI system is permitted to do, reconstruct material actions it has taken, isolate or disable it when necessary, and prevent unnecessary access to operational technology and safety critical systems.

For systems capable of producing the most serious consequences, Congress should require appropriate assurance before production deployment or material changes. Assessments should be designed around the actual risk presented and should permit qualified internal testing, independent evaluation, or recognition of equivalent federal and sector-specific assessments. Testing should not create unacceptable risk to live operations, and representative environments, testbeds, digital twins, or staging systems should be used when production testing would threaten safety or continuity of service.

AI-related incident reporting should be integrated into existing cybersecurity reporting frameworks rather than layered on top of them. Where an incident involving a covered AI system is already reportable under CIRCIA or another materially equivalent federal requirement, an entity should not be required to submit substantially duplicative reports. At the same time, the government should be able to obtain, when known and reasonably available, the AI-specific information necessary to understand whether autonomous behavior, prompt injection, model or retrieval manipulation, third party dependencies, or other AI-related factors contributed to the incident and whether similarly situated entities may be at risk.

The federal government should also establish a consistent methodology for evaluating model provenance and AI supply chain risk in sensitive critical infrastructure environments. Relevant factors should include the identity, ownership, control, and jurisdiction of the developer and material service providers; legal obligations that could compel access or assistance to a foreign government; the integrity and distribution of model weights and software dependencies; hosting, telemetry, remote administration, update channels, and data egress; known vulnerabilities or compromised distributions; and the owner or operator's ability to isolate, monitor, update, replace, or revoke access to the model. Open-weight or foreign-developed models should not be treated as inherently insecure, but the government should not ignore specific, evidence-based risks merely because a model is inexpensive, widely available, or capable.

CISA, working with the National Institute of Standards and Technology (NIST) and other technically capable agencies, should also develop the capacity to evaluate advanced AI cyber capabilities that are relevant to critical infrastructure protection. Evaluations should examine not only benchmark performance, but whether models can reliably perform consequential cyber tasks when combined with tools, scaffolding, additional inference time, or modified safeguards. Public findings should improve defender awareness without disclosing vulnerabilities, evaluation details, or proprietary information in a manner that would facilitate malicious activity.

Regulatory harmonization should be a design requirement from the outset. Critical infrastructure owners and operators should not be forced to satisfy multiple materially duplicative AI cybersecurity standards, assessments, or incident reporting regimes for the same system. Congress should pursue a nationally coherent baseline for the narrow category of AI systems capable of materially affecting critical infrastructure, while preserving generally

applicable State authority over areas such as safety, reliability, privacy, consumer protection, procurement, criminal law, and tort liability where those requirements do not create a direct conflict or substantially duplicative cybersecurity obligation.

The Committee's objective is to reduce material cybersecurity risk without creating a general federal licensing regime for artificial intelligence or dictating which models, vendors, architectures, or technologies private entities must use. Effective requirements should be adaptable as capabilities change, focused on measurable security outcomes, and developed with sustained participation from critical infrastructure operators, AI developers, cybersecurity practitioners, researchers, standards organizations, and other experts.

Challenge: Frontline Defenders Often Have the Fewest Resources

State, local, tribal, and territorial governments and many critical infrastructure owners and operators are among the entities most frequently targeted by cybercriminals and foreign adversaries. They manage sensitive information, operate essential services, and maintain systems whose failure can affect public safety. Yet many lack the funding, personnel, technical expertise, and procurement capacity needed to defend against sophisticated threats.

SLTT governments maintain voter records, tax information, court systems, public health data, emergency communications, and other sensitive resources. They may also own or operate water and wastewater systems, transportation networks, emergency services, and other critical infrastructure. A successful cyberattack can interrupt services, compromise personal information, impose significant recovery costs, and erode public confidence.

Many of these entities rely on aging systems and specialized technologies that cannot be replaced quickly. Operational technology may remain in service for decades because replacement requires significant capital investment, specialized engineering, scheduled downtime, and coordination with vendors. In other cases, organizations may depend on software or equipment that has reached the end of its supported life but remains necessary for daily operations.

End-of-life technology creates particular risk because vendors no longer provide routine security updates, patches, or technical assistance. Vulnerabilities may remain unaddressed, while the organization may lack visibility into the affected systems or the resources to replace them. For smaller governments, utilities, and health care providers, these risks may remain unresolved for years because immediate operational needs take priority over long-term modernization.

Resource constraints also affect the ability to hire and retain cybersecurity personnel, maintain accurate asset inventory, deploy multi-factor authentication, monitor networks, conduct exercises, and respond to incidents. Threat actors understand these weaknesses and often target organizations that are easier to compromise but still provide access to valuable data, trusted networks, or essential functions.

A compromise at a less resourced organization can also create consequences beyond the initial victim. Attackers may use access to a local government, vendor, or service provider to reach other systems, steal trusted credentials, or disrupt interconnected services. The national importance of an entity cannot be measured solely by its size or budget.

Recommendation: Sustain Federal Support and Address Legacy Technology Risk

"Cybersecurity is national security. As threats grow and evolve, we must constantly be at the ready," said Rep. Vince Fong (R-CA), a member of the Cybersecurity and Infrastructure Protection Subcommittee as he hosted a roundtable in April 2026 with Chairman Garbarino, CISA leadership, and local stakeholders from California's Central Valley to discuss the cybersecurity landscape. "That means bringing together leaders from every level of government and the private sector to strengthen our defenses and stay ahead of emerging risks."[268]

Congress should continue and improve programs that help SLTT governments and critical infrastructure entities reduce cyber risk. The State and Local Cybersecurity Grant Program (SLCGP) should be reauthorized and sufficiently funded so that jurisdictions can continue building capabilities that cannot be sustained through local resources alone. The Committee supports the *Protecting Information by Local Leaders for Agency Resilience Act* (H.R. 5078), or *PILLAR Act*, introduced by Rep. Andy Ogles (R-TN), who serves as the Chairman of the Subcommittee on Cybersecurity and Infrastructure Protection.[269] This bipartisan bill makes updates to the program and provides a long-term reauthorization of SLCGP, and it was passed by the House in November 2025.

The program should support risks across information technology, operational technology, and emerging AI systems. Eligible activities should include asset visibility, identity security, incident response, shared services, workforce development, vulnerability management, backup and recovery, and the replacement or mitigation of unsupported technology. Funding should be flexible enough to reflect differences among states and localities while remaining tied to measurable improvements in security and resilience.

Federal support should also encourage durable capabilities rather than one-time purchases that recipients cannot operate or maintain. Shared security services, statewide operations centers, regional partnerships, and pooled procurement can allow smaller jurisdictions to obtain expertise and technology that would otherwise be unaffordable. CISA and FEMA should ensure that grant administration does not impose burdens that prevent the least resourced communities from participating.

Congress should also examine tax incentives, procurement reforms, cost-sharing arrangements, and other mechanisms to reduce risks associated with end-of-life technology. Incentives could encourage vendors to provide limited security support, vulnerability notifications, compensating controls, or transition assistance after routine product support ends. Any such approach should avoid creating an indefinite obligation to maintain obsolete systems or reducing incentives for owners and operators to modernize.

Federal programs should also help entities identify unsupported technology before it becomes a crisis. Asset inventories, vendor disclosure, lifecycle planning, and advance notice of support termination can allow organizations to budget and plan for replacement. Where immediate replacement is not possible, CISA and sector partners should provide practical mitigation guidance that accounts for operational requirements and safety constraints.

Cyber campaigns conducted or supported by foreign governments create national security risks even when the immediate victim is a small locality, rural hospital, or municipal utility. The federal government has a legitimate role in helping frontline entities build resilience. That support should be targeted, accountable, and designed to ensure that essential services remain available before, during, and after a cyber incident.

BORDER SECURITY AND ENFORCEMENT

In the aftermath of September 11, 2001, Congress and the Executive Branch fundamentally reshaped border security and immigration enforcement with the goal of preventing terrorists from exploiting weakness in the immigration system.

Challenge: Incomplete Biometric Entry-Exit Tracking

One of the original recommendations from the 9/11 Commission Report was the implementation of a comprehensive biometric entry-exit system to identify visa overstays. Congress mandated the biometric entry-exit program in 1996 and worked to strengthen the program after the attacks of September 11th. Despite repeated congressional intervention and funding allocations, the program remains incomplete. However, positive steps have been taken toward implementation. CBP expects that airports will have fully implemented biometric exit screening in addition to their completed entry screening later this year.[270] Biometric entry is in the process of implementation at seaports of entry through pilot programs, and pedestrian land entry is complete. Pedestrian land exit programs are still in planning phases. Additionally, biometric entry-exit for vehicle travel, including commercial vehicles, has not been implemented.[271]

Incomplete biometric entry-exit tracking presents a significant challenge to border security, complicating efforts to reliably verify who enters and exits the United States. In the absence of comprehensive biometric verification at both entry and departure, gaps can emerge in immigration enforcement and situational awareness, inhibiting the ability to track the movements of foreign nationals in the United States. These gaps are apparent specifically at land ports of entry, where CBP does not routinely staff exit lanes, and in the lack of a standardized process for nonimmigrants subject to I-94 requirements to voluntarily report their departure.[272]

GAO's 2025 assessment of DHS's acquisition programs indicated that inconsistent funding and shifting priorities have hampered the deployment of biometric entry-exit systems.[273] Biometric entry-exit was originally intended to be funded by congressionally authorized visa application fees, called the 9-11 Response and Biometric Entry–Exit Fee. However, by 2024, revenue had only reached $17.5 million against the $67 million annual program cost.[274]

In 2016, CBP adjusted its approach to biometric exit capability by partnering with airlines and airports to acquire and deploy new technology.[275] While private sector investment in emerging technology reduces the burden on federal partners, substantial changes to the acquisition schedule impacted costs and implementation.[276] U.S. airports have limited secure areas to conduct outbound inspections or checkpoints to capture biometric information and record crossing into the United States.[277] Additionally, at land ports of entry, traffic congestion creates a barrier to recording comprehensive biometrics of the occupants of a vehicle.[278]

In FY 2023, CBP identified 39,005,712 visa holding nonimmigrants that were expected to depart the U.S. by air or sea. Of those, an estimated 510,363 aliens remained in the country after they were scheduled to depart.[279] Without the full implementation of biometric entry-exit at all airports, seaports, and land ports of entry, there is no sure way to identify potential threats or visa overstays that remain in the country illegally.

Recommendation: Full Implementation of Biometric Entry-Exit System

While great progress has been made in the rollout of biometric entry-exit for passengers entering the country, CBP has acknowledged that a comprehensive system for collecting biometric information from departing nonimmigrants remains incomplete. The Committee recommends continued funding and congressional oversight to aid in full implementation of the biometric entry-exit system at all airports with international arrivals and departures, seaports, and land ports of entry. The *OBBBA* provided over $6.1 billion for border security technology, including the continued deployment of biometric entry-exit at ports of entry.[280] While this funding is not allocated to biometric entry-exit in its entirety, CBP has an opportunity to advance the program using a portion of these funds. Given the shortfall in fee-based funding to adequately keep pace with the cost of full implementation of the program, Congress should consider providing additional funding or making modifications to the 9-11 Response and Biometric Entry–Exit Fee to ensure completion.

Challenge: Modernize and Strengthen Screening and Vetting Processes

The 9/11 Commission Report recommends that security measures related to screening and vetting must be continuously adjusted to maintain modernity and address migration patterns.[281] In FY 2024, CBP processed more than 400 million passengers and pedestrians for admission to the United States and arrested another 2.9 million at the border. The same year, the Department of State received 14,245,969 total nonimmigrant visa applications,[282] and USCIS received 12,938,465 applications and petitions requiring adjudication.[283] As AI and machine learning models have consistently shown promise in streamlining and reducing workload on personnel in the private sector, the government has an opportunity to utilize this technology to modernize screening and vetting for visa and petition reviews, as well as the processing of detained individuals.

Recommendation*: *Expand Utilization of Emerging Technologies and International Partnerships

As mentioned previously, the *OBBBA* provided over $6.1 billion for border security technology, including systems that utilize AI to support CBP personnel at the Southwest border.[284] The integration of AI into new and existing infrastructure like NII, tower systems, and other border security technology allows officers and agents to focus on their work in the field while the technology detects and identifies threats at and between ports of entry.

AI and machine learning technology deployed between ports of entry can be programmed to distinguish between a human crossing the border versus another animated object, ensuring resources are deployed when needed. At ports of entry, autonomized systems allow NII equipment to recognize and flag contraband, learning common techniques used to smuggle drugs, weapons, and people into the United States.

During the 118th Congress, Rep. Nick LaLota (R-NY) introduced the *Detection Equipment and Technology Evaluation to Counter the Threat of Fentanyl and Xylazine Act of 2024* (H.R. 8663), or the *DETECT Fentanyl and Xylazine Act of 2024*, which authorized S&T to undertake efforts to improve technologies and equipment for illicit drug detection. The Committee supported this bill, and it was signed into law in December 2024 (P.L. 118-634).[285] As this legislation applied emerging technologies to the Department's border security and drug interdiction mission, a similar approach can be taken to improve screening and vetting processes.

With continued congressional oversight and funding, the Committee recommends additional federal agencies consider the use of artificial intelligence to streamline and improve visa and immigration screening. For example, USCIS and the Department of State could adopt AI or machine learning programs that are trained to detect irregularities or falsified information on visa applications and change of status petitions, potentially improving the accuracy and timeliness of document review.

Finally, the Committee recognizes that protecting the United States often begins far away from its physical borders. In this vein, the Committee also recognizes that TCOs, by definition, operate across borders and that combatting their reach requires an international effort. Both CBP and the Department of State have a long history of partnering with law enforcement in foreign countries to exchange and share information in furtherance of investigations into TCO networks. Initiatives like CBP's Biometric Data Sharing Program (BDSP) are also a key part of this data-sharing ecosystem. The Committee recommends that DHS and the Department of State assess the efficacy of past and present law enforcement fusion centers established in foreign countries and continue to expand these partnerships as prudent. The Committee also recommends a further expansion of the BDSP program to a greater number of countries to increase situational awareness and vetting of travelers who may have a nexus to the United States.

Challenge: Northern Border Security Vulnerabilities

The 9/11 Commission Report emphasizes that the U.S. border system must be integrated into a larger network of screening protections and counterterrorism support. Since FY 2022, hundreds of individuals on the TSDS have been encountered at or between ports of entry at the Northern border each year.[286] Efforts to secure the Southwest border have been effective in decreasing apprehensions and encounters of aliens in the south, but measures must be taken to ensure traffic of aliens and TCOs does not continue shifting north.

Recommendation: Allocate Additional Resources for Northern Border Security

The Committee recommends strengthening Northern border security by increasing personnel assigned to Northern border sectors, improving intelligence sharing between the U.S. and Canada, expanding and modernizing technology in all northern border sectors, building a smart barrier which will serve as a deterrent for would-be illegal border crossers, and improving maritime surveillance around the Great Lakes.

Challenge: Incomplete Deployment of Non-Intrusive Inspection (NII) Technology

The 9/11 Commission Report contains recommendations for the screening of cargo entering the country and the *Implementing Recommendations of the 9/11 Commission Act of 2007* further solidified the need for passenger and cargo screening, especially at airports.[287] Screening of cargo and vehicles at land ports of entry and seaports is imperative to ensure illicit drugs, weapons, including weapons of mass destruction, and potential terrorists do not enter the United States.

Recommendation: Expand the Use of Non-Intrusive Inspection Technology

The Committee recommends expanding the use of non-intrusive inspection technology to include deploying additional large and small scale, as well as handheld, units to screen commercial and passenger vehicles at land ports of entry and at seaports for illicit contraband

such as fentanyl, and other foreign materials. The Committee also recommends expanding the use of artificial intelligence capabilities to detect and identify illicit materials.

During a Border Security and Enforcement Subcommittee hearing on NII in January 2026, Subcommittee Chairman Michael Guest (R-MS) reiterated the importance of continued investments in these capabilities, stating that "regardless of the prior shortcomings in the NII program, the capabilities NII affords to our frontline CBP officers keeping our ports secure are invaluable. We must continue to invest responsibly in NII technology. This technology has a proven track record in facilitating CBP's ability to detect and prevent smuggling into our country."[288]

Emergency Management and Technology

Challenge: Inconsistent Administration of Preparedness Grant Programs

Through its administration of HSGP, including SHSP and UASI, and other grant programs, FEMA assists state, local, tribal, and territorial efforts in preparing for, protecting against, mitigating, responding to, and recovering from acts of terrorism. In the twenty-five years since the September 11th attacks, FEMA's administration of these programs has strengthened information sharing networks between SLTT governments and fusion centers, helped law enforcement and other first responder agencies pay for training and exercise programs, increased security protections for soft targets and crowded places, enhanced cybersecurity resiliency, and supported other security priorities**.**

Witness testimony has consistently identified grant funding as a key resource for supporting counterterrorism operations. For example, during a hearing of the Full Committee on February 24, 2026, "Before the Whistle: Assessing Information Sharing and Security Collaboration Ahead of Major Events," Deputy Chief Joseph Mabin of the Kansas City Missouri Police Department highlighted the following capabilities enabled by receipt of grant funding: "Since 2003, federal homeland security grants—particularly the Urban Area Security Initiative and the State Homeland Security Grant Program—have allowed our region to build a mature, multi-disciplinary preparedness framework. These investments helped establish and continue to sustain the Kansas City Regional Fusion Center, our primary intelligence hub. Through this federal support, we have built interoperable radio communications and strengthened intelligence sharing. We have enhanced specialized response capabilities—including hazmat, explosive ordnance disposal, and tactical weapons of mass destruction (WMD) teams—that train together and can deploy regionwide. We conduct thousands of training hours each year through tabletop, functional, and full-scale exercises. All of this allows for real-time situational awareness and response across jurisdictions."[289]

However, year-to-year changes in grant guidance and administration can cause confusion for grant applicants and recipients, potentially creating gaps in preparedness. In administering the UASI program, for instance, FEMA uses a risk formula to determine which jurisdictions will be funded under the program. Specifically, eligibility "…is determined through an analysis of relative risk of terrorism faced by the 100 most populous Metropolitan Statistical Areas in the United States, in accordance with the *Homeland Security Act of 2002*, as amended."[290] Year-to-year changes in the terrorism risk picture, fluctuations in grant funding levels, and changes in DHS's risk formula can result in jurisdictions losing eligibility for the program.

Additionally, drastic changes to allocated funding amounts for jurisdictions can undermine the ability of states and urban areas to use their funds to plan long-term terrorism risk reduction strategies. During the FY 2025 preparedness grants cycle, after already having received grant applications from recipients, FEMA announced new "final allocations" for states and urban areas under these grant programs which differed significantly from previously announced "target allocations."[291] These abrupt changes instigated legal action which, while ultimately successful in restoring funding back to "target allocation" amounts, delayed the finalization of preparedness grant award amounts until well into the next fiscal year, thereby slowing states' abilities to make critical homeland security investments.[292]

Recommendation: Stabilize Grant Administration with Consistent Processes

In order to streamline grant applications, reviews, and final funding obligations, FEMA should follow consistent grant administration processes and improve communication with Congress and stakeholders. This should include advance notice on changes to National Priority Areas (NPAs) and other eligibility requirements under FEMA grant programs. Lack of clarity in grant eligibility requirements and timelines unnecessarily undermine collective security efforts across the country. Transparency and collaboration are critical to the successful implementation of these grant programs, and the Committee will continue to conduct oversight of FEMA's guidance and processes.

Challenge: Heightened Risks Associated with Special Events

History has repeatedly shown that mass spectator events, particularly major global sporting events, provide a clear opportunity for nation-state adversaries, foreign terrorist organizations, and lone-wolf extremists to conduct acts of terror on the world stage. Indeed, FTOs have been known to exploit high-profile mass gathering events as targets, recognizing their strategic value and vulnerability.[293] Events such as concerts, sporting events, and national commemorations are considered high value for these groups, enabling threat actors to easily achieve broader ideological or destabilization objectives.[294] These patterns are especially concerning given that the United States will continue to host major international special events over the course of the next decade, including the 2028 Los Angeles Summer Olympics and Paralympics and the 2034 Salt Lake City Winter Olympics and Paralympics.

Recommendation: Ensure Sufficient Funding for Special Events in Advance

In advance of several major special events, including the 2026 Fédération Internationale de Football Association (FIFA) World Cup, America250 and Freedom250 celebrations, and the 2028 Los Angeles Summer Olympics and Paralympics, the Committee worked to secure supplemental security funding through the *One Big Beautiful Bill Act* (H.R. 1), or *OBBBA*. As a result of the Committee's work, the *OBBBA* provided $625 million to enhance security for the 2026 FIFA World Cup, $1 billion for the 2028 Los Angeles Olympics and Paralympics, and $500 million to allow SLTT law enforcement agencies to purchase Counter-Unmanned Aircraft Systems (C-UAS) detection and mitigation equipment.[295]

While FEMA has not yet finalized plans to administer funds for the 2028 Los Angeles Summer Olympics and Paralympics, it should review its management and administration of supplemental FIFA World Cup security funds to better support its administration of related grant programs for future special events. In completing its assessments, FEMA should work with

SLTT jurisdictions and its DHS intelligence partners to collect data as appropriate and collaborate with Congress to share its assessments ahead of any legislative initiatives to provide funds for future major special events like the 2034 Salt Lake City Winter Olympics and Paralympics.

In advance of major special events in 2026, the Committee formed a Task Force on Enhancing Security for Special Events in the United States (Task Force). Under the guidance of Task Force Chairman Michael T. McCaul (R-TX) and Task Force Ranking Member Nellie Pou (D-NJ), the Task Force has conducted oversight and investigated security needs for special events.[296]

Challenge: Strengthening Core Preparedness and Incident Management Capabilities

As a result of the issuance of PPD-8, effective establishment of the National Preparedness System (NPS), in pursuit of the National Preparedness Goal (NPG), became a core component of NIMS and incident command implementation. The NPG, defined as "a secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk," is composed of five mission areas and features thirty-two identified core capabilities corresponding to one or more of the mission areas.[297] For localities that often lack sufficient resources, maturing these core capabilities on their own can be difficult.

The NPS outlines an organized process for preparedness activities to achieve the NPG. Within the implementation of the NPS, NIMS is key for building and strengthening capabilities, enabling the prioritization and effective allocation of limited resources, and providing flexible and standardized all-hazards incident support.[298] NIMS also underlies principles of mutual aid; indeed, the National Emergency Management Association, which works to administer the Emergency Management Assistance Compact, an all-hazards mutual aid compact serving all states and several territories,[299] has incorporated NIMS guidance by including such information as resource typing and job position qualifications into mutual aid request and offer processes between jurisdictions.[300]

Available tools for states and local communities to operationalize the NPS in pursuit of the NPG include the Threat and Hazard Identification and Risk Assessment (THIRA) and the Stakeholder Preparedness Review (SPR). The THIRA helps communities understand their risks and determine the level of capability needed to address those risks.[301] The SPR is a self-assessment of a jurisdiction's current capability levels against the targets identified in the THIRA.[302] FEMA uses the data collected through the THIRA and SPR processes to disseminate annual National Preparedness Reports detailing trends in threats, hazards, and persistent and emerging capability gaps. Recent editions of the National Preparedness Report have discussed the need for states and regions to continue to expand on their efforts to build core capabilities, including in the areas of mass care services and infrastructure systems.[303] Ultimately, the success of NIMS implementation into the NPS depend upon the abilities and propensities of states and localities to recognize preparedness gaps and strengthen their core capabilities.

Recommendation: Continued Funding for the Emergency Management Performance Grant (EMPG)

FEMA's various preparedness grants, including SHSP, UASI, and the Emergency Management Performance Grant (EMPG), are provided to jurisdictions with the goal of building and strengthening core capabilities,[304] and completion of both the THIRA and the SPR are required to receive funds through FEMA's preparedness grant programs.[305]

Witnesses before the Committee emphasized the importance of FEMA's preparedness initiatives in hearing testimony. Ms. Carrie Speranza, CEM, President of the U.S. Council of the International Association of Emergency Managers, stated the following in her testimony before the Subcommittee on Emergency Management and Technology in March 2025: "FEMA must maintain its role in driving change through its preparedness programs. These programs serve as the underlying foundation from which all local and state emergency management capabilities are derived. Through this investment, FEMA helps to establish national standards for state and local personnel so that assets can be provided through mutual aid. This capability is essential, as illustrated by Hurricanes Helene and Milton, where over 6,300 public safety personnel deployed for 290 mutual aid missions. Preparedness is not a matter of insurance before a disaster. Instead, these FEMA preparedness programs provide assurances that we can aid each other in times of disaster, and preparing through planning, training, exercising, and standardization is crucial."[306]

At the same hearing, Mr. Daniel Kaniewski, a former FEMA Deputy Administrator of Resilience, noted that "FEMA's pre-disaster programs – such as the Homeland Security Grant Program… – incentivize resilience."[307]

EMPG focuses on the building, sustaining, and maturation of the thirty-two core capabilities as defined in the NPG. EMPG awards all fifty-six states and territories a base amount of available funding and distributes the remaining balance of the funding according to population share.[308] Furthermore, projects funded by EMPG are not to exceed a federal cost share of more than fifty percent, ensuring that states and local communities are incentivized to spend their own resources on building emergency management and response capacity.[309]

Witness testimony has also attested to the effectiveness of the EMPG program. In his testimony before the Subcommittee, Mr. Timothy Manning, a former FEMA Deputy Administrator for Protection and National Preparedness, described EMPG as "the backbone of emergency management in America," and stated that "EMPG is the program that supports the vast majority of state and local government emergency management programs from emergency operations centers to preparedness and response teams, and disaster training and exercises. Without it, few states and local governments could support the level of preparedness and response that America currently enjoys."[310]

The Committee therefore urges continued and reliable funding for FEMA preparedness grant programs, including SHSP, UASI, and EMPG, for the purposes of building core capabilities across the five mission areas of the NPG throughout the nation.

Challenge: Lack of Standard NIMS Implementation

The effectiveness of the NIMS framework in coordinating all-hazards response across jurisdictions depends on the ability of incident management personnel to respond to any number of potential disaster scenarios with a standardized level of capability. Effective training is critical to building a common understanding and ensuring that responders apply NIMS concepts across SLTT jurisdictions and partners.[311]

Recommendation: Effective Training and Reauthorization of the National Domestic Preparedness Consortium (NDPC)

DHS partners with and funds the National Domestic Preparedness Consortium (NDPC) to build all-hazards preparedness and response capacity for state and local partners. The NDPC works to deliver training to SLTT partners through the partnership of seven member institutions,[312] each specializing in a different component of emergency preparedness and response:

- The Center for Domestic Preparedness (CDP) in Anniston, Alabama, FEMA's premier all-hazards training institution, provides trainees with expertise in handling CBRN and explosive threats through its Chemical, Ordnance, Biological, and Radiological Training Facility. Additionally, the CDP's Advanced Responder Training Complex simulates real-life environments to prepare trainees to handle a variety of man-made and natural disasters, and the CDP's Noble Training Facility is the only hospital facility in the nation that provides disaster preparedness and response training to hospital staff and healthcare professionals.[313]
- The Texas A&M Engineering Extension Service's National Emergency Response and Recovery Training Center in College Station, Texas, provides all-hazards competence in areas such as cybersecurity, crisis communications, hazardous materials awareness and operations, health and medical services, infrastructure protection, search and rescue, and threat and risk assessment, among other items.[314]
- The Energetic Materials Research and Testing Center at New Mexico Tech in Socorro, New Mexico, specializes in teaching trainees how to respond to threat scenarios pertaining to explosives, incendiary devices, and UAS.[315]
- The National Center for Biomedical Research and Training/Academy of Counter-Terrorist Education at Louisiana State University in Baton Rouge, Louisiana, focuses on providing expertise in responding to CBRN and WMD threats, counterterrorism operations, and preparedness for high-consequence events affecting a variety of disciplines and sectors.[316]
- The National Disaster Preparedness Training Center at the University of Hawaii in Honolulu, Hawaii, is the only member of the NDPC whose primary mission entails cultivating preparedness for natural disasters.[317]
- The U.S. Department of Energy's (DOE) National Nuclear Security Administration's Counterterrorism Operations Support Center for Radiological/Nuclear Training program located at the Nevada National Security Site works to provide SLTT emergency managers with expertise in responding to terrorist use and deployment of radiological and nuclear weapons.[318]
- MxV Rail's Security and Emergency Response Training Center in Pueblo, Colorado, provides training to SLTT law enforcement, emergency response officials, and hazardous materials (HAZMAT) teams to be able to respond to surface transportation and hazardous materials emergencies.[319]

Since its inception, the NDPC, through its constituent partners, has delivered training to over 4,200,000 partners.[320] While the NDPC continues to receive annual appropriations, its authorization in statute has lapsed, rendering the consortium and its mission vulnerable to administrative uncertainty. To ensure that state and local law enforcement, first responders, and

emergency managers continue to receive all-hazards training in pursuit of strengthening core capabilities, the Committee supports Congress formally reauthorizing the consortium.

Challenge: Dissolution of the Countering Weapons of Mass Destruction Office (CWMD)

Though not thoroughly considered within the scope of the 9/11 Commission Report, DHS has played an important role in providing for domestic security measures against WMDs, including CBRN threats, especially following a series of anthrax attacks which occurred not long after 9/11 (in an incident otherwise known as "Amerithrax").[321] The 9/11 Commission did warn that Al Qaeda had tried to acquire weapons of mass destruction for years and that the United States would continue to be a prime target for terrorist organizations if they were able to gain access to those weapons.[322]

Initially, DHS efforts to counter WMD threats were spread across different components and agencies. The Domestic Nuclear Detection Office (DNDO) was established within DHS as the lead agency within the U.S. government for implementation of domestic nuclear detection efforts, including a managed and coordinated response to radiological and nuclear threats, as well as integration of federal nuclear forensic programs.[323] The Office of Health Affairs (OHA) led coordination of DHS biological and chemical defense activities and operated the National Biosurveillance Integration Center (NBIC), the designated government entity charged with integration, analysis, and dissemination of the nation's biosurveillance information.[324]

In December 2017, using authorities provided under section 872 of the *Homeland Security Act of 2002*,[325] the Secretary of Homeland Security reorganized the various DHS CBRN functions into a new Countering Weapons of Mass Destruction Office (CWMD). The intent of the new CWMD Office was to elevate and streamline DHS efforts to prevent terrorists from using WMDs against the United States. On December 21, 2018, President Trump signed the *Countering Weapons of Mass Destruction Act of 2018* into law to fully establish and authorize CWMD, combining DNDO and the majority of OHA.[326]

Though CWMD's statutory authorization was sunset on December 21, 2023, it had maintained operations for years through funding provided in successive continuing resolutions. Ultimately, the FY 2026 President's Budget Request proposed dissolving CWMD and moving its personnel and functions to other DHS components,[327] which was enacted following the passage of FY 2026 DHS appropriations, albeit in a different structure than proposed in the budget request.[328]

Recommendation: Ensuring Continuity of DHS CBRN Functions

CWMD was responsible for administering several CBRN security initiatives, such as the BioWatch program, Securing the Cities (STC), Mobile Detection Deployment Program (MDDP), and NBIC. The BioWatch program is a monitoring system that collects and tests air samples for biological agents likely to be used in a bioterrorism attack. The monitoring system is in over 30 major metropolitan areas across the United States, and the program is locally operated through a cooperative funding agreement with DHS.

The STC program provides financial assistance and equipment to state, local, and tribal organizations to develop robust regional detection that seeks to prevent the successful planning, movement, and deployment of nuclear or radiological weapons and component materials within the United States.[329] CWMD's MDDP program similarly seeks to provide detection and

monitoring capabilities and equipment to support state and local law enforcement agencies to effectively counter CBRN threats. MDDP units, which include equipment and technical support personnel, "are typically deployed to support federal and SLTT law enforcement partners as they secure special, large-scale events such as concerts, marathons, parades, and college and professional sports."[330]

NBIC is responsible for analyzing information about health and disease events to ensure that the nation's response is well-informed and minimizes impacts to public health and the economy. NBIC serves as a bridge between federal and SLTT partners to integrate information from thousands of sources about biological threats to humans, animals, and plants.[331]

Now dissolved, CWMD's functions have been transferred to components and agencies throughout DHS, in accordance with enacted FY 2026 appropriations. FEMA absorbed CWMD's federal assistance portfolio, to include BioWatch, STC, and MDDP, while the Office of Health Security (OHS) took on management of NBIC. Furthermore, S&T incorporated CWMD's research and development (R&D) portfolio into its own activities, and U.S. Customs and Border Protection (CBP) acquired CWMD's role in procuring large-scale radiation portal monitors.

With the recency of the transition of these functions, it remains too soon to tell how the effectiveness of these various missions may be impacted, or if further consolidation or transition will be prudent or necessary. Though the Committee's oversight into this matter is ongoing, it recognizes the importance of DHS's various CBRN security functions and will consider legislation if necessary to ensure that DHS continues to keep the American public safe from WMDs.

Challenge: Ensuring Reliable Detection and Characterization of Bioterrorist Threats

Even before the dissolution of CWMD and the dispersal of its functions, the BioWatch system had been routinely criticized due to its inability to inform officials of threats in real-time and the common occurrence of false alarms stemming from its failure to always distinguish between harmless germs and the lethal pathogens that terrorists would be likely to unleash in an attack.[332]

In 2019, DHS began a major acquisition program, the Biological Detection for the Twenty First Century (BD21), to move toward the next generation of national biodetection. The BD21 program was intended to address some of BioWatch's limitations, including shortening the detect-to-warn timeline, and providing more efficient detection of an aerosolized attack involving a biological agent.[333] However, the effort stalled.

Recommendation: Improve Biodetection Capabilities and Support Granting Statutory Authorization to the National Biodefense Analysis and Countermeasures Center (NBACC)

To address these longstanding concerns related to the BioWatch program, Subcommittee on Emergency Management and Technology Chairman Strong introduced the *DHS Biodetection Improvement Act* (H.R. 706).[334] As the technology behind the BioWatch program was initially developed in coordination with the DOE national laboratories, this bill would require DHS to submit a strategy for how it will coordinate with DOE to address biodetection research and development. It will help DHS establish a blueprint for what the next generation of biological detection should look like. This bill was passed by the House in March 2025.

The Committee also recommends that Congress take steps to strengthen DHS's other equities in the biosecurity and biodefense mission space. In the aftermath of the 2001 anthrax attacks, DHS established the National Biodefense Analysis and Countermeasures Center (NBACC).[335] NBACC, the first DHS national laboratory, supports intelligence assessments, preparedness planning, response, emerging threat characterization, and bioforensic analyses through its two facilities, the National Bioforensic Analysis Center (NBFAC) and the National Biological Threat Characterization Center (NBTCC).[336] NBACC also plays an important role in assisting federal law enforcement, including the FBI, in biocrimes and investigations.[337] Despite the importance of NBACC's mission set, it has never been formally authorized by Congress. To ensure the continuation of the laboratory's vital work in biothreat characterization and bioforensic analysis, the Committee recommends Congress consider legislation to codify the functions of the NBACC facility.

Challenge: Countering Emerging Agroterrorist Threats and Ensuring Intergovernmental Collaboration

In June 2025, the DOJ charged several Chinese nationals associated with the University of Michigan in connection with attempts to smuggle potentially dangerous biological agents into the country.[338] One of the identified biological agents, *fusarium graminearum*, was a fungus classified as a potential agroterrorist weapon known to cause "head blight," a disease of wheat, barley, maize, and rice, which is responsible for billions of dollars in economic losses worldwide each year.[339] These occurrences highlighted the scale of the threat that foreign nation-state adversaries, agroterrorist actors, and other malicious actors pose to the food and agriculture critical infrastructure sector of the United States.

Threats to the food and agriculture critical infrastructure sector are not new. In November 2022, President Biden signed National Security Memorandum 16 (NSM-16), "Strengthening the Security and Resilience of United States Food and Agriculture,"[340] which mandated the creation of an Interim Risk Review to identify major threats to the food and agriculture critical infrastructure sector and identify mitigation strategies.[341] CBRN threats in particular have the potential to plague the critical infrastructure sector and its related industries. Intentional CBRN attacks against food and agriculture are often conducted to achieve economic destabilization, loss of trust in government, and the spreading of mass social panic. CBRN threats can also be conducted to impact public human health. Certain biological threats, including specific transboundary animal diseases, are zoonotic, and thus capable of being transmitted from animals to humans.

Recommendation: Improve Agroterrorism Preparedness and Resilience at All Levels of Government

The Committee has found that preparedness exercises that bring together various stakeholders at all levels of government and the private sector have the potential to significant improve collective readiness. Following two oversight hearings on agroterrorism, Subcommittee on Emergency Management and Technology Chairman Strong introduced the *Civil Preparedness for Agroterrorism Exercise Act of 2026* (H.R. 9394).[342] This bill would require DHS to conduct an exercise aimed at enhancing prevention, response, recovery, and mitigation efforts pertaining to agroterrorism within four years of enactment, and would require the participation of relevant federal, state, and local agencies, as well as private sector owners and operators of agricultural and related critical infrastructure.

In testimony before the subcommittee in February 2026, Ashley Grant, Ph.D., MPH, the Senior Health Security and Biodefense Advisor for DHS OHS, spoke to the effectiveness of existing exercise initiatives to mitigate the impacts of unintentionally introduced disease threats to food and agriculture, such as New World screwworm: "…on January 14, 2026, OHS led a comprehensive tabletop exercise in El Paso, Texas, focused on strategic preparedness and response to potential New World screwworm (NWS) infestations… OHS worked across the federal interagency and with state, local, and tribal partners to convene over 250 participants including operational decision-makers from federal, state, local, and tribal agencies, representing law enforcement, public health, agriculture, environmental response sectors, and other critical partners… Key outcomes included strengthened coordination and identification of planning and capacity gaps, including the need for targeted education and outreach to a broader set of stakeholders. The exercise also highlighted trade implications, laboratory bottlenecks, and the importance of an approach that integrates clinical, public health, food, agriculture, and veterinary sectors."[343]

The *Civil Preparedness for Agroterrorism Exercise Act of 2026* would strengthen state and local biological threat preparedness by ensuring that DHS is engaging relevant stakeholders in conducting an exercise pertaining to biological disease threats which are maliciously introduced by agroterrorism actors. Given the potential vulnerabilities to the U.S. food and agriculture sector demonstrated by the incidents at the University of Michigan, the Committee supports swift passage of the bill.

While not specific to agroterrorism, the Committee also supports the *Weatherizing Infrastructure in the North and Terrorism Emergency Readiness Act of 2025* (H.R. 3106), led by Rep. Tim Kennedy (D-NY), the Ranking Member of the Subcommittee on Emergency Management and Technology, which requires DHS to develop and conduct an exercise with various stakeholders to enhance preparedness for a terrorist attack occurring during an extreme cold weather event, with particular focus on the potential cascading impacts on critical infrastructure. This bill was passed by the House in July 2026.

Challenge: Expiration of FirstNet Authorization

Since the authorization of the FirstNet Authority within the National Telecommunications and Information Administration (NTIA) in 2012, FirstNet has become increasingly relied upon to provide broadband-based communication services to public safety agencies, such as law enforcement, fire, and rescue and emergency medical responders. Recent estimates indicate that over 31,000 public safety agencies and organizations in the United States are subscribed to the FirstNet network.[344]

Despite this considerable level of adoption, however, the FirstNet Authority's statutory authorization is currently set to expire in February 2027. The failure to reauthorize FirstNet would introduce a great deal of uncertainty into the future of the program, including with regards to what other federal entity, if any, will continue to operate the network. This uncertainty may contribute to a loss of service for the public safety agencies who utilize FirstNet.

Recommendation: Support FirstNet Reauthorization

Recognizing the vital role that FirstNet plays within the realm of public safety, especially in light of the network's dedicated spectrum and continuous priority coverage for first responders, the Committee views a potential lapse in authorization for FirstNet and loss of coverage for first responders relying on the network as an unacceptable outcome that would reverse important gains made since the September 11th attacks. To ensure that public safety agencies continue to benefit from reliable broadband-based communications networks, the Committee supports efforts to reauthorize FirstNet. The *First Responder Network Authority Reauthorization Act of 2026* (H.R. 7386), was passed by the House on April 20, 2026.[345]

Challenge: Rising Demand for SAFETY Act Liability Protections

Pursuant to the *Support Anti-Terrorism by Fostering Effective Technologies* (*SAFETY*) *Act*, which was included within the *Homeland Security Act of 2002*,[346] DHS is authorized to provide incentives for the development and deployment of anti-terrorism technologies by creating systems of risk and litigation management. DHS S&T accomplishes this through the Office of SAFETY Act Implementation (OSAI), which evaluates applications for technologies to receive *SAFETY Act* liability protections. Approved technologies receive degrees of liability protection in accordance with the technology's demonstrated effectiveness and reliability, ranging from developmental testing and evaluation designation (DTED) technologies, designated technologies, and certified technologies. DTED technologies receive the fewest liability protections, while certified *SAFETY Act* technologies receive the most robust degree of liability protection.[347]

However, *SAFETY Act* applications have increased significantly. In a January 2026 hearing before the Committee, DHS Under Secretary for Science and Technology Pedro M. Allende stated that S&T's OSAI had experienced "a 50% increase in applications which [S&T] attribute[d] to [the] FIFA [World Cup], LA 2028, and America250" events.[348]

Recommendation: Increased Funding for OSAI

To ensure that private sector stakeholders do not experience disincentives preventing the development or deployment of anti-terrorism technologies that contribute to a culture of preparedness, it is imperative that the DHS S&T OSAI receive sufficient resources to keep pace with the rise in demand of liability protections resulting from emerging market trends. The FY 2027 DHS S&T Congressional Budget Justification requested an additional $12,000,000 for OSAI to address the anticipated rise in demand for liability protections due to upcoming high-threat profile special events.[349] The Committee was pleased to see this request for additional funds and supports funding OSAI at an appropriate level so that it may provide risk and liability protections for qualified anti-terrorism technologies within an appropriate timeframe.

SUPPORTING 9/11 RESPONDERS AND SURVIVORS

Supporting 9/11 Responders and Survivors

In conjunction with national efforts to strengthen homeland security in the days, months, and years following the attacks of September 11, 2001, the United States also managed a more tangible effort: cleaning up the sites of the attack so that the nation could begin to rebuild. In less than one year, workers, first responders, and volunteers cleared 1.8 million tons of debris from the World Trade Center, finishing three months ahead of schedule.[350] Despite this impressive feat, complications emerged soon thereafter as those operating at Ground Zero began receiving diagnoses of various illnesses and cancers at an alarming rate.

Following the attacks, the Environmental Protection Agency (EPA) declared that the air and water near Ground Zero was safe to breathe and drink.[351] Based on this assessment, personnel engaged in rescue and recovery efforts were not adequately advised to take necessary precautions to reduce risk of exposure to the toxic substances present at the site. This erroneous advice resulted in the exposure of over 400,000 individuals to hundreds of hazardous chemicals, the effects of which continue to persist twenty-five years later.[352]

It was not until 2011 – ten years after 9/11 – that comprehensive legislation aimed at providing support for those diagnosed with chronic illnesses and cancers was implemented. The *James Zadroga 9/11 Health and Compensation Act of 2010* established the World Trade Center Health Program (WTCHP) to meet this need. [353] Administered by the National Institute for Occupational Safety and Health (NIOSH) within the Centers for Disease Control and Prevention (CDC), the program provides a mechanism for federal payment of "medically necessary treatment of certified conditions, as well as any medically associated health conditions" for individuals who receive medical diagnoses relating to rescue and recovery efforts at the World Trade Center, Pentagon, and Shanksville, Pennsylvania.[354]

In 2015, Congress passed the *James Zadroga 9/11 Health and Compensation Reauthorization Act* as part of the *Consolidated Appropriations Act, 2016,* reauthorizing the program until 2090.[355] In 2019, the limits on WTCHP responder and survivor enrollments were increased to address growing cases of 9/11-related diagnoses.[356] In 2023, the WTCHP received increased funding, and the program was required to engage in research efforts concerning health and education impacts of exposure to 9/11-related toxins on individuals aged twenty-one and younger at the time of the attacks.[357] In 2024, the WTCHP received additional funding, and enrollment eligibility was expanded to include military personnel and federal employees and contractors at the Pentagon and Shanksville.[358]

To eliminate the risk of future funding shortfalls, a permanent solution was required to ensure continued solvency of the WTCHP. Following the bipartisan efforts of Chairman Garbarino in the House, and Senator Kirsten Gillibrand (D-NY) in the Senate, the calculation for the program's annual appropriation was amended, so that funding is now proportional to enrollment trends instead of being based on increases in the consumer price index.[359] This change provided a permanent fix to the program's funding calculation, eliminating the risk of cuts or disruptions and upholding the promise of care for 9/11 responders and survivors.

Today, the WTCHP provides critical medical monitoring and treatment services to more than 140,000 9/11 responders and survivors across all fifty states and in 434 of 435 congressional districts. Since the attack, 9/11-related illnesses have claimed more lives than those lost in the initial attacks, with more diagnoses and deaths reported each day.[360] As program enrollments and

identification of 9/11-related illnesses continue, so too must Congress' efforts to ensure the WTCHP has the resources and support needed to uphold the program's mandate.

The Committee also recognizes the invaluable work and contributions of Dr. John Howard, MD, in his role as Administrator of the WTCHP. His steadfast commitment and dedication to serving its members have been essential to the success of the program since its creation in 2011. The Committee emphasizes the importance of stable leadership and staffing of the WTCHP to ensure care and resources are provided to those who need it in an efficient and effective manner. The Committee additionally recognizes the importance of ensuring the WTCHP covers all diseases affecting victims and the need to continue evaluating additional diseases for eligibility as new research emerges.

As the nation remembers the bravery and sacrifice of those lost on September 11, 2001, we must also recognize the countless individuals who are still confronting the effects of the attacks twenty-five years later. The United States is indebted to all those who contributed to the rescue and recovery efforts in the days, months, and years that followed. Their service to the nation shall never be forgotten.

Conclusion

The United States must remain ever vigilant against foreign and domestic threats to homeland security. As identified in the Committee's analysis of homeland security successes, developments, and priority areas for improvement in the twenty-five years since September 11, 2001, the nation has in many respects made significant progress toward bolstering national security and ensuring the safety of the American people. Such progress is notably exemplified by the nation's recent successes in facilitating the safety and security of 2026 FIFA World Cup teams and spectators, and the general public at America250 and Freedom250 celebrations across the United States. In anticipation of these events, the Committee focused intently on the rapidly evolving threat posed by malicious drones, ensuring that federal and SLTT law enforcement partners had the authorities and training needed to conduct C-UAS operations during the World Cup games and semiquincentennial celebrations.

To that end, the federal government has made great strides toward implementing the 9/11 Commission's original forty-one recommendations. At the same time, this no-fail mission will live on in perpetuity, requiring the constant commitment of current and future generations to the safety and security of the United States.

As examined by the Committee, various Commission recommendations remain unfulfilled due to delays in implementation and the changing nature of the modern threat picture, which includes new challenges that could not have been contemplated in the early 2000s.

Developments in terrorist activity and organizational structures, the rise of homegrown violent extremism and lone wolf actors, and the role that the internet plays in expanding the reach and influence of U.S. adversaries has challenged the homeland security enterprise's historical focus on foreign-based terror groups. This has made it easier than ever before for malign actors to direct and conduct domestic attacks against the United States, even with limited resources and training. Identified resurgences of intelligence siloing must also be immediately corrected, as these very lapses in information sharing played a significant role in the ability of the attacks of September 11th to be carried out. The federal government must enhance its ability to share timely and efficient intelligence across the IC, as well as to state and local law enforcement through the DHS Office of Intelligence and Analysis. Doing so will enhance the nation's ability to identify, respond to, and prevent threats to the homeland.

The rise of cyber as an attack vector and advancements in artificial intelligence, especially agentic AI, has further complicated contemporary homeland security practices. The nation increasingly relies on interconnected services and critical infrastructure, elevating the risk of cascading effects of cyberattacks even when specific services or infrastructure have not been directly targeted by our adversaries. Developments in artificial intelligence have also made it easier for unsophisticated threat actors to conduct complex attacks against the United States that would have previously required far greater resources and planning. As the U.S. works to address the national security implications of the emergence of cyber and AI-related threats, Congress and the Executive Branch must work closely with SLTT and private sector partners to ensure federal efforts align with operational realities and strengthen cybersecurity without hampering competition and innovation.

The United States must similarly maintain a robust aviation security system. It is essential that TSA have the resources and support necessary to protect the traveling public. This can be

accomplished through continued congressional and Executive Branch support for the research, development, testing, and evaluation of innovative screening and vetting technologies, as well as stable, reliable funding streams oriented toward safety and efficiency. At the same time, the federal government must work to improve the traveler experience through enhanced passenger risk assessment and targeted resource allocation to decrease low-risk passenger wait times while maintaining TSA's rigorous security standards.

SLTT partners must similarly have the support and resources necessary to enhance counterterrorism preparedness, response, and mitigation capabilities. A key factor in accomplishing this objective is promoting stability in annual homeland security program and grant funding allocations. Recent delays and inconsistencies in the disbursement of federal funding to states and localities have resulted in unnecessary and preventable challenges for law enforcement and first responders amidst a rising national threat environment. The federal government should exist as a trusted and reliable partner in the nation's shared homeland security mission. Challenges resulting from the management of recent grant and programmatic funding cycles should be swiftly remediated to prevent future delays and improve federal and SLTT collaboration when it comes to national security.

Finally, as the nation continues to strengthen its homeland security capabilities to counter twenty-first century threats, the United States must take care to uphold long-established civil liberties and privacy protections. Intelligence and threat assessment activities must maintain strict compliance with constitutional limitations on information gathering, and those handling sensitive data must be held to the highest standards. Congress and the Executive Branch must continue to engage in rigorous oversight of the homeland security enterprise to make sure the right balance is struck between public safety and personal privacy.

In the twenty-five years since the attacks of September 11, 2001, the United States has continued to meet the moment when faced with new and emerging threats. In keeping with the mandate of ensuring the nation is never again subject to a catastrophic terror attack on U.S. soil, the Committee on Homeland Security's review of the state of national security twenty-five years later serves to further this objective through ongoing assessment and identification of policy and oversight objectives to strengthen the United States' ability to protect the homeland and keep the American people safe from harm.

As the only House Committee created as a direct result of post-9/11 national security reforms, the Committee has undertaken this effort in solemn remembrance of those lost on September 11, 2001, and in the years thereafter, to whom the Committee and the nation owe an immeasurable debt. While the United States' homeland security mission will never be finished, it is the Committee's objective that this report shall serve as a valuable benchmark for current and future national security professionals as they continue this vital work.

As the first generation born post-9/11 begins to enter the workforce, it is essential that future national security leaders understand how the attacks of September 11, 2001, have shaped the direction of homeland security policy over the last twenty-five years, and why continued commitment to this objective must never wane. Such knowledge not only ensures the legacies of those lost live on, but also serves as a continuous reminder of what is at stake when vigilance falters.

To this end, the Committee will once again convene in New York City on the 25th anniversary of the attacks to visit the 9/11 Memorial and Museum and pay tribute to those lost, as will countless others at the Pentagon and in Shanksville, Pennsylvania. The Committee also supports recent funding for the expansion of the Pentagon's 9/11 educational footprint. As the only 9/11 attack site without a public education center, this funding will support ongoing efforts to expand 9/11 educational opportunities across the National Capital Region. Such education is invaluable in ensuring our nation upholds the promise to "Never Forget."

As we approach the twenty-fifth anniversary of the attacks of September 11, 2001, the United States of America remains steadfast in its commitment to safeguarding the nation against threats to the homeland and the Committee extends its sincere gratitude to all those who dedicate their careers and their lives to this collective mission.

Appendices

Official Committee Activity

FULL COMMITTEE

Hearing: "Unconstrained Actors: Assessing Global Cyber Threats to the Homeland." January 22, 2025.

Hearing: "Preparing the Pipeline: Examining the State of America's Cyber Workforce." February 5, 2025.

Hearing: "Innovation Nation: Leveraging Technology to Secure Cyberspace and Streamline Compliance." May 28, 2025. *Field Hearing, The Hoover Institution at Stanford University, 426 Galvez Mall, Stanford, CA*

Briefing on Scattered Spider. September 9, 2025.

Briefing with General Paul M. Nakasone (U.S. Army, Ret.). November 18, 2025.

Hearing: "Worldwide Threats to the Homeland." December 11, 2025.

Hearing: "Oversight of the Department of Homeland Security: CISA, TSA, S&T." January 21, 2026.

Hearing: "Before the Whistle: Assessing Information Sharing and Security Collaboration Ahead of Major Events." February 4, 2026.

Classified Briefing on PRC Typhoon-Cluster Campaigns. February 4, 2026.

Briefing on AI and National Security (1). March 18, 2026.

Hearing: "Funding Lapse and Security Gaps: Assessing the Harmful Impacts of the DHS Shutdown on Americans." March 25, 2026.

Briefing on AI and National Security (2). April 16, 2026.

Event: "Demo Day: Jailbreaking AI in Real Time" April 22, 2026.

Briefing on Mythos Preview. May 13, 2026.

Hearing: "TSA Modernization: Industry Perspectives on Key Security and Travel Reforms 25 Years After 9/11." May 20, 2026.

Briefing on AI and National Security (3). June 9, 2026.

Hearing: "A Review of the Fiscal Year 2027 Budget Request for DHS." June 3, 2026.

COUNTERTERRORISM AND INTELLIGENCE

Hearing: "The Digital Battlefield: How Terrorists Use the Internet and Online Networks for Recruitment and Radicalization." March 4, 2025.

Hearing: "The Rise of Anti-Israel Extremist Groups and Their Threat to U.S. National Security." June 11, 2025.

Briefing: "Outpaced and Outdated: Addressing the Definitional Discrepancies, Implementation Gaps, and Resource Constraints Hindering U.S. Efforts to Combat Domestic Terrorism." December 18, 2025.

Briefing with DHS Office of Intelligence & Analysis. January 14, 2026.

Site Visit to United States Secret Service Accelerated Candidate Event. February 27, 2026. *Leesburg, Virginia*.

Briefing with United States Secret Service. March 24, 2026.

Briefing: "Partnership in Action: A Roundtable Focused on DHS's Coordination with Law Enforcement." May 14, 2026.

Briefing on Nihilistic Violent Extremism. June 25, 2026.

Site Visit to International Police Coordination Center. July 7, 2026. *Leesburg, Virginia.*

TRANSPORTATION AND MARITIME SECURITY

Hearing: "Examining the PRC's Strategic Port Investments in the Western Hemisphere and the Implications for Homeland Security." February 11, 2025.

Hearing: "America on the Global Stage: Examining Efforts to Secure and Improve the U.S. Travel System and Prepare for Significant International Events." April 8, 2025.

Hearing: "Beijing's Air, Space, and Maritime Surveillance from Cuba: A Growing Threat to the Homeland." May 6, 2025.

Hearing: "From Cartels to Coastlines: An Examination of U.S. Federal Efforts to Confront Illicit Maritime Activities in U.S. Waters." June 10, 2025. *Joint Hearing with the Subcommittee on Border Security and Enforcement*

Hearing: "Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home." July 15, 2025.

Hearing: "Securing Global Communications: An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure." November 20, 2025.

Hearing: "Frontline Defenders: How the Coast Guard's Deployable Specialized Forces Combat Narcoterrorists and other Maritime Threats on the High Seas." February 3, 2026.

Site Visit to DCA TSA Systems Integration Facility. July 23, 2026. *Ronald Reagan Washington National Airport, Arlington, Virginia.*

Cybersecurity and Infrastructure Protection

Hearing: "Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime." March 11, 2025.

Hearing: "Cybersecurity is Local, Too: Assessing the State and Local Cybersecurity Grant Program." April 1, 2025.

Hearing: "*In Defense of Defensive Measures: Reauthorizing Cybersecurity Information Sharing Activities that Underpin U.S. National Cyber Defense.*" May 15, 2025.

Hearing: "*Security to Model: Securing Artificial Intelligence to Strengthen Cybersecurity.*" June 12, 2025.

Hearing: "*Fully Operational: Stuxnet 15 Years Later and the Evolution of Cyber Threats to Critical Infrastructure.*" July 22, 2025.

Hearing: "*The Quantum, AI, and Cloud Landscape: Examining Opportunities, Vulnerabilities, and the Future of Cybersecurity.*" December 17, 2025. *Joint Hearing with the Subcommittee on Oversight, Investigations, and Accountability*

Hearing: "*Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland.*" January 13, 2026.

Briefing on DPRK Remote IT Worker Schemes. March 5, 2026.

Hearing: "*DeepSeek and Unitree Robotics: Examining the National Security Risks of PRC Artificial Intelligence, Robotics, and Autonomous Technologies and Building a Secure U.S. Technology Base.*" March 17, 2026.

Hearing: "*Data Centers, Telecommunications Networks, and Space-Based Systems: Modernizing DHS's SRMA Role for the Communications and IT Sectors.*" April 29, 2026.

Hearing: "*State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities.*" May 21, 2026.

Hearing: "*The AI Security Landscape: How Frontier Models, Agentic AI, and AI Coding Tools Are Reshaping Cybersecurity and Critical Infrastructure Resilience.*" June 4, 2026.

Border Security and Enforcement

Hearing: "Exploring the Use of Unmanned Aircraft Systems Across the DHS Enterprise." April 1, 2025. *Joint Hearing with the Subcommittee on Emergency Management and Technology*

Hearing: "Case by Case: Returning Parole to its Proper Purpose." July 15, 2025. *Joint Hearing with the Subcommittee on Oversight, Investigations, and Accountability*

Hearing: "Smarter Borders, Safer Nation: Expanding the Use of Non-Intrusive Inspection Technology." January 22, 2026.

Hearing: "Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans." April 21, 2026.

Hearing: "Northern Exposure: Assessing the Evolving Threat Landscape at America's Northern Border." June 30, 2026.

EMERGENCY MANAGEMENT AND TECHNOLOGY

Hearing: "*Future of FEMA: Perspectives from the Emergency Management Community.*" March 4, 2025.

Hearing: "*Mass Gathering Events: Assessing Security Coordination and Preparedness*." May 21, 2025.

Hearing: "*Surveying the Threat of Agroterrorism: Perspectives on Food, Agriculture, and Veterinary Defense.*" September 16, 2025.

Briefing on Chemical, Biological, Radiological, and Nuclear Threats. January 13, 2026.

Hearing: "*Surveying the Threat of Agroterrorism, Part II: Assessing Federal Government Efforts.*" February 11, 2026.

Site Visit to Redstone Arsenal. April 23-24, 2026. *Huntsville, Alabama*

Site Visit to FEMA Headquarters. June 4, 2026. *Washington, District of Columbia*

Abbreviations

A4A – Airlines for America
ACE – Accelerated Candidate Event
ACLED – Armed Conflict Location and Event Data
AFGE – American Federation of Government Employees
AI – Artificial Intelligence
AMO – Air and Marine Operations
ANAB – ANSI-American Society for Quality National Accreditation Board
ANSI – American National Standards Institute
AQ – Al Qaeda
ATSA – Aviation and Transportation Security Act
AUVSI – Association for Uncrewed Vehicle Systems International

BD21 – Biological Detection for the Twenty-First Century

CAPPS – Computer-Assisted Passenger Prescreening System
CAT – Credential Authentication Technology
CBP – Customs and Border Protection
CBRN – Chemical, Biological, Radiological, and Nuclear
CDC – Centers for Disease Control and Prevention
CDP – Center for Domestic Preparedness
CIA – Central Intelligence Agency
CIRCIA – Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA – Cybersecurity and Infrastructure Security Administration
CISA 2015 – Cybersecurity Information Sharing Act of 2015
CIRCIA – Cyber Incident Reporting for Critical Infrastructure Act
CLMN – Chinese-Language Money Laundering Networks
CT – Computed Tomography
CTOC – Countering Transnational Organized Crime
C-UAS – Counter-Unmanned Aircraft Systems
CVE – Common Vulnerabilities and Exposures
CWMD – Countering Weapons of Mass Destruction Office

DCA – Ronald Reagan Washington National Airport
DCI – Director of Central Intelligence
DFW – Dallas Fort Worth International Airport
DHS – Department of Homeland Security
DNDO – Domestic Nuclear Detection Office
DNI – Director of National Intelligence
DOE – Department of Energy
DOJ – Department of Justice
DPRK – North Korea (Formally known as the Democratic People's Republic of Korea)
DTED – Developmental Testing and Evaluation Designation
DVE – Domestic Violent Extremist

EBSP – Electronic Baggage Screening Program

EDS – Explosives Detection Systems
EMPG – Emergency Management Performance Grant
EO – Executive Order
EOL – End-of-life
EPA – Environmental Protection Agency

FAA – Federal Aviation Administration
FBI – Federal Bureau of Investigation
FDNY – New York City Fire Department
FEMA – Federal Emergency Management Agency
FIFA – Fédération Internationale de Football Association
FTO – Foreign Terrorist Organization
FY – Fiscal Year

GAO – Government Accountability Office
GenAI – Generative Artificial Intelligence

HART – Homeland Advanced Recognition Technology
HSA – Homeland Security Act of 2002
HSGP – Homeland Security Grant Program
HSI – Homeland Security Investigations
HSIN – Homeland Security Information Network
HSPD – Homeland Security Presidential Directive
HVE – Homegrown Violent Extremist

I&A – Office of Intelligence and Analysis
IAIP – Directorate for Information Analysis and Infrastructure Protection (IAIP)
IC – Intelligence Community
ICE – U.S. Immigration and Customs Enforcement
ICS – Incident Command System
ID – Identity document
IDENT – Automated Biometric Identification System
INS – Immigration and Naturalization Service
IPCC – International Police Coordination Center
IRTPA – Intelligence Reform and Terrorism Prevention Act of 2004
ISAC – Information Sharing and Analysis Center
ISE – Information Sharing Environment
ISIS – Islamic State of Iraq and Syria
IT – Information Technology

JTTF – Joint Terrorism Task Force

LPD – Last point of departure

MDDP – Mobile Detection Deployment Program
MTS – Maritime Transportation System

MTSA – Maritime Transportation System Act

NATO – North Atlantic Treaty Organization
NBACC – National Biodefense Analysis and Countermeasures Center
NBFAC – National Bioforensic Analysis Center
NBIC – National Biosurveillance Integration Center
NBTCC – National Biological Threat Characterization Center
NCBC – National Counter Proliferation and Biosecurity Center
NCITE – National Counterterrorism Innovation, Technology, and Education Center
NCPC – National Counter Proliferation Center
NCTC – National Counterterrorism Center
NCUTC – National Counter-Unmanned Aircraft Systems Training Center
NDPC – National Domestic Preparedness Consortium
NEADS – U.S. Air Force Northeast Air Defense Sector
NII – Non-Intrusive Inspection
NIMS – National Incident Management System
NIOSH – National Institute for Occupational Safety and Health
NIP – National Intelligence Program
NIST – National Institute of Standards and Technology
NPG – National Preparedness Goal
NPS – National Preparedness System
NSM – National Security Memorandum
NSM-22 – National Security Memorandum on Critical Infrastructure Security and Resilience
NSSE – National Special Security Events
NSTS – National Strategy for Transportation Security
NTIA – National Telecommunications and Information Administration
NVE – Nihilistic Violent Extremist
NWS – New World Screwworm
NYPD – New York City Police Department

OBBBA – One Big Beautiful Bill Act
ODNI – Office of the Director of National Intelligence
OEC – Office of Emergency Communications
OEM – New York City Mayor's Office of Emergency Management
OHA – Office of Health Affairs
OHS – Office of Health Security
OSAI – Office of SAFETY Act Implementation
OSS – One-Stop Security
OT – Operational Technology

PAPD – Port Authority of New York and New Jersey Police Department
PCLOB – Privacy and Civil Liberties Oversight Board
PKEMRA – Post-Katrina Emergency Management Reform Act
PPD – Presidential Policy Directive
PPD-41 – Presidential Policy Directive on United States Cyber Incident Coordination
PQC – Post-Quantum Cryptography

PRC – People's Republic of China

R&D – Research and Development
RSSP – Reimbursable Screening Services Program

S&T – Science and Technology Directorate
SAFETY – Support Anti-Terrorism by Fostering Effective Technologies
SEAR – Special Event Assessment Rating
SHSP – State Homeland Security Grant Program
SLCGP – State and Local Cybersecurity Grant Program
SLTT – State, Local, Tribal, and Territorial
SPR – Stakeholder Preparedness Review
SRMA – Sector Risk Management Agency
STC – Securing the Cities

TCO – Transnational Criminal Organization
TEDAC – Terrorist Explosive Device Analytical Center
THIRA – Threat and Hazard Identification and Risk Assessment
TSA – Transportation Security Administration
TSC – Terrorist Screening Center
TSDB – Terrorist Screening Database
TSDS – Terrorist Screening Dataset
TSIF – TSA Systems Integration Facility
TSO – Transportation Security Officer
TTIC – Terrorist Threat Integration Center
TTP – Tactics, Techniques, and Procedures
TWIC – Transportation Worker Identification Card

U.K. – United Kingdom
UAS – Unmanned Aircraft Systems
UASI – Urban Area Security Initiative
U.S. – United States of America
US&R – Urban Search and Rescue
USCIS – U.S. Citizenship and Immigration Service
USG – United States Government
USSS – United States Secret Service

WIMWIG – Widespread Information Management for the Welfare of Infrastructure and Government Act
WMD – Weapon of Mass Destruction
WTC – World Trade Center
WTCHP – World Trade Center Health Program

Endnotes

[1] Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107-306, § 601-611, 116 Stat. 2383, 2408-2413 (2002).
[2] *Id.*
[3] National Commission on Terrorist Attacks Upon the United States, (Sep. 20, 2004) (on file with Nat'l Archives and Records Administration) https://9-11commission.gov/ (last visited July 30, 2026).
[4] THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004).
[5]Michael E. Devine and Clayton M. Levy, Cong. Rsch. Serv., *Intelligence Recommendations of the 9/11 Commission and Implementing Legislation* (2026).
[6] *September 11, Chronology,* DEP'T OF HOMELAND SEC.: NEWS: PUBLICATIONS LIBRARY: DO BUSINESS WITH DHS, https://www.dhs.gov/september-11-chronology (last visited July 23, 2026).
[7] *Id.*
[8] *Id.*
[9] CNN, *Another Hijacker was Stopped for Traffic Violation,* CNN, (Jan. 9, 2002), https://edition.cnn.com/2002/US/01/09/inv.hijacker.traffic.stops/.
[10] Yuvraj Tyagi, *9/11 Attacks Timeline: How Al-Qaeda Hijackers Targeted the Twin Towers, Pentagon, and Flight 93,* TIMESNOW (Sep. 12, 2025), https://www.timesnownews.com/world/us/us-news/9-11-attacks-timeline-how-al-qaeda-hijackers-targeted-the-twin-towers-pentagon-and-flight-93-on-september-11-article-152784678.
[11] Dep't of Homeland Sec., *supra* note 6.
[12] *Id.*
[13] *September 11 Attack Timeline*, 9/11 MEMORIAL AND MUSEUM: TIMELINES, https://timeline.911memorial.org/timeline/10681 (last visited July 30, 2026).
[14] *Id.*
[15] *How Many People Were Killed in the September 11 Attacks?*, BRITTANICA, https://www.britannica.com/topic/How-many-people-were-killed-in-the-September-11-attacks (last visited July 24, 2026).
[16] *9/11 by the Numbers,* NY MAGAZINE: NEWS: ARTICLES, https://nymag.com/news/articles/wtc/1year/numbers.htm (last visited July 24, 2026).
[17] *Supra* note 4 at 280.
[18] *Id.*
[19] *Id.*
[20] *Id.* at *283*.
[21] *Id.* at *285*.
[22] *Id.* at *293*.
[23] *Id.*
[24] *Events of the Day*, NATIONAL SEPTEMBER 11 MEMORIAL & MUSEUM (last visited Aug. 7, 2026), https://www.911memorial.org/learn/resources/911-primer/module-1-events-day.
[25] *Supra* note 4 at 311.
[26] *Id.* at 316.
[27] *Creation of the Department of Homeland Security*, DEP'T OF HOMELAND SEC.: ABOUT DHS: HISTORY, https://www.dhs.gov/creation-department-homeland-security (last visited July 24, 2026).
[28] *Id.*
[29] Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).
[30] *Timeline*, TRANSP. SEC. ADMIN.: ABOUT: TSA HIST., https://www.tsa.gov/timeline (last visited July 27, 2026).
[31] *Proposal to Create the Department of Homeland Security*, DEP'T OF HOMELAND SEC.: NEWS: PUBL'N LIBR., https://www.dhs.gov/publication/proposal-create-department-homeland-security (last visited July 24, 2026).
[32] *Id.*
[33] *Who Joined DHS*, DEP'T OF HOMELAND SEC.: ABOUT DHS: HIST., https://www.dhs.gov/who-joined-dhs (last visited July 24, 2026).
[34] Aviation and Transportation Security Act.
[35] *Organizational Chart,* DEP'T OF HOMELAND SEC.: NEWS: PUBL'N LIBR. (May 19, 2026), https://www.dhs.gov/organizational-chart.

[36] Devan Markham, *21 Years After 9/11, A Look Inside the NYPD Counterterrorism Bureau*, NEWSNATION (Sep. 11, 2022), https://www.newsnationnow.com/us-news/sept11-anniversary/9-11-nypd-coutnerterrorism-bureau/.
[37] *Joint Terrorism Task Forces*, FED. BUREAU OF INVESTIGATION: WHAT WE INVESTIGATE, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces (last visited July 27, 2026).
[38] *Office of Intelligence and Analysis*, DEP'T OF HOMELAND SEC.: ABOUT DHS: ORG.: OPERATIONAL AND SUPPORT COMPONENTS, https://www.dhs.gov/office-intelligence-and-analysis (last visited July 27, 2026).
[39] Judy Schneider, Cong. Rsch. Serv., House Select Committee on Homeland Security: A Fact Sheet, RS21431 (2004).
[40] *Id.*
[41] Adopting rules for the One Hundred Ninth Congress, H.R. Res. 5, 109th Cong. (2005).
[42] H. COMM. ON RULES, 119TH CONG., RULES ADOPTED BY THE COMMITTEES OF THE HOUSE OF REPRESENTATIVES (Comm. Print 119-7).
[43] National Commission on Terrorist Attacks Upon the United States*, supra* note 3.
[44] *Id.* at 367.
[45] *Id.* at 369.
[46] *Id.* at 370.
[47] *Id.* at 374.
[48] *Id.* at 376.
[49] *Id.*
[50] *Id.* at 377.
[51] *Id.*
[52] *Id.* at 378.
[53] *Id.* at 379.
[54] *Id.*
[55] *Id.* at 380.
[56] *Id.* at 381.
[57] *Id.* at 382.
[58] *Id.* at 385.
[59] *Id.* at 387.
[60] *Id.* at 389.
[61] *Id.* at 390.
[62] *Id.*
[63] *Id.* at 391.
[64] *Id.* at 393.
[65] *Id.*
[66] *Id.* at 394.
[67] *Id.* at 394-5.
[68] *Id.* at 395.
[69] *Id.* at 396.
[70] *Id*. at 397.
[71] *Id.*
[72] *Id.* at 398.
[73] *Id.* at 403.
[74] *Id.* at 411.
[75] *Id.* at 415.
[76] *Id.*
[77] *Id.* at 416.
[78] *Id.* at 417.
[79] *Id.* at 418.
[80] *Id.* at 420.
[81] *Id.* at 421.
[82] *Id.* at 422.
[83] *Id.* at 425-6.
[84] *Id.* at 428.
[85] *Id.*
[86] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[87] Homeland Security Act of 2002.
[88] Dep't of Homeland Sec., *Proposal to Create the Department of Homeland Security*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/publication/proposal-create-department-homeland-security (last visited July 24, 2026).
[89] Homeland Security Act of 2002.
[90] Ed Carpenter, Erika Trautman, *The Terrorist Threat Integration Center,* PBS, https://www.pbs.org/wgbh/pages/frontline/shows/sleeper/homeland/ttic.html (last visited Aug. 12, 2026).
[91] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 69 Fed. Reg. 6901 (Feb. 11, 2004).
[92] National Counterterrorism Center, 69 Fed. Reg. 53589 (Sept. 1, 2004).
[93] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-58, 118 Stat. 3638 (2004).
[94] Dep't of Homeland Sec., *Department Six-point Agenda,* DEP'T OF HOMELAND SEC., https://www.dhs.gov/department-six-point-agenda (last visited Aug. 12, 2026).
[95] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007).
[96] 50 U.S.C. § 3306 (2018).
[97] Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022).
[98] Press Release, U.S. Customs and Border Prot., *DHS announces Final Rule to advance the Biometric Entry/Exit* Program, U.S. CUSTOMS AND BORDER PROT. (Nov. 20, 2025).
[99] Don Rassler, Kristina Hummel, Brian Dodwell & Ned Curry, *The Changing Character of Terrorism and U.S. Counterterrorism*, 18 C.T.C. SENTINEL 19 (Nov./Dec. 2025), https://ctc.westpoint.edu/the-changing-character-of-terrorism-and-u-s-counterterrorism/ (last visited Aug. 6, 2026).
[100] *Id*.
[101] *Id*.
[102] *Rise of Anti-Israel Extremist Groups and Their Threat to U.S. National Security: Hearing Before the H. Comm. On Homeland Sec.,* 119th Cong. (June 11, 2025).
[103] Rassler et al., supra, at 1
[104] Off. of the Dir. of Nat'l. Intell., The National Counterterrorism Center, OFF. OF THE DIR. OF NAT'L. INTELL., https://www.odni.gov/about/mission-centers-directorates/nctc/about/ (last visited Aug. 6, 2026).
[105] Press Release, Nat'l Counterterrorism Ctr*., NCTC Supports Law Enforcement, Disrupts FTO-Designated Cartels and Gangs*, NAT'L COUNTERTERRORISM CTR., (Aug. 25, 2025).
[106] Press Release, Off. of the Dir. Of Nat'l Intell., First 100 Days: DNI Gabbard Prioritizes Intelligence Reports To Secure The Southern Border, OFF. OF THE DIR. OF NAT'L. INTELL., (Apr. 28, 2025).
[107] *Id*.
[108] Rassler et al., supra, at 1
[109] Armed Conflict Location & Event Data Project, *Q&A | The Islamic State's Pivot to Africa*, ACLED (Sept. 4, 2025).
[110] Isabel Jones, Jakob Guhl, Jacob Davey & Moustafa Ayad, *Young Guns: Understanding a New Generation of Extremist Radicalization in the United States*, INST. FOR STRATEGIC DIALOGUE (Aug. 2023).
[111] Rassler et al., supra, at 1.
[112] Michael C. McGarrity, *Confronting the Rise of Domestic Terrorism in the Homeland,* FED. B.OF INVEST. (May 8, 2019).
[113] Fed. Bureau of Investigation, FBI Statement on the Attack in New Orleans, FED. BUREAU OF INVESTIGATION (Jan. 1, 2025).
[114] Press Release, Off. of Pub. Affs*., U.S. Dep't of Justice, Multiple Suspects Charged for Having Firearms in Conspiracy to Provide Material Support to ISIS*, DEP'T OF JUSTICE (Nov. 3, 2025).
[115] Jones et al, supra 11.
[116] Nat'l Inst. of Justice, *Five Things About the Role of the Internet and Social Media in Domestic Radicalization,* NAT'L INST. OF JUSTICE (Dec. 18, 2023).
[117] DEP'T OF HOMELAND SEC., 2025 HOMELAND THREAT ASSESSMENT (2024).
[118] *Id*.
[119] 18 U.S.C. § 2331 (1992).
[120] Alexander Meleagrou Hitchens, Meghann Conroy & Moustafa Ayad, *The Age of Incoherence? Understanding Mixed Ideology Extremism,* PROGRAM ON EXTREMISM AT THE GEORGE WASHINGTON UNIV. (Sept. 19, 2023).
[121] *Id.*
[122] Daveed Gartenstein-Ross et al*., Composite Violent Extremism: A Radicalization Pattern Changing the Face of Terrorism*, LAWFARE (Nov. 22, 2022).
[123] Meredith Deliso, *The Challenges to U.S. Security Posed by 'Salad Bar' Extremism*, ABC NEWS (May 31, 2023).

[124] Jones et al., supra, at 11
[125] *Supra*, note 18.
[126] National Institute of Standards and Technology, *Framework for Cyber-Physical Systems: Volume 2, Working Group Reports*, NIST Special Publication 1500-202, at 22–23 (June 2017).
[127] U.S. Department of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace* (Oct. 19, 2020).
[128] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *State Energy Security Plan Optional Drop-In: IT/OT and Cyber Threat Overview* (May 2022); *see also* Taylor Telford, et al., *Fuel Shortages Crop Up in Southeast, Gas Prices Climb After Pipeline Hack*, Washington Post (May 11, 2021).
[129] National Security Agency et al., *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*, Cybersecurity Advisory AA23-144A (May 24, 2023); Sarah Krouse et al., *China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack*, THE WALL STREET JOURNAL (Sep. 26, 2024).
[130] *Supra* note 4 at 384.
[131] Bureau of Econ. Analysis, U.S. Dep't of Com., *U.S. International Trade in Goods and Services: December 2001,* U.S. DEP'T OF COM. (2002); Bureau of Econ. Analysis, U.S. Dep't of Com., *U.S. International Trade in Goods and Services: June 2026,* U.S. DEP'T OF COM. (2026).
[132] Press Release, *Chairman Brecheen: "This is only scratching the surface of these criminal enterprises",* H. COMM. ON HOMELAND SEC. (Sep. 18, 2025).
[133] Matthew Chin, *Chinese Organized Crime Networks Moved $16 Billion in Crypto in 2025, According to Report,* CNBC (Feb. 2, 2026, 1:08 AM).
[134] *Id.*
[135] *See* FinCEN, FIN-2025-A003, *FinCEN Advisory on the Use of Chinese Money Laundering Networks by Mexico-Based Transnational Criminal Organizations to Launder Illicit Proceeds,* FINCEN (Aug. 28, 2025); *see also* U.S. Immigr. and Customs Enf't, *Cornerstone Report* No. 48, *Chinese Money Laundering Organizations (CMLOs) - Use of Counterfeit Chinese Passports,* U.S. IMMIGR. AND CUSTOMS ENF'T (Jan. 2, 2024).
[136] *Id.*; *Understanding the Use of Cryptocurrencies by Cartels,* TRM LABS, (Jan. 21, 2025).
[137] *Understanding the Use of Cryptocurrencies by Cartels,* TRM LABS, (Jan. 21, 2025)
[138] *Id.*
[139] *See* Press Release, U.S. Immigr. & Customs Enf't, *ICE Leads Investigation as 4 Mexican Nationals Charged in International Smuggling Conspiracy Bringing Migrants from Canada into the U.S.*, U.S. IMMIGR. & CUSTOMS ENF'T (May 12, 2025).
[140] Press Release, U.S. Customs & Border Prot., *Dual Drug Loads Intercepted in Detroit and Port Huron*, U.S. CUSTOMS & BORDER PROT. (Sept. 15, 2025).
[141] U.S. Customs & Border Prot., *Drug Seizure Statistics* U.S. CUSTOMS & BORDER PROT. (last updated Jul. 16, 2026) https://www.cbp.gov/newsroom/stats/drug-seizure-statistics.
[142] U.S. Customs & Border Prot., *Nationwide Encounters*, U.S. CUSTOMS & BORDER PROT. (last updated Jul. 16, 2026) https://www.cbp.gov/newsroom/stats/nationwide-encounters.
[143] Fin. Crimes Enf't Network, *USA PATRIOT Act*, U.S. DEP'T OF THE TREASURY, https://www.fincen.gov/resources/statutes-and-regulations/usa-patriot-act (last visited Aug 6, 2026).
[144] *Online Scams, Crypto Fraud, and Digital, Extortion: An Examination of How Transnational Criminal Networks Target Americans Part II: Joint Classified Briefing Before the H. Comm. On Homeland Sec.,* 119th Cong. (July 14, 2026).
[145] U.S. Immigr. & Customs Enf't, *International Offices*, U.S. IMMIGR. & CUSTOMS ENF'T https://www.ice.gov/contact/international-offices (last visited Aug 6, 2026).
[146] 50 U.S.C § 3056 (2018).
[147] Implementing the 9/11 Commission Recommendations Act of 2007.
[148] Intelligence Reform and Terrorism Prevention Act of 2004.
[149] Dep't of Homeland Sec., *Office of Biometric Identity Mgmt., OBIM: A Decade in Review,* DEP'T OF HOMELAND SEC. (2024).
[150] Abigail F. Kolker, Cong. Rsch. Serv., *Trusted Traveler Programs,* R46783 (2021).
[151] U.S. Customs & Border Prot., *Full Regulatory Impact Analysis for the Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States Final Rule,* U.S. CUSTOMS & BORDER PROT. (2025).
[152] Abigail F. Kolker, Cong. Rsch. Serv., *Immigration: The U.S. Entry-Exit System,* R47541 (2025).
[153] Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, 85 Fed. Reg. 74,162, 74,170 (proposed Nov. 18, 2020) (to be codified at 8 C.F.R. pts. 215 & 235).

[154] *See* Press Release, U.S. Dep't of State, *Department of State Begins Issuance of an Electronic Passport,* U.S. DEP'T OF STATE (Feb. 17, 2006).
[155] U.S. Dep't of State, *A Strategy for Transitioning to the New Passport,* U.S. DEP'T OF STATE (Sept. 26, 2025).
[156] BICES, *International Forum for Cooperation and Security*, BICES https://web.ifc.bices.org/default (last visited Aug 6, 2026).
[157] Margaret White, *The Global Impact of 9/11*, POLICE CHIEF MAG. (Sept. 2021).
[158] REAL ID Act of 2005, Pub. L. No. 109-13, div. B, tit. II, §§ 201–208, 119 Stat. 302–16 (2005) (codified as amended in scattered sections of 49 U.S.C.).
[159] Transp. Sec. Admin., *About Real ID: Transportation Security Administration,* DEP'T OF HOMELAND SEC., https://www.tsa.gov/realid/about-realid (last visited July 30, 2026).
[160] Transp. Sec. Admin., *Credential Authentication Technology*, DEP'T OF HOMELAND SEC., https://www.tsa.gov/travel/security-screening/credential-authentication-technology (last visited Aug. 7, 2026).
[161] Transp. Sec. Admin., *TSA PreCheck® Touchless ID*, DEP'T OF HOMELAND SEC., https://www.tsa.gov/touchless-id (last visited Aug. 7, 2026).
[162] FAA Reauthorization Act of 2018, Pub. L. No. 115-254 § 1912, 132 Stat. 3552-3554 (codified at 49 U.S.C. § 114 note).
[163] Transp. Sec. Admin., *TWIC*, DEP'T OF HOMELAND SEC., https://www.tsa.gov/twic (last visited July 30, 2026).
[164] Aviation and Transportation Security Act.
[165] 6 U.S.C. § 1101 (2018).
[166] Transp. Sec. Admin., *2014 National Strategy for Transportation Security*, DEP'T OF HOMELAND SEC. (2015).
[167] FAA Reauthorization Act of 2018, Pub. L. No. 115-254, div. K, tit. I, § 1965, 132 Stat. 3606, 3606 (2018).
[168] Transp. Sec. Admin., *National Strategy for Transportation Security*, DEP'T OF HOMELAND SEC., (2026).
[169] Gov't. Accountability Off., *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (2004).
[170] *Id.*
[171] *Supra* note 4 at 392.
[172] *Id.*
[173] Dep't of Homeland Sec., *DHS/TSA/PIA-018 TSA Secure Flight Program*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/publication/dhstsapia-018-tsa-secure-flight (last visited Aug. 7, 2026).
[174] Secure Flight Program, 49 CFR § 1560.3 (2008).
[175] *Id*.
[176] Transp. Sec. Admin., *Electronic Baggage Screening Program*, DEP'T OF HOMELAND SEC., https://www.tsa.gov/for-industry/electronic-baggage-screening, (last visited Aug. 5, 2026).
[177] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, tit. XVI, § 1607(a), 121 Stat. 266, 483 (2007).
[178] *Id.*
[179] FAA Reauthorization Act of 2018, Pub. L. No. 115-254, div. K, tit. I, § 1912, 132 Stat. 3552 (2018).
[180] Privacy and Civil Liberties Oversight Bd, *History and Mission*, [180] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., https://www.pclob.gov/About/HistoryMission (last visited Aug 6, 2026).
[181]Implementing Recommendations of the 9/11 Commission Act of 2007.
[182] Homeland Security Act of 2002.
[183] Implementing Recommendations of the 9/11 Commission Act of 2007.
[184] *Id.*
[185] *Id.*
[186] Homeland Security Act of 2002.
[187] HOMELAND SEC. PRESIDENTIAL DIRECTIVE-5: MANAGEMENT OF DOMESTIC INCIDENTS, DEP'T OF HOMELAND SEC. (FEB. 28, 2003).
[188] FED. EMERGENCY MGMT. AGENCY, 20 YEARS OF NIMS: NATIONAL INCIDENT MANAGEMENT SYSTEM 2024 (2024) AT 11, https://www.fema.gov/sites/default/files/documents/fema_npd-20-years-of-nims.pdf.
[189] Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, § 611, 120 Stat. 1355, 1391 (2006).
[190] Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, § 648, 120 Stat. 1355, 1391 (2006).
[191] Dep't of Homeland Sec., *Presidential Policy Directive 8: National Preparedness*, DEP'T OF HOMELAND SEC. (Mar. 30, 2011).

[192] Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, tit. VI, subtit. B, § 6204, 126 Stat. 156, 209 (2012).
[193] Fed. Commc'ns Comm'n, *700 MHz Public Safety Spectrum*, FED. COMMC'NS COMM'N (last updated Jun. 19, 2020), https://www.fcc.gov/700-mhz-public-safety-narrowband-spectrum.
[194] Colby Leigh Pechtol and Amanda H. Peskin, Cong. Rsch. Serv., *First Responder Network (FirstNet) Authority: Reauthorization and Selected Issues*, R48923 (2026).
[195] Post-Katrina Emergency Management Reform Act of 2006, Pub. L. No. 109-295, tit. VI, § 671(b), 120 Stat. 1433, 1433 (2006).
[196] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2, 132 Stat. 4168, 4168–86 (2018).
[197] Implementing Recommendations of the 9/11 Commission Act of 2007.
[198] Voluntary Private Sector Accreditation and Certification Preparedness Program, 73 Fed. Reg. 79140 (2008).
[199] Voluntary Private Sector Accreditation and Certification Preparedness Program, 75 Fed. Reg. 34148 (2010).
[200] ANSI Nat'l. Accred. Bd., *PS-Prep*, ANSI NAT'L. ACCRED. BD., https://anab.ansi.org/accreditation/ps-prep/ (last visited Aug. 7, 2026).
[201] National Counterterrorism Center, 69 Fed. Reg. 53589 (2004).
[202] Off. of the Dir. of Nat'l Intell., The National Counterterrorism Center | *History*, OFF. OF THE DIR. OF NAT'L INTELL., https://archive.dni.gov/index.php/nctc-who-we-are/history (last visited Aug 6, 2026).
[203] Michael E. DeVine, Cong. Rsch. Serv., *The Director of National Intelligence (DNI)*, IF10470 (2025).
[204] Cent. Intell. Agency, Off. of Inspector Gen., *Office of Inspector General Report on Central Intelligence Agency Accountability Regarding Findings and Conclusions of the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, IG 2003-0005-IN (June 2005).
[205] 6 U.S.C. § 121 (2024).
[206] Dep't of Homeland Sec., *Homeland Security Information Network (HSIN)* DEP'T OF HOMELAND SEC., https://www.dhs.gov/what-hsin (last visited Aug. 6, 2026).
[207] Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1500 et seq.,
[208] 6 U.S.C. § 121 (2024).
[209] U.S. Gov't Accountability. Off., *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (2025).
[210] Exec. Order 14,180, Council To Assess the Federal Emergency Management Agency, 90 Fed. Reg. 8743 2025).
[211] Press Release, U.S. Att'y's Off., E.D. Mich., *Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for their Work at a University of Michigan Laboratory*, U.S. Dep'. of Justice (Jun. 3, 2025); Press Release, U.S. Att'y's Off., ., E.D. Mich., *Alien from Wuhan, China, Charged with Making False Statements and Smuggling Biological Materials into the U.S. for Her Work at a University of Michigan Laboratory*, U.S. Dep't of Justice (Jun. 9, 2025).
[212] Julia Jacobo, *What to Know About Fusarium Graminearum, the Biological Pathogen Allegedly Smuggled into the US*, ABC NEWS, Jun. 5, 2025.
[213] U.S. Dep't of Agric., *Farm Security is National Security*, U.S. DEP'T OF AGRIC. (Jul. 8, 2025).
[214] Exec. Order No. 14,305, Restoring American Airspace Sovereignty, 90 Fed. Reg. 24719 (2025).
[215] *Historic Interagency Coordination for the FIFA World Cup 2026™ Concludes*, FED. EMERGENCY MGMT. AGENCY (Jul. 27, 2026).
[216] Jerome P. Bjelopera & Kristin Finklea, Cong. Rsch. Serv., *Domestic Federal Law Enforcement Coordination: Through the Lens of the Southwest Border*, R43583 (2014).
[217] Dep't of Homeland Sec., *National Network of Fusion Centers Fact Sheet*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/national-network-fusion-centers-fact-sheet (last visited May 11, 2026).
[218] Off. of the Dir. of Nat'l Intell., *History*, OFF. OF THE DIR. OF NAT'L INTELL. , https://www.dni.gov/index.php/nctc-who-we-are/history (last visited Jan. 22, 2026).
[219] Intelligence Reform and Terrorism Prevention Act of 2004.
[220] *Id*.
[221] Press Release, *Committee Advances 19 Bills in Bipartisan Votes to Modernize TSA, Refocus I&A, Enhance Border Security, Prepare for Emerging Threats,* H. COMM. ON HOMELAND SEC. (June 24, 2026)
[222] H.R. 7443, 119th Cong. (2026).
[223] H.R. 7773, 119th Cong. (2026).
[224] H.R. 7436, 119th Cong. (2026).
[225] H.R. 2212, 119th Cong. (2025).

[226] Nandita Bose & Ted Hesson, *National Guard Shooting Suspect Radicalized in U.S., Homeland Secretary Says*, REUTERS (Nov. 30, 2025).
[227] 6 U.S.C. § 101 (2024).
[228] 18 U.S.C. § 2331 (2024).
[229] Int'l Ctr. for Not-for-Profit L., *Terrorism Laws in the United States*, INT'L CTR. FOR NOT-FOR-PROFIT L., https://www.icnl.org/resources/terrorism-laws-in-the-united-states (last visited Jan. 22, 2026).
[230] Press Release, Off. of Pub. Aff. for the Dep't of Justice, '764' Extremist Group Leader Pleads Guilty to RICO, Child Exploitation Charges, DEP'T OF JUSTICE (Dec. 19, 2025).
[231] FBI Dall., *FBI Dallas Open Letter to Parents, Guardians, and Teachers,* FED. BUREAU OF INVESTIGATION (May 12, 2026).
[232] Nat'l Counterterrorism, Innovation, Tech. & Educ. Ctr. (NCITE), *Prosecuting Nihilistic Violent Extremism: An Examination of Federal and State Charges Against 764 and Related Networks,* UNIV. OF NEB. AT OMAHA (Dec. 20, 2025).
[233] Hudson Crozier, et al., *Member of Satanic "764" Cult Charged After 13-Year-Old Girl Found Hanging in the Parking Lot*, THE LIBERTY DAILY (Oct. 16, 2025); Press Release, U.S. Att'y's Off., for the D.C., *Leaders of 764 Arrested and Charged for Operating Global Child Exploitation Enterprise*, DEP'T OF JUSTICE (Apr. 30, 2025).
[234] David Yaffe-Bellany, *Terrorist Groups Use A.I. as a Battle Consultant, Not Just a Propaganda Tool*, N.Y. TIMES (July 10, 2026).
[235] Press Release, *Rep. Pfluger's Generative AI Terrorism Risk Assessment Act Advanced by House Committee on Homeland Security*, OFF. OF CONGRESSMAN AUGUST PFLUGER (Sept. 3, 2025).
[236] Nat'l Counterterrorism, Innovation, Tech. & Educ. Ctr. (NCITE), *Malign Use of AI: Uncensored and Abliterated Models. U.S. Congressional Committee on Homeland Security*, UNIV. OF NEB. AT OMAHA (Apr. 22, 2026).
[237] The Associated Press, *The FBI Arrested an Afghan Man Who Officials Say Was Planning an Election Day Attack*, NPR (Oct. 8, 2024); *WATCH: FBI Says Driver Responsible for Deadly New Orleans Rampage Acted Alone in Act of "Terrorism"*, PBS NEWSHOUR (Jan. 2, 2025).
[238] H.R. 1736, 119th Cong. (2025).
[239] H.R. 1212, 119th Cong. (2025).
[240] *Supra*, note 44.
[241] H.R. 8168, 119th Cong. (2026).
[242] Angelique Chrisafis, *'It was war': Survivors of 2016 Nice attack describe experiences in court,* THE GUARDIAN (Sep. 21, 2022).
[243] H.R. 1608, 119th Cong. (2025).
[244] H.R. 4070, 119th Cong. (2025).
[245] H.R. 1327, 119th Cong. (2025).
[246] H.R. 6846, 119th Cong. (2025).
[247] Press Release, *Rep. Crane Leads Legislation Addressing Drone Threats Informed by Overseas Conflicts,* H. COMM. ON HOMELAND SEC. (Dec. 19, 2025).
[248] Nat'l Counterterrorism, Innovation, Tech. & Educ. Ctr. (NCITE), UNIV. OF NEB. OMAHA, https://www.unomaha.edu/ncite/index.php (last visited Aug. 6, 2026).
[249] Aviation and Transportation Security Act.
[250] *Id.*
[251] Transp. Sec. Admin., *Security Fees*, DEP'T OF HOMELAND SEC., https://www.tsa.gov/for-industry/security-fees (last visited June 17, 2026).
[252] Douglas Holtz-Eakin, *Budgetary Bait and Switch*, AM. ACTION FORUM (Mar. 10, 2026).
[253] Bart Elias et al., Cong. Rsch. Serv., *Transportation Security: Background and Issues for the 119th Congress,* R48543 (2025).
[254] SAFEGUARDS Act, H.R. 8770, 119th Cong. (2026).
[255] 49 U.S.C. § 44920
[256] Reimbursable Screening Services Program Extension Act of 2026, H.R. 9391, 119th Cong. (2026)
[257] Press Release, Transp. Sec. Admin., *"One Stop Security" Pilot Program Aims to Simplify International Travel,* TRANSP. SEC. ADMIN. (Aug. 27, 2025).
[258] One-Stop Pilot Program Extension Act of 2026, H.R. 9388, 119th Cong. (2026)
[259] Improving Travel for Military Members Act , H.R. 9328, 119th Cong. (2026).
[260] Transp. Sec. Admin., *Announcing New TSA PreCheck "Serve with Honor, Travel with Ease" Benefits for the Military Service Community,* TRANSP. SEC. ADMIN. (July 2, 2025).

[261] Email correspondence between TSA OLA and House Homeland Committee Staff (March – May 2025) (on file with author).
[262] , Improving Travel for American Families Act, H.R. 8897, 119th Cong. (2026).
[263] Transp. Sec. Admin., *Families on the Fly*, DEP'T OF HOMELAND SEC., https://www.tsa.gov/travel/travel-tips/families-fly (last visited May 14, 2026).
[264] *Budget Hearing – Fiscal Year 2025 Request for the Cybersecurity and Infrastructure Security Agency: Hearing Before the Subcomm. on Homeland Security of the H. Comm. on Appropriations*, 118th Cong. (Mar. 28, 2023) (statement of Congressman Dave Joyce, Subcommittee Chairman).
[265] U.S. Gov't Accountability Off., *Cybersecurity Regulations: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements*, GAO-26-108606 (Jul. 22, 2026).
[266] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, div. Y, 136 Stat. 1038 (2022); The White House, *President Trump's Cyber Strategy for America* (Mar. 6, 2026).
[267] OpenAI, *OpenAI and Hugging Face Partner to Address Security Incident During Model Evaluation,* OPENAI (Jul. 21, 2026).
[268] Press Release, *Chairman Garbarino, Rep. Fong Lead Cyber Roundtable with CISA, Regional Stakeholders in California's Central Valley,* H. COMM. ON HOMELAND SEC. (Apr. 13, 2026).
[269] H.R. 5078, 119th Cong. (2025).
[270] U.S. Customs & Border Prot*., Full Regulatory Impact Analysis for the Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States Final Rule 3* (2025).
[271] U.S. Customs & Border Prot*., Full Regulatory Impact Analysis for the Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States Final Rule 3* (2025).
[272] U.S Customs & Border Prot., *Customs Bulletin and Decisions*, Vol. 58, No. 19, at 16-17 (2024).
[273] U.S. Gov't Accountability Off., *DHS Annual Assessment: Improved Guidance on Revised Acquisition Goals Would Enhance Transparency*, GAO-25-107317 (Feb. 25, 2025).
[274] Anthony Kimerv, *DHS' biometric programs hampered by shifting priorities and budget shortfalls,* BIOMETRIC UPDATE (Feb 27, 2025).
[275] U.S. Gov't Accountability Off., *Border Security: DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain*, GAO-17-170 (Feb. 27, 2017).
[276] *Id.*
[277] *Id.*
[278] *Id.*
[279] U.S. Customs & Border Prot., *Entry/Exit Overstay Report: Fiscal Year 2023 Report to Congress,* DEP'T OF HOMELAND SEC. (Aug. 5, 2024).
[280] One Big Beautiful Bill Act, Pub. L. No. 119-21, 139 Stat. 72 (2025).
[281] *Supra* note 4 at 389.
[282] U.S. Dep't of State, *Worldwide Nonimmigrant Visa (NIV) Workload by Visa Category: Fiscal Year 2024,* U.S. DEP'T OF STATE, https://travel.state.gov/content/dam/visas/Statistics/Non-Immigrant-Statistics/NIVWorkload/FY%202024NIVWorkloadbyVisaCategory.pdf (last visited Aug. 12, 2026). ; U.S. Customs and Border Prot., *CBP Traveler and Conveyance Statistics,* U.S. Dep't of Homeland Security, (last updated Aug. 14, 2026) https://www.cbp.gov/newsroom/stats/travel ; U.S. Customs and Border Prot., *CBP Enforcement Statistics: Fiscal Year 2024,* U.S. Dep't of Homeland Security, (last updated Aug. 14, 2026) https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics.
[283] U.S. Citizenship & Immigr. Servs., *Statement of Financial Condition: Fiscal Year 2024 Report to Congress, Immigration Examinations Fee Account,* DEP'T OF HOMELAND SEC., (July 21, 2025).
[284] One Big Beautiful Bill Act, Pub. L. No. 119-21, 139 Stat. 72 (2025).
[285] DETECT Fentanyl and Xylazine Act of 2024, Pub. L. No. 118-186, 138 Stat. 2636 (2024).
[286] U.S. Customs & Border Prot., *CBP Enforcement Statistics*, DEP'T OF HOMELAND SEC., https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics (last visited Aug. 12, 2026).
[287] Implementing Recommendations of the 9/11 Commission Act of 2007.
[288] Press Release, *Subcommittee Chairman Guest Opens Hearing on CBP's Non-Intrusive Inspection Technology,* H. Comm. on Homeland Sec. (Jan. 22, 2026).
[289] *Before the Whistle: Assessing Information Sharing and Security Collaboration Ahead of Major Events: Hearing Before the H. Comm on Homeland Sec.*, 119th Cong. (Feb. 24, 2026) (testimony of Deputy Chief Joseph Mabin, Patrol Bureau, Kansas City Missouri Police Department).
[290] U.S. Gov't Accountability Off., *Homeland Sec. Grants: DHS Implemented National Priority Areas but Could Better Document and Communicate Changes*, GAO-23-106930 (2024).

[291] *State of Illinois v. Noem*, No. 1:25-cv-00495, (D.R.I.).
[292] Press Release, Wash. State Off. of the Att'y Gen., *AG Brown Protects Homeland Security Funding from Politically Motivated Cuts as Federal Government Drops Appeal,* WASH. STATE OFF. OF THE ATT'Y GEN., (May 7, 2026).
[293] Off. of the Dir. of Nat'l. Intell. *Large Public Gatherings Attractive Targets for Violent Extremists,* JOINT COUNTERTERRORISM ASSES. TEAM, https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/163s-Large-Public-Gatherings-Attractive-Targets-for-Violent-Extremists.pdf (last visited Aug. 12, 2026).
[294] Dep't of Homeland Sec., Off. of Intell. and Anal. Homeland Threat Asses. (2025).
[295] One Big Beautiful Bill Act, Pub. L. No. 119-21, 139 Stat. 72 (2025).
[296] See the *Final Report of the Task Force on Enhancing Security for Special Events in the United States*.
[297] The 32 core capabilities are (1) Planning, (2) Public Information and Warning, (3) Operational Coordination, (4) Forensics and Attribution, (5) Intelligence and Information Sharing, (6) Interdiction and Disruption, (7) Screening, Search, and Detection, (8) Access Control and Identity Verification, (9) Cybersecurity, (10) Physical Protective Measures, (11) Risk Management for Protection Programs and Activities, (12) Supply Chain Integrity and Security, (13) Community Resilience, (14) Long-Term Vulnerability Reduction, (15) Risk and Disaster Resilience Assessment, (16) Threats and Hazards Identification, (17) Critical Transportation, (18) Environmental Response/Health and Safety, (19) Fatality Management Services, (20) Fire Management and Suppression, (21) Infrastructure Systems, (22) Logistics and Supply Chain Management, (23) Mass Care Services, (24) Mass Search and Rescue Operations, (25) On-Scene Security, Protection, and Law Enforcement, (26) Operational Communications, (27) Public Health, Healthcare, and Emergency Medical Services, (28) Situational Assessment, (29) Economic Recovery, (30) Health and Social Services, (31) Housing, and (32) Natural and Cultural Resources.
[298] FED. EMERGENCY MGMT. AGENCY, 20 YEARS OF NIMS: NATIONAL INCIDENT MANAGEMENT SYSTEM 2024 (2024) at 15.
[299] *What is EMAC?*, EMERGENCY MANAGEMENT ASSISTANCE COMPACT (EMAC), https://www.emacweb.org/index.php/learn-about-emac/what-is-emac (last visited Aug. 7, 2026); *see also* Joint resolution granting the consent of Congress to the Emergency Management Assistance Compact, Pub. L. No. 104-321, 110 Stat. 3874 (1996).
[300] FED. EMERGENCY MGMT. AGENCY, 20 YEARS OF NIMS: NATIONAL INCIDENT MANAGEMENT SYSTEM 2024 (2024) at 20.
[301] *National Risk and Capability Assessment*, FED. EMERGENCY MGMT. AGENCY (Jun. 12, 2023),
[302] *Id.*
[303] Homeland Security Today, *FEMA's National Preparedness Report Focuses on Mass Care, Cybersecurity, and Infrastructure Resilience*, HOMELAND SECURITY TODAY (Jan. 17, 2025).
[304] U.S. Gov't Accountability Off., NATIONAL PREPAREDNESS: *Additional Actions Needed to Address Gaps in the Nation's Emergency Management Capabilities,* GAO-20-297 *at* 12-13, (2020).
[305] *Fiscal Year 2026 Homeland Security Grant Program Notice of Funding Opportunity*, DEP'T OF HOMELAND SEC. (Jun. 24, 2026) at 54; *see also Fiscal Year 2026 Emergency Management Performance Grant Program Notice of Funding Opportunity*, U.S. DEP'T OF HOMELAND SEC. (Jun. 15, 2026) at 9.
[306] *Future of FEMA: Perspectives from the Emergency Management Community: Hearing Before the Subcomm. on Emergency Management and Technology of the H. Comm. on Homeland Sec.*, 119th Cong. (Mar. 4, 2025) (testimony of Carrie Speranza, President, U.S. Council of the International Association of Emergency Managers).
[307] *Id.*, *see* testimony of the Honorable Daniel Kaniewski, Managing Director, Public Sector, Marsh McLennan.
[308] *Fiscal Year 2026 Emergency Management Performance Grant Program Notice of Funding Opportunity*, U.S. DEP'T OF HOMELAND SEC. (Jun. 15, 2026) at 70.
[309] *Id.* at 8.
[310] *Future of FEMA: Perspectives from the Emergency Management Community: Hearing Before the Subcomm. on Emergency Management and Technology of the H. Comm. on Homeland Sec.*, 119th Cong. (Mar. 4, 2025) (testimony of the Honorable Timothy Manning, Private Citizen, *Former Deputy Administrator for Protection and National Preparedness*, *Fed'l Emergency Management Agency*).
[311] FED. EMERGENCY MGMT. AGENCY, 20 YEARS OF NIMS: NATIONAL INCIDENT MANAGEMENT SYSTEM 2024 (2024) at 22.
[312] *Training*, NATIONAL DOMESTIC PREPAREDNESS CONSORTIUM, https://ndpc.us/training/ (last visited Aug. 7, 2026).
[313] *About*, FED. EMERGENCY MGMT. AGENCY CTR. FOR DOMESTIC PREPAREDNESS, https://cdp.dhs.gov/about (last visited Aug. 7, 2026).
[314] *NERRTC Online Training*, TEX. A&M ENG'G EXTENSION SERV., https://teex.org/program/nerrtc-online-training/ (last visited Aug. 7, 2026).

[315] *New Mexico Tech/EMRTC First Responder Training*, N.M. TECH ENERGETIC MATERIALS RSCH. AND TESTING CTR., https://www.nmttraining.com/ (last visited Aug. 7, 2026).
[316] *LSU | NCBRT Training. Preparing. Innovating.*, LA. STATE UNIV. NAT'L CTR. FOR BIOMEDICAL RSCH. AND TRAINING/ACAD. OF COUNTER-TERRORIST EDUC., https://www.ncbrt.lsu.edu/ (last visited Aug. 7, 2026).
[317] NAT'L DISASTER PREPAREDNESS TRAINING CTR. AT THE UNIV. OF HAW., https://ndptc.hawaii.edu/ (last visited Aug. 7, 2026).
[318] *Counter Terrorism Operations Support (CTOS) Center for Radiological/Nuclear Training*, NEV. NAT'L SEC. SITES, https://nnss.gov/mission/global-security-programs/counter-terrorism-operations-support-ctoscenter-for-radiological-nuclear-training-at-the-t-1-training-area/ (last visited Aug. 7, 2026).
[319] SEC. AND EMERGENCY RESPONSE TRAINING CTR. (SERTC), https://sertc.org/ (last visited Aug. 7, 2026).
[320] *Preparing Those Who Protect Our Nation*, NATIONAL DOMESTIC PREPAREDNESS CONSORTIUM (NDPC), https://ndpc.us/ (last visited Aug. 7, 2026).
[321] *Amerithrax or Anthrax Investigation*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/history/cases-and-criminals/amerithrax-or-anthrax-investigation (last visited Aug. 7, 2026).
[322] *Supra* note 56.
[323] *Domestic Nuclear Detection Office*, U.S. DEP'T OF HOMELAND SEC. (Aug. 1, 2024).
[324] *Off. of Health Affairs*, U.S. DEP'T OF HOMELAND SEC. (Aug. 1, 2024); *see also The National Biosurveillance Integration Center Fact Sheet*, U.S. DEP'T OF HOMELAND SEC. (May 10, 2022).
[325] Section 872 of the Homeland Security Act of 2002 authorizes the Secretary of Homeland Security to reorganize agencies and components of the Department, provided he or she notifies Congress 60 days in advance of the proposed reorganization; *see* Homeland Security Act of 2002.
[326] Counter Weapons of Mass Destruction Act of 2018, Pub. L. No. 115-387, 132 Stat. 5191 (2018).
[327] *Dep't of Homeland Sec. Countering Weapons of Mass Destruction Budget Overview: Fiscal Year 2026 Congressional Justification*, U.S. DEP'T OF HOMELAND SEC. (2025).
[328] Homeland Security and Further Additional Continuing Appropriations Act, 2026, Pub. L. No. 119-86, 96 Stat. 1920 (2026).
[329] U.S. Gov't Accountability Off., *Nuclear Terrorism Prevention: DHS Has Strengthened the Securing the Cities Program, but Actions Are Needed to Address Key Remaining Challenges*, GAO-24-106922 (Mar. 20, 2024).
[330] *Supporting Federal, State, Local, Tribal, and Territorial Partners*, U.S. DEP'T OF HOMELAND SEC. (Jun. 18, 2024).
[331] U.S. Gov't Accountability Off., *Biodefense: National Biosurveillance Integration Center Has Taken Steps to Address Challenges, but Could Better Assess Results,* GAO-24-106142 (Nov. 29, 2023).
[332] U.S. Gov't Accountability Off., *Biodefense: DHS Exploring New Methods to Replace BioWatch and Could Benefit from Additional Guidance,* GAO-21-292 (May 20, 2021).
[333] *Id.*
[334] DHS Biodection Improvement Act, H.R. 706, 119th Cong. (2025).
[335] Drew Endy, Sarah Moront, Vassilis Andrea Alexopoulos, Raj Patel, Rhea Jain, and Britney Bennett, *Biosecurity Really: A Strategy for Victory*, HOOVER INST., BIO-STRATEGIES & LEADERSHIP INITIATIVE (Oct. 8, 2025).
[336] *National Biodefense Analysis and Countermeasures Center*, U.S. DEP'T OF HOMELAND SEC. (Apr. 27, 2026).
[337] Kerry Breen, *Bio Lab Found in Las Vegas is Similar to Scene Discovered in California, Raising Questions from Officials*, CBS NEWS (Feb. 5, 2026).
[338] Press Release, U.S. Att'y's Off., E.D. Mich., *Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for their Work at a University of Michigan Laboratory*, DEP'T OF JUSTICE (June 3, 2025); Press Release, U.S. Att'y's Off., E.D. Mich., *Alien from Wuhan, China, Charged with Making False Statements and Smuggling Biological Materials into the U.S. for Her Work at a University of Michigan Laboratory*, DEP'T OF JUSTICE (Jun. 9, 2025).
[339] Julia Jacobo, *What to Know About Fusarium Graminearum, the Biological Pathogen Allegedly Smuggled into the US*, ABC NEWS, (Jun. 5, 2025).
[340] The White House, *NSM-16: National Security Memorandum on Strengthening the Security and Resilience of United States Food and Agriculture,* THE AM. PRESIDENCY PROJECT (Nov. 10, 2022).
[341] U.S. Food and Drug Admin., *Strengthening the Security and Resilience of U.S. Food and Agriculture:120-Day Interim Risk Review,* U.S. FOOD AND DRUG ADMIN. (Jul. 13, 2023).
[342] Civil Preparedness for Agroterrorism Exercise Act of 2026, H.R. 9394, 119th Cong. (2026).
[343] *Surveying the Threat of Agroterrorism, Part II: Assessing Federal Government Efforts: Hearing Before the Subcomm. on Emergency Management and Technology of the H. Comm. on Homeland Sec.*, 119th Cong. (Feb. 11,

2026) (testimony of Ashley Grant, Ph.D., MPH, Senior Health Security and Biodefense Advisor, Off. of Health Sec., U.S. Dep't of Homeland Sec.).
[344] Colby Leigh Pechtol and Amanda H. Peskin, *Supra* note 191.
[345] First Responder Network Authority Reauthorization Act of 2026, H.R. 7386, 119th Cong. (2026).
[346] Homeland Security Act of 2002, § 861-865.
[347] *The Office of SAFETY Act Implementation*, U.S. DEP'T OF HOMELAND SEC. (Apr. 21, 2026).
[348] *Oversight of the Dep't of Homeland Sec.: CISA, TSA, S&T: Hearing Before the H. Comm. on Homeland Sec.*, 119th Cong. (Jan. 21, 2026) (statement of the Honorable Pedro Allende, Under Secretary, Science and Technology Directorate (S&T), U.S. Dep't of Homeland Sec.).
[349] *Dep't of Homeland Sec. Science and Technology Directorate Budget Overview: Fiscal Year 2027 Congressional Justification*, U.S. DEP'T OF HOMELAND SEC. (2026).
[350] *May 30, 2002: Ground Zero Cleanup Operation Officially Ends*, INT'L CTR. FOR 9/11 JUSTICE: COMPLETE 9/11 TIMELINE, https://ic911.org/complete-timeline/may-30-2002-ground-zero-cleanup-operation-officially-ends/ (last visited July 28, 2026).
[351] Katie Reilly, *Former EPA Leader Apologizes for Saying New York Air Was Safe After 9/11*, TIME (Sept. 10, 2016), https://time.com/4486557/epa-leader-apology-911-september-11-air/.
[352] 9/11 MEMORIAL AND MUSEUM: LEARN: RESOURCES: DUST: ILLNESS & ADVOCACY AFTER 9/11, https://www.911memorial.org/illness-and-advocacy-after-911 (last visited July 28, 2026).
[353] James Zadroga 9/11 Health and Compensation Act of 2010, Pub. L. No. 111-347, 124 Stat. 3623.
[354] CTRS. FOR DISEASE CONTROL AND PREVENTION: WORLD TRADE CTR. HEALTH PROGRAM: ABOUT: ABOUT THE PROGRAM, https://www.cdc.gov/wtc/about.html (last visited July 28, 2026).
[355] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015).
[356] Continuing Appropriations Act, 2020, and Health Extenders Act of 2019, Pub. L. No. 116-59, 133 Stat. 1093 (2019).
[357] Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, 136 Stat. 4459 (2022).
[358] National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, 137 Stat. 136 (2023).
[359] Consolidated Appropriations Act, 2026, Pub. L. No. 119-75, 140 Stat. 173 (2026).
[360] Carl Campanile & David Meyer, *More People Have Now Died From 9/11 Illnesses Than During Sept. 11 Attacks*, NEW YORK POST (Sept. 12, 2021), https://nypost.com/2021/09/12/more-people-have-now-died-from-9-11-illnesses-than-during-the-attacks/.