Review of the 9/11 Commission Report

House Permanent Select Committee on Intelligence
Chairman Rick Crawford (R-AR)
Ranking Member Jim Himes (D-CT)
9/11 Review Task Force Co-Chair Elise Stefanik (R-NY)
9/11 Review Task Force Co-Chair Josh Gottheimer (D-NJ)

U.S. House of Representatives

Letter from the Committee

Twenty-five years after the attacks of September 11th, our nation continues to reflect on the profound loss of life and the enduring impact that tragic day had on our national security, our institutions, and our collective consciousness. The anniversary is not only a moment of remembrance, but also an opportune time to assess how far our nation has come and how far we still must go to address the vulnerabilities those attacks so starkly revealed. The scars of that day remain etched not only in our skyline, but also in our memory—quiet reminders of both our vulnerability and our resolve. We honor the memory of the 2,977 innocent lives lost on September 11, 2001, whose stories, sacrifices, and enduring legacies remain forever remembered in the heart of our nation. In addition, we honor the first responders who later lost their lives to 9/11-related illnesses sustained through their heroic service.

Established in the aftermath of 9/11, the National Commission on Terrorist Attacks Upon the United States issued a comprehensive report in July 2004 detailing the intelligence, policy, and structural deficiencies that contributed to our failure to prevent the September 11th attacks. Its findings led to sweeping reforms across the Intelligence Community, including the establishment of the Office of the Director of National Intelligence and the National Counterterrorism Center, as well as to significant changes in information sharing, interagency coordination, and congressional oversight.

As the House Permanent Select Committee on Intelligence, we have a continuing responsibility to ensure that the lessons of 9/11 are fully internalized. This report reviews the progress made toward addressing intelligence failures identified by the 9/11 Commission. It evaluates the effectiveness of reforms implemented over the past quarter century, identifies areas where meaningful improvements have been achieved, and highlights gaps that persist in today's increasingly complex and evolving threat environment.

Despite the persistent threats posed by terrorism, the threat landscape within the United States has greatly evolved since 2001. Nevertheless, the core challenge in solving these issues remains the same: ensuring that our Intelligence Community is able to detect, analyze, and disrupt threats before they reach our shores or borders. Whether the threat comes from terrorists, adversary nations, malign cyber actors, or transnational criminal organizations, the need for timely and accurate intelligence to inform policymakers and warfighters has never been more acute. ***Our nation's adversaries are actively exploiting our free and open society and are working in imaginative ways to achieve their strategic objectives.*** We must learn from our past and not lose sight of this reality.

This report is intended to serve as both a retrospective assessment and a forward-looking roadmap. It underscores the importance of sustained vigilance, robust oversight, and continued adaptation in the face of established and emerging risks. It also reaffirms our commitment to supporting the men and women of the Intelligence Community, whose work is critical to the security of the American people.

Lastly, reminding the public and educating future generations about the profound and enduring impact of the September 11th attacks is essential to preserving the memory of those who were lost, understanding the consequences that followed, and ensuring that the lessons learned continue to inform our nation's security and preparedness. Our hope is that this report contributes to that responsibility by documenting the legacy of September 11th, evaluating the reforms undertaken in its aftermath, and identifying the lessons that must guide the United States in confronting the threats of the future. We recommit ourselves to ensuring such a tragedy of that scale is never repeated. The work of safeguarding our country is never complete, and it is through efforts like this review that we strive to meet that enduring obligation.

9/11 Commission Recommendations, Government Implementation, and Review

In the 22 years since the *9/11 Commission Report* (Report) was published, the federal government has implemented many of its recommendations. Of the 41 recommendations proposed in the Report, a subset were dedicated to reforming the Intelligence Community (IC). Congress adopted some of these recommendations shortly after the Report's release and enacted others in the years that followed.

As stated in the Report, the intended purpose of the Commission's recommendations was to spur change within the intelligence and law enforcement communities to mitigate the "transnational danger [of] Islamist terrorism"[1] to the homeland. To that end, the Commission argued that "[t]he government should combine [resources and people] more effectively, achieving a unity of effort,"[2] and made five overarching recommendations:

- unifying strategic intelligence and operational planning against Islamist terrorists across the foreign-domestic divide with a National Counterterrorism Center;
- unifying the Intelligence Community with a new National Intelligence Director;
- unifying the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional governmental boundaries;
- unifying and strengthening congressional oversight to improve quality and accountability; and
- strengthening the FBI and homeland defenders.[3]

The Report represented one of the most ambitious attempts to reshape the IC enterprise in decades. Former New Jersey Governor and 9/11 Commission Chairman Thomas Kean later recounted the driving motivation behind the Commission's efforts this way:

> If the FBI [Federal Bureau of Investigation] and the CIA [Central Intelligence Agency] and 14 other intelligence agencies had been talking to each other, most of us feel that the attack would have been prevented. We reorganized the whole intelligence apparatus so instead of several agencies there's now one head—the Director of National Intelligence [DNI]—[now] people from the various agencies meet together and share information.[4]

While policymaker and public interest in the Report have waxed and waned in the years since its release, its impact on the IC has been permanent and profound.

This section discusses the Report's recommendations for the IC, examines the historical record of whether Congress adopted, implemented in modified form, or declined certain recommendations, and evaluates the effectiveness of their implementation.

Unifying Counterterrorism Strategic Intelligence and Operational Planning

Recommendation Adopted: Creation of NCTC

The Report's first major IC recommendation was to unify "strategic intelligence and operational planning against Islamist terrorists across the foreign-domestic divide" by creating a National Counterterrorism Center (NCTC).[5] Specifically, the Report recommended that NCTC conduct "joint operational planning *and* joint intelligence, staffed by personnel from the various agencies."[6] The Commission wanted NCTC to develop plans that "would assign operational responsibilities to lead agencies, such as State, the CIA, the FBI, [the Department of] Defense and its combatant commands, Homeland Security, and other agencies."[7] These plans and operations would "follow the policy direction of the president and the National Security Council."[8] The Commission also proposed that NCTC "lead strategic analysis, pooling all-source intelligence, foreign and domestic, about transnational terrorist organizations with global reach" and have "the main responsibility for strategic analysis and net assessment" as well as providing warning.[9] Finally, the Report recommended the NCTC director be appointed by the President and confirmed by the Senate, and report directly to a national intelligence director.[10]

President George W. Bush initially created NCTC under the authority of the Director of Central Intelligence (DCI) by way of Executive Order 13354 on August 27, 2004—roughly a month after the Report's release.[11] NCTC absorbed and expanded the existing Terrorist Threat Integration Center—effectively a precursor organization established a year prior to merge and analyze all terrorist-related threat information.

Shortly after President Bush's Executive Order, Congress codified NCTC with the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[12] Under IRTPA, NCTC was to function as the primary organization for "analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism."[13] The latter excepted authority was intended to be retained by the FBI. NCTC was also charged with conducting strategic operational planning for counterterrorism activities and supporting other agencies' counterterrorism efforts, [14] though it did not assume the full operational role envisioned in the Report.[15]

In line with the Commission's stated aim, Congress designed NCTC to break down the siloes across the counterterrorism communities —an animating principle following the 9/11 attacks. Increased coordination and information sharing was to become the modus operandi. Congress gave NCTC statutory authority to assign roles and responsibilities to other agencies, while making clear that NCTC "may not direct the execution of counterterrorism operations."[16] Under IRTPA, NCTC answered to the newly established DNI, as the Commission suggested.

Recommendation in the Rearview

In the early years after NCTC was established, there were several Islamist-inspired terrorist attacks that occurred in the United States that received widespread attention. In 2009, Nidal Hasan launched an attack on the Fort Hood Army Base, leaving 13 dead and more than 30

injured. At the time, the Chairman of the Homeland Security Committee, Senator Joe Lieberman, called the attack "the most destructive terrorist attack on America since September 11, 2001."[17] Senator Susan Collins, the Ranking Member of the Committee, said the attack "raises questions about whether there are unnecessary restrictions on information sharing"[18] among law enforcement and intelligence agencies. At the time of the attack, reports indicated that Hasan had previously been in contact with a known terrorist living in Yemen, information that was not available to all agencies.[19] Due to Hasan's status as an Army Major, this attack raised questions about information sharing between FBI, the Department of Defense (DOD), and NCTC.

In another case from December 2009, a traveler from Nigeria, Umar Farouk Abdulmutallab, attempted to set off an incendiary device onboard an aircraft approaching Detroit—which ultimately failed to detonate. Although information about Abdulmutallab "was available to all-source analysts at the CIA and NCTC prior to the attempted attack, the dots were never connected, and as a result, the problem appear[ed] to be more about a component failure to 'connect the dots,' rather than a lack of information sharing."[20] As President Barack Obama said, "[T]his was not a failure to collect intelligence; it was a failure to integrate and understand the intelligence that we already had."[21]

The Obama administration cited specific failures by the counterterrorism community—NCTC and CIA in particular. The White House press release stated, "NCTC and CIA personnel who are responsible for watchlisting did not search all available databases to uncover additional derogatory information that could have been correlated with Mr. Abdulmutallab."[22] The release went on: "A series of human errors occurred—delayed dissemination of a finished intelligence report and what appears to be incomplete/faulty database searches on Mr. Abdulmutallab's name and identifying information."[23]

In 2012, prompted in part by the Fort Hood attack and failed Detroit airline bombing, the DNI, Attorney General, and NCTC issued new guidelines to improve information sharing and retention of "terrorism information" in federal databases.[24] These new guidelines sought to expand NCTC's ability to obtain, retain, and analyze data in federal databases to help thwart terrorist attacks.

To this day, questions remain as to whether NCTC has all the necessary authorities and tools to deliver on its critical mission, especially in a world where the line between domestic and foreign terrorist threats has increasingly eroded. Testifying before the Committee on May 20, 2026, Dr. Bruce Hoffman, Senior Fellow for Counterterrorism & Homeland Security at the Council on Foreign Relations, questioned why "the principal agency responsible for the analysis and synthesis of terrorist threats and implementation of coordinated counterterrorism strategic operations is legaly barred from taking action to counter domestic terrorism," believing this to be "a dangerous anachronism."[25]

At the same time, the expansion of government data retention at NCTC necessarily raises concerns about protecting the privacy of American citizens. It remains an open question as to whether the right balance has been struck between giving NCTC the necessary tools for national security and protecting Americans' privacy when combatting threats of terrorism, both foreign and domestic.

While terrorist attacks have occurred since the creation of NCTC, raising important questions about its initial efficacy, the center's capabilities have grown since its establishment to match the threat evolution. *The Committee firmly believes that NCTC continues to have an important role to play and is more effective as an independent center distinct from other federal agencies and departments*. NCTC is critical in the counterterrorism fight.

While NCTC has been subject to some criticism, there are a few considerations observers must keep in mind. Perhaps most importantly, the 9/11 Commission believed it would be impossible to eliminate all terrorist attacks:

> We do not believe it is possible to defeat all terrorist attacks against Americans, every time and everywhere…No president can promise that a catastrophic attack like that of 9/11 will not happen again. History has shown that even the most vigilant and expert agencies cannot always prevent determined, suicidal attackers from reaching a target.[26]

Additionally, many of these attacks were carried out by "homegrown" terrorists or lone wolves inspired by foreign terrorist organizations but not in close coordination with or tasked by such organizations. Although domestic terrorism is not a primary responsibility of the IC, reforms to interagency information sharing between intelligence and law enforcement agencies seems to have proven successful in identifying and disrupting U.S.-based individuals in open coordination with foreign terrorist organizations.

Finally, many successes associated with improved information sharing and coordination facilitated by NCTC likely go unreported. Positive stories highlighting these accomplishments rarely draw much attention. Furthermore, the need to protect intelligence and law enforcement sources and methods, as well as to ensure operational security, often requires successful disruptions remain concealed from the public eye. Conversely, intelligence and law enforcement community failures are often criticized in media reporting. This is not to diminish the vital function the media serves in our republic, but rather to recognize the nature of reporting priorities. Media reports often ignite debate and can drive reforms to our system of government, which is a welcome mechanism of change.

As the 9/11 Commission Report says, "the American people are entitled to expect their government to do its very best. They should expect that officials will have realistic objectives, clear guidance, and effective organization."[27] The Committee believes that while NCTC has experienced some hiccups, it is presently the effective organization the American people deserve—with proper congressional oversight.

Unifying the Intelligence Community

Recommendation Adopted: Creation of the DNI and ODNI

The Commission's second major recommendation was to replace the Director of Central Intelligence (DCI) with a "National Intelligence Director" to unify the Intelligence Community.[28] At the time, the DCI performed three main functions: (1) serve as the president's principal intelligence advisor, (2) manage the broader IC, and (3) direct the CIA's day-to-day operations. The Report concluded this was "Too many jobs,"[29] stating that:

> The DCI now has at least three jobs. He is expected to run a particular agency, the CIA. He is expected to manage the loose confederation of agencies that is the intelligence community. He is expected to be the analyst in chief for the government, sifting evidence and directly briefing the President as his principal intelligence adviser. No recent DCI has been able to do all three effectively. Usually what loses out is management of the Intelligence Community, a difficult task even in the best case because the DCI's current authorities are weak. With so much to do, the DCI often has not used even the authority he has.[30]

In response, the Commission proposed a National Intelligence Director (later codified by Congress as the Director of National Intelligence (DNI)) to oversee the IC, manage its budget, improve the efficiency and integration of its programs, and foster greater collaboration between agencies.[31] The DNI would also serve as the principal intelligence advisor to the president, enabling the CIA Director (DCIA) to focus on CIA functions.

As was the case with NCTC, Congress established the DNI through provisions contained in IRTPA.[32] IRTPA also established the Office of the Director of National Intelligence (ODNI) to support the DNI's new functions.[33] ODNI was to be staffed by permanent federal employees, contractors, and military personnel detailed from other intelligence agencies or commands.[34] Since its creation, ODNI has undergone reorganizations consistent with the priorities of successive administrations as well as changes required by Congress. Under the law, the DNI, not the DCIA, is intended to be the principal intelligence advisor to the President.

Recommendation in the Rearview

With the benefit of 20-plus years of experience, the Committee strongly supports the recommendation of the 9/11 Commission, adopted by Congress, to establish the DNI role and accompanying ODNI to shoulder some of the DCI's responsibilities. The Committee agrees with former-DCI George Tenet when he wrote, "A strong case can be made that the three roles in which I served—as head of the Intelligence Community, Director of CIA, and the president's principal intelligence advisor—were too much for any one person."[35] While Tenet simultaneously cautioned against creating a new structure without considering the implications, the Committee believes the 9/11 Commission's recommendation in favor of the new DNI role was correct. Ultimately, the case for a DNI remains as compelling today as it did in the wake of 9/11.

However, three concerns persist regarding the DNI's efficacy: (1) inconsistency in IC management, (2) bureaucratic bloat and inefficiencies as a byproduct of establishing another IC component, and (3) whether the DNI is adequately performing its intended core function as the President's principal intelligence advisor.

First, the Committee believes effective IC management is—and should continue to be—the DNI's primary mission. The DNI plays a valuable role in synchronizing IC collection efforts and analytic priorities, orchestrating authoritative assessments, and supporting overall coordination and collaboration across agencies. However, structural challenges to ODNI's ability to effectively manage the IC remain. Indeed, at the Committee's May 20, 2026 hearing, Dr. Hoffman recounted that, in 2011, 10 years after the Report was issued, the 9/11 Commission's co-chairs expressed dismay that the DNI was still not 'the driving force for Intelligence Community integration that the 9/11 Commission had envisioned.' [They] also noted that the DNI's role over budget and personnel remained 'lamentably ambiguous. These concerns have arguably not abated."[36]

Second, consistent concerns about bureaucratic bloat at ODNI have existed since its creation. What was initially envisioned as a lean, coordinating organization with a "relatively small staff of several hundred people"[37] quickly had its workforce increased significantly and its missions broadened. During the May 20, 2026 hearing before the Committee, Jamil Jaffer, Founder and Executive Director of the National Security Institute at the Antonin Scalia Law School at George Mason University, stated:

> ODNI has gotten way bigger than I think we ever expected it to be. I think narrowing it down and focusing it on a couple of things — budget, authorities, integration — those should be its core rather than all the other things it's got its hands in…. It ought to be a tiger team: smaller, tighter, more focused on integration.[38]

Dr. Hoffman concurred: "I would agree with Professor Jaffer that ODNI has gotten much larger than it was ever intended to be."[39] Former FBI Deputy Director and TSA Administrator John Pistole noted that ODNI "was a great idea to institutionalize the different aspects of the IC, especially as it relates to the collection and analysis and then collection requirements for each of the different agencies," but has "probably outgrown its usefulness in terms of the size and should be streamlined to focus on those key aspects that will help identify and prevent terrorist attacks from happening in the homeland."[40] There have been attempts at rightsizing ODNI, but questions have emerged about whether recent downsizing efforts will have a detrimental effect on key oversight and integration functions of ODNI, which go beyond curtailing unnecessary bloat.

For example, in August 2025, DNI Tulsi Gabbard released a memorandum announcing ODNI's efforts to "eliminate redundant missions, functions and personnel."[41] In this memorandum, ODNI stated that its "ability to fulfill its core mission of protecting Americans against present and future threats has degraded."[42] Since its creation in the aftermath of 9/11, ODNI claimed that it had "become bloated, radically expanded in size, and distracted by tasks and requirements that fall outside its mandate."[43]

Accordingly, ODNI announced changes to its Foreign Malign Influence Center, Cyber Threat Intelligence Integration Center, Mission Integration Directorate, and National Intelligence Council, as well as the elimination of the External Research Council and the Strategic Futures Group. ODNI also announced its intent to "refocus[] functions within … the National Counterproliferation and Biosecurity Center."[44]

The final major concern is whether the DNI is functioning as the president's principal intelligence advisor. Since its inception, tensions between the DNI and DCIA have emerged. With each administration comes different policies and priorities—and different personnel upon whom the president chooses to rely. Some presidents prefer counsel from the DCIA over the DNI, while others may prefer the converse. At times, the DNI had not been properly empowered to carry out full oversight of the IC or did not take full ownership of the role, creating power vacuums that were oftentimes filled by the DCIA or other leaders. These tensions have been present in nearly every administration and have led to a fractured culture within the IC and a DNI role that has not been carried out as originally intended.

Multiple individuals interviewed throughout the process of developing this report expressed similar sentiments, stating that the president's principal intelligence advisor seems to change with every administration. To be sure, given CIA's storied history and operational responsibilities, especially compared to the relatively young ODNI, this is unsurprising. Nevertheless, the overall result is an atmosphere of competition within the upper echelons of the IC vying for the president's attention. This inconsistency, presented every four to eight years, creates downstream effects of uncertainty in the IC about who, statutory responsibilities aside, actually serves as the president's principal intelligence advisor and IC leader.

Recommendation Adopted: Declassification of Topline National Intelligence Program Budget

Another Commission recommendation was to declassify the topline National Intelligence Program (NIP) budget appropriation, stating that "the overall amounts of money being appropriated for national intelligence and to its component agencies should no longer be kept secret."[45] This was intended to foster transparency while not publicly revealing sensitive information. As the Commission explained:

> The top-line figure by itself provides little insight into U.S. intelligence sources and methods. The U.S. government readily provides copious information about spending on its military forces, including military intelligence. The [I]ntelligence [C]ommunity should not be subject to that much disclosure. But when even aggregate categorical numbers remain hidden, it is hard to judge priorities and foster accountability.[46]

In 2007, Congress required the DNI to disclose the NIP appropriation annually but allowed for the President to "waive or postpone the disclosure" if it "would damage national security."[47] ODNI made the first such disclosure that fall.[48] In 2010, Congress amended the law to require the disclosure of the budget *requested* for the NIP for the upcoming fiscal year.[49] While federal law requires only the annual NIP budget request figure to be disclosed, the

Secretary of Defense also began disclosing the annual topline Military Intelligence Program (MIP) budget amount in 2010. The Secretary of Defense also released the total MIP budget appropriations for the three prior fiscal years dating back to 2007.[50]

Recommendation in the Rearview

The Committee believes that adoption of this recommendation has benefited not just Congress and the American people, but the IC as well. Because this recommendation increased transparency, it has fostered greater trust and goodwill among the American public toward the IC—without any observed significant cost to national security. In retrospect, this relatively simple change to the IC has had an outsized positive impact. Transparency should always be the objective in a constitutional republic, unless national security is placed in jeopardy. That is exactly what this recommendation has achieved in the years since it was proposed.

Recommendation Adopted and Since Modified: Establishment of Intelligence Center to Prevent Proliferation of Weapons of Mass Destruction

At the time of 9/11, al Qaeda was the largest transnational Sunni Islamist terrorist organization in the world. The group was founded in the late 1980s by Osama bin Laden and other militants, and issued a series of fatwahs, or legal rulings under Islamic law, that directed attacks against the U.S. and the West in the early 1990s. In August 1996, Bin Laden formally declared war on the United States and in February 1998 declared that "If someone can kill an American soldier, it is better than wasting time on other matters."[51] This eventually led to the al Qaeda launching a series of attacks overseas and eventually led to the terror organization's 9/11 attacks.[52]

The 9/11 Commission Report highlighted al Qaeda's aspirations to acquire weapons of mass destruction (WMDs),[53] noting that "[t]he greatest danger of another catastrophic attack in the United States will materialize if the world's most dangerous terrorists acquire the world's most dangerous weapons."[54] The Report added that, in 1998, there were "reports that Bin Ladin's associates thought their leader was intent on carrying out a 'Hiroshima.'"[55] Accordingly, the Commission offered several recommendations to prevent the proliferation of WMDs, including the establishment of a national intelligence center for joint collection and analysis of intelligence related to the proliferation of WMDs.[56] This new center was to be placed under the authority of the DNI. The import of such a center was echoed by the 2005 Commission on the Intelligence Capabilities of the United States Regarding WMDs.[57]

Congress heeded the 9/11 Commission's recommendation and established the National Counterproliferation Center (NCPC) in the 2004 IRTPA.[58] Since creating NCPC, Congress has modified its mission to meet emerging challenges. For example, during the COVID-19 pandemic, Congress modified NCPC's responsibilities to address public health emergencies, adding a new biosecurity mission.[59] NCPC was subsequently renamed the National Counterproliferation and Biosecurity Center (NCBC) and was tasked with managing intelligence related to "emerging foreign biological threats, including diseases with pandemic potential."[60]

Recommendation in the Rearview

As part of the broader changes undertaken in August 2025, NCBC was significantly reduced and functionally absorbed into other parts of ODNI, rather than continuing in its previous form as a robust standalone mission center. ODNI argued, "Elements within the National Intelligence Council already monitor intelligence related to the proliferation of weapons of mass destruction, making NCBC redundant."[61] Since the redesignation to NCBC during COVID-19, "[I]t has become apparent that taking action to address global health issues falls well outside of ODNI's core mission."[62]

The Committee agrees with the 9/11 Commission Report's recommendation about the need for an intelligence component to focus on the proliferation of WMDs. While the Committee understands ODNI's judgment that NCBC was redundant, WMDs and counterproliferation must remain an area of core focus for the IC. With changes in international WMD arms agreements, new states pursuing nuclear energy, and the constant threat of nonstate actors acquiring such weapons, the counterproliferation of WMDs has only grown in importance. While avoiding redundancy, it is vital that the IC maintain counterproliferation expertise.

The WMD challenge is complicated by the related and equally important issue of biosecurity. The COVID-19 pandemic revealed the terrifying and enduring danger of biological threats, and the imperative that the IC be well-postured to collect and analyze intelligence related to such threats.

Strengthening the FBI and Homeland Defenders

Recommendation Adopted: Continued FBI Role in Domestic Intelligence

The 9/11 Commission considered endorsing the creation of a new domestic intelligence agency but ultimately concluded it would not be necessary "if our other recommendations are adopted—to establish a strong national intelligence center, part of NCTC, that will oversee counterterrorism intelligence work, foreign and domestic, and to create a [DNI] who can set and enforce standards for the collection, processing, and reporting of information."[63]

Instead, the Commission believed that the FBI was best situated to fill this role, especially if the Bureau substantially enhanced its intelligence capabilities. The Commission validated concerns about the FBI conducting domestic intelligence because the agency "has long favored its criminal justice mission over its national security mission,"[64] leading to questions about whether it could competently and promptly deliver on intelligence work. In the aftermath of the 9/11 attacks, it became clear the FBI had prioritized its law enforcement responsibilities over its intelligence mission, a posture that may have contributed to its failure to detect and disrupt the plot.

This was a reasonable development; after a series of scandals regarding domestic surveillance from the 1950s through the 1970s that resulted in public congressional investigations, the FBI pivoted away from domestic intelligence efforts. The Commission explained, "The FBI was criticized, rightly, for the overzealous domestic intelligence investigations disclosed during the 1970s."[65] At least partly as a result, "[t]he pendulum swung away from those types of investigations during the 1980s and 1990s."[66]

Despite this, the Commission noted that the FBI had "maintained an active counterintelligence function and was the lead agency for the investigation of foreign terrorist groups operating inside the United States."[67] The FBI was now needed to rise to the occasion and:

> [B]e able to direct its thousands of agents and other employees to collect intelligence in America's cities and towns—interviewing informants, conducting surveillance and searches, tracking individuals, working collaboratively with local authorities, and doing so with meticulous attention to detail and compliance with the law. The FBI's job in the streets of the United States would thus be a domestic equivalent, operating under the U.S. Constitution and quite different laws and rules, to the job of the CIA's operations officers abroad.[68]

The Commission also assessed that establishing a new domestic intelligence agency outside of the Department of Justice would challenge legal oversight and noted, "Abuses of civil liberties could create a backlash that would impair the collection of needed intelligence."[69] In addition to "exacerbat[ing] existing information-sharing problems," a new agency would "need to acquire assets and personnel"—infrastructure the FBI already maintained.[70]

The Commission was supportive of then-FBI Director Robert Mueller's pursuit of reforms to improve the FBI's intelligence capabilities, including creating an Office of Intelligence, improving recruitment and training for intelligence professionals, and promoting greater intelligence sharing among the FBI's field offices.[71] The Commission wanted to ensure that these reforms were "more fully institutionalized" and recommended that a "specialized and integrated national security workforce should be established at the FBI consisting of "agents, analysts, linguists, and surveillance specialists, who [were] recruited, trained, rewarded, and retained to ensure the development of an institutional culture imbued with a deep expertise in intelligence and national security."[72] This was sufficient for the Commission, and for Congress, which ultimately never moved to create a new domestic intelligence agency.

Recommendation in the Rearview

The Committee agrees with the Report's recommendation against the creation of a new domestic intelligence agency to address the terrorism threat. We conclude, as did the 9/11 Commission, that the FBI is the proper organization for this role. The domestic intelligence infrastructure at the FBI was already in place, including the personnel, processes, training, and capabilities to effectively deliver on this mission while maintaining the integral arrest authorities to mitigate terrorist plots.

In the wake of the 9/11 attacks, then-FBI Director Robert Mueller adopted reforms to enhance and improve the FBI's intelligence capabilities. As Mr. Pistole testified at the May 20, 2026 hearing, this was one of the "major sea changes for the FBI," where it transformed "from probably the premier law enforcement agency in the world, perhaps, to that of a collection, analysis, and information-sharing agency."[73] The Committee believes this recalibration has brought many successes in keeping the American people safe but also carries risks which call for continued robust oversight.

For example, as with any human institution, there have been abuses of intelligence capabilities over the last two decades. Robust public debate, especially as it relates to the Foreign Intelligence Surveillance Act, has been front and center. The Committee acknowledges that any misuse or abuse raises serious questions about the need to protect the civil liberties of the American people while protecting national security. The Reforming Intelligence and Securing America Act passed in 2024 is the latest necessary reform in a series of legislative actions.

The Committee is mindful that there is consistent push and pull within the FBI about the degree to which the organization is an *intelligence* organization in addition to a law enforcement organization. This tension may not be fully solvable, but it certainly demands the attention of senior leaders within the FBI to strike the best balance in support of national security missions.

While imperfections exist within the FBI which necessitate consistent oversight attention, and reforms are occasionally necessary, the Committee ultimately agrees that creating a new domestic intelligence agency was not the proper path to address the threat—particularly because, within the homeland, FBI must disrupt threats instead of merely collecting intelligence on them. Moreover, with the surveillance controversies that have emerged at the FBI, creating a new domestic intelligence agency would likely only exacerbate these concerns. Instead, the FBI is the proper place for these capabilities, and Congress must remain vigilant in its oversight role to hold FBI accountable and prevent misuse or abuse.

The Committee also agrees with the Report's emphasis on the FBI establishing and maintaining a deep, expert counterterrorist arm. While the FBI's responsibilities are myriad, it is vital that there remain a fully staffed cohort who are not drawn away from the counterterrorism mission.

Recommendation Not Adopted: Cede CIA Paramilitary Operations to Department of Defense

Another recommendation in the 9/11 Commission Report was for DOD to have a leading role in paramilitary operations, removing paramilitary authorities from the CIA.[74] The Report stated that "[t]he United States should concentrate [paramilitary] responsibility and necessary legal authority in one entity,"[75] finding CIA paramilitary operations to be redundant with those already existing within the DOD. It further determined that the CIA lacked the required military training to carry out paramilitary operations.[76] The Commission stated: "Whether the price is measured in either money or people, the United States cannot afford to build two separate capabilities for carrying out secret military operations, secretly operating standoff missiles and secretly training foreign military or paramilitary forces."[77] Accordingly, the Commission recommended that CIA paramilitary responsibilities "be consolidated with the capabilities for training, direction, and execution of such operations already being developed in the Special Operations Command."[78]

This recommendation was never adopted by Congress, nor was it ever accepted by the Executive Branch. In November 2004, President Bush asked the Secretary of Defense and the DCI to review this recommendation and to submit their views on the matter by February 2005.[79] Prior to the February deadline, the CIA Director provided unclassified testimony to the Senate

Select Committee on Intelligence that the CIA and DOD disagreed with the Commission's recommendation.[80] Furthermore, in an NBC News article from 2005, it was reported that then-Secretary of Defense Donald Rumsfeld and then-CIA Director Porter Goss opposed the 9/11 Commission's recommendations.[81] The two senior officials reportedly stated in a letter that "' Neither the CIA nor (the Defense Department) endorses the commission's recommendation on shifting the paramilitary mission or operations.'"[82] The letter continued, "'We do not believe change is required in the responsibility of the CIA for foreign intelligence collection and covert action or activities, or that of the DoD for traditional military activities.'"[83]

To date, Congress has not realigned CIA's paramilitary operations to the DOD. However, Section 1013 of IRTPA (P.L. 108-458) does require DOD and CIA to develop joint procedures "to improve the coordination and deconfliction of operations that involve elements" of the CIA and DOD. Additionally, IRTPA maintains that if the CIA and DOD have separate missions ongoing in the same geographical regions, they are required to establish procedures to come to a "mutual agreement on the tactical and strategic objectives for the region and a clear delineation of operational responsibilities to prevent conflict and duplication of efforts."

Recommendation in the Rearview

With respect to the 9/11 Commission's recommendation to shift CIA's paramilitary operations to DOD—a recommendation not adopted by Congress—the Committee recognizes there are good-faith arguments on both sides of the issue.

The Commission identified inefficiencies, ineffectiveness and redundancies by having two components separately engaged in paramilitary activities. The Commission also warned that paramilitary operations at CIA could draw attention and resources away from core foreign intelligence missions. However, the principal argument against the Commission's recommendation involves the current policy constraint in Executive Order 12333 that covert actions are conducted exclusively by the CIA unless the President tasks another agency. Covert actions are activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly. Simply stated, the United States requires operational capabilities where the government's involvement is not apparent, acknowledged, and can be disavowed.

Therefore, Congress should debate whether to reconsider the Commission's recommendations to consolidate paramilitary activities within the DOD's special operations forces.

Unifying Effort in Sharing Information

A Work in Progress: Incentivizing and Enabling Information Sharing

The 9/11 Commission Report emphasized the need for both structural and cultural improvements to information sharing between intelligence agencies. Fundamentally, the Report noted, "Each agency's incentive structure opposes sharing, with risks (criminal, civil, and

internal administrative sanctions) but few rewards for sharing information."[84] This was particularly salient in the divisions between intelligence and law enforcement communities, including both within and external to the FBI.[85]

The Report also highlighted the importance of information sharing with federal agencies beyond the Intelligence Community, many of which lacked sufficient equipment to substantively participate in classified conversations. Concurrently, other agencies had access to vast amounts of information not traditionally considered intelligence, but which could be invaluable for analysis.

The Report suggested pursuing a "decentralized network model" by which officers across agencies could access each other's reports, while incorporating security measures.[86] It warned against overclassification and excessive compartmentation of information among agencies and endorsed portion-marking to ensure that even if source characterizations are too sensitive to share, the fundamental information garnered still can be proliferated.[87]

Beyond structural concerns, the Report strongly described the lack of information-sharing culture in some IC agencies, noting an "almost obsessive protection of sources and methods."[88] The Report similarly noted, "Agencies uphold a 'need-to-know' culture of information protection rather than promoting a 'need to share' culture of integration."[89]

Congress attempted to address some of these concerns through IRTPA, which tasked the newly created DNI with promoting intelligence information sharing within the Intelligence Community and required the Executive to establish a secure information sharing environment for intelligence and related information.[90]

Recommendation in the Rearview

Intelligence sharing has greatly improved since 9/11, in part due to technological advancements that facilitated greater IC-wide access to intelligence reports and assessments. There is no longer an unbreachable 'wall' between law enforcement and intelligence information, though hurdles still exist in making sure information garnered in either instance is appropriately shared with the other. This is also an endemic concern with operational reporting, which sometimes does not 'meet threshold' for inclusion in a formal report, though it may be a small but important part of an otherwise unsolved puzzle – as was evident in CIA's undistributed reports regarding its tracking of one of the hijackers.[91]

Intelligence agencies have also recently been publishing more internal products, visible to their senior leaders but not other agencies. This worrying trend minimizes coordination and dampens cross-agency sharing of analytic judgments, rendering potentially poorer assessments and siloed thinking.

Finally, while it has made great strides, the IC still can improve how it shares critical information with federal agencies outside of the intelligence community. These 'NT-50s' include agencies such as the Departments of Agriculture and Commerce, whose work increasingly overlaps with national security.

Unifying and Strengthening Congressional Oversight

Recommendation Partially Adopted: Changes in Congressional Oversight

In its Report, the 9/11 Commission called Congress's oversight of intelligence and counterterrorism "dysfunctional" and proposed several relevant reforms.[92] Insisting that the "House and Senate intelligence committees lack the power, influence, and sustained capability,"[93] the Commission recommended HSPCI and the Senate Select Committee on Intelligence (SSCI) be merged into a joint committee on intelligence, and that this joint committee include a subcommittee on oversight.[94] As an alternative to creating this new joint intelligence committee, the Commission recommended a novel approach: combining authorization and appropriation authorities for the IC in each chamber's congressional intelligence committee.[95] This approach, if adopted, would be novel, as there are no examples of authorizing and appropriating powers combined under any other congressional committee of jurisdiction.

The Commission also recommended separating the National Intelligence Program (NIP) appropriation from defense appropriations.[96] To date, Congress has not adopted either recommendation. Currently, the Intelligence Authorization Act (IAA), which authorizes NIP activities, and the Defense Appropriations Act, which funds most of those activities, are considered separately in their respective authorizing and appropriation committees. This process oftentimes leads to differences between what is authorized and appropriated. This disconnect has caused significant concerns relating to the intelligence committees' ability to conduct oversight. Some national security experts believe that by combining authorizations and appropriations, HPSCI and SSCI would be able to conduct better oversight.

The Report also recommended changing HPSCI and SSCI rules so that the majority did not exceed the minority representation by more than one member.[97] It also recommended abolishing term limits on the intelligence committees to allow members to accumulate experience.[98]

As for oversight measures that Congress has adopted, Senate Resolution 445 (S.Res. 445) and House Resolution 35 (H.Res. 35) contain provisions incorporating some of the Report's recommendations.

In October 2004, S.Res. 445 was adopted by the Senate, increasing the authority of SSCI. S.Res. 445 also amended S.Res. 400 to expand the jurisdiction of the Senate Committee on Homeland Security and Government Affairs to include intelligence oversight.[99] It also provided SSCI with the jurisdiction to hold hearings and report on presidential nominations of civilians to senior IC positions before they are confirmed by the full Senate.[100] It created ex officio member seats to the Chair and Ranking Member of the Senate Armed Services Committee.[101] It also abolished the eight-year term limit on SSCI members and removed the requirement that to the greatest extent practicable one-third of its members did not serve on the committee during the previous Congress.[102] Finally, it created a Subcommittee on Oversight and provided for the establishment of a Subcommittee on Intelligence in the Senate Committee on Appropriations.[103] However, to date, this new subcommittee has not been implemented.

H.Res. 35, passed in January 2007, established the Select Intelligence Oversight Panel (SIOP) of the House Committee on Appropriations (HAC) to:

> Review and study on a continuing basis budget requests for and execution of intelligence activities; make recommendations to relevant subcommittees of the Committee on Appropriations; and, on an annual basis, prepare a report to the Defense Subcommittee of the Committee on Appropriations [HAC-D] containing budgetary and oversight observations and recommendations for use by such subcommittee in preparation of the classified annex to the bill making appropriations for the Department of Defense.[104]

The SIOP would "be composed of not more than 13 Members… appointed by the Speaker, of whom no more than eight may be from the same political party."[105] It would include the HAC chairman and ranking member, the HAC-D chairman and ranking minority member, six additional HAC members, and three HPSCI members.[106] Despite the creation of the SIOP, HAC-D still retained the authority to report an intelligence bill to the full House Appropriations Committee (HAC).

Four years after the SIOP's creation, it was disbanded.[107] After the SIOP was dissolved, HPSCI and HAC agreed to have three HAC members participate in HPSCI hearings and briefings. Then-HPSCI Chairman Mike Rogers stated, "This partnership will knit together the Intelligence Committee with the Appropriators and will allow key appropriators important insights into the Intelligence Community which they fund."[108] He continued, "The 9/11 Commission recommended that the Congressional authorization and appropriation committees work more closely on intelligence matters."[109] Arrangements to foster greater collaboration between HPSCI members and appropriators remain in place to date.

Recommendation in the Rearview

The Committee agrees with the Commission's position that "strengthening congressional oversight may be among the most difficult and important…Few things are more difficult to change in Washington than congressional committee jurisdiction and prerogatives. To a member, these assignments are almost as important as the map of his or her congressional district."[110] While much has changed in the world since the release of the Report, challenges with reforming congressional oversight have not.

While the 9/11 Commission Report's recommendation to create a joint committee on intelligence to consolidate authorizations and appropriations in HPSCI and SSCI has never materialized, these novel recommendations still draw attention today. At the May 20, 2026 hearing before the Committee, Mr. Jaffer testified that "Congress ought to take seriously the recommendation made by the 9/11 Commission[] from over two decades ago that our appropriations system for intelligence is broken," and further stated that "there are ideas about [establishing] a joint committee, ideas about combining authorizations and appropriations."[111] He concluded that, at the very least, Congress should consider creating intelligence appropriations subcommittees within the House and Senate Appropriations Committees.[112]

At the May 20, 2026 hearing, Representative Dan Crenshaw asked Mr. Jaffer why he thought the 9/11 Commission recommendation to combine appropriations and authorizations within the Committee was a good idea, to which Mr. Jaffer responded:

> It would make life a lot easier if the authorizers could decide where the money was going to be spent and then actually put those monies on target, it would solve the two-step problem of having to convince more people about a given issue. [HPSCI] has a specific role and mission — it was designed to focus in on intelligence programs…If you're separated from the money…it makes it impossible to actually action [those priorities]. Think about all the overhead collection programs that we have that this committee has sought to prioritize but can't get the Appropriations Committee to support…So if you combined it, that would make life easier for this committee, it would take the real experts in this room and allow you to actually put lead on target…If we can't get there [combining authorizations and appropriations], then the next step might be creating an intelligence subcommittee [within Appropriations]…[and cross-appoint] members of this committee, including the Chair and the Ranking Member, to that Appropriations [sub]committee, and you'd essentially solve the problem but work within the current constraints.[113]

In the same hearing, Mr. Pistole agreed, and stated that the current process was challenging and stated that "[h]aving to testify before both authorizers and appropriators" was "cumbersome."[114] Instead, "combining them into a streamlined process, maybe not some kind of hybrid, would help everybody in terms of addressing national security issues…There needs to be a sense of urgency on all sides, and having this…bifurcated process I think gets away from that sense of urgency."[115]

The Committee agrees with Mr. Jaffer and Mr. Pistole's assessment reiterating the 9/11 Commission's recommendation to more closely align the authorization and appropriations bodies within Congress to better tailor funds for the Intelligence Community. The need for stronger congressional oversight was great in the immediate aftermath of 9/11, and that need has only grown in the two decades since it was proposed.

A Work in Progress: Adopting Traveler Screening and a Biometric Entry-Exit Screening System

The Committee would be remiss if it neglected to address recommendations contained in the 9/11 Commission Report related to screening foreign nationals traveling in and out of the United States—and the serious threat unvetted travelers can pose to the homeland. Indeed, the 9/11 story itself is one of known terrorists moving freely across borders, skirting screening protocols, and altering identification documents to evade law enforcement. The 9/11 Commission addressed the threat posed by lax screening policies by injecting border security—not previously "seen as a national security matter" in "national security circles" at the time—into the national security discourse.[116]

The Commission believed closer interaction between border security agencies and the Intelligence Community could help address this threat: "Since officials at the borders encounter

travelers and their documents first and investigate travel facilitators, they must work closely with intelligence officials…Dedicated specialists and ongoing linkages with the intelligence community are also required," including "intelligence on indicators of terrorist travel."[117]

The Commission "found that as many as 15 of the 19 hijackers were potentially vulnerable to interception by border authorities" and further stated, "Analyzing their characteristic travel documents and travel patterns could have allowed authorities to intercept 4 to 15 hijackers and more effective use of information available in U.S. government databases could have identified up to 3 hijackers."[118] The Commission continued, saying that "the routine operations of [U.S.] immigration laws…inevitably shaped al Qaeda's planning and opportunities."[119] The Commission found that:

> Had the immigration system set a higher bar for determining whether individuals are who or what they claim to be—and ensuring routine consequences for violations—it could potentially have excluded, removed, or come into further contact with several hijackers who did not appear to meet the terms for admitting short-term visitors.[120]

The Report found that "two systemic weaknesses came together in our border system's inability to contribute to an effective defense against the 9/11 attacks: a lack of well-developed counterterrorism measures as a part of border security and an immigration system not able to deliver on its basic commitments, much less support counterterrorism."[121]

Positing that "[t]argeting travel is at least as powerful a weapon against terrorists as targeting their money,"[122] the Commission offered multiple recommendations to improve vetting of foreign nationals entering the borders of our country:

- "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."[123]
- "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 systemwide 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."[124]
- "The Department of Homeland Security, properly supported by Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for screening qualified travelers…Linking biometric passports to good data systems and decision-making is a fundamental goal…[T]oday, a terrorist can defeat the link to electronic records by tossing away an old passport and slightly altering the name in the new one."[125]

This last recommendation regarding the implementation of a biometric entry-exit system to prevent terrorist travel into the homeland—informed by the preceding two recommendations—is the focus of this section.

Today, the status of air, sea, and land biometric entry-exit collection systems varies. The following graphic captures the status of biographic and biometric entry-exit systems at various points of entry (POEs) in the United States:

Mode of Travel	Biographic	Biometric
Air entry	Complete	Complete
Air exit	Complete	Nearly complete[a]
Sea entry	Complete	Complete
Sea exit	Complete	Incomplete
Land entry—pedestrians	Complete	Complete
Land entry—vehicles	Complete	Incomplete
Land exit—northern border	Complete	Incomplete
Land exit—southern border	Incomplete; using re-entry data	Incomplete

Sources: DHS, *Traveler Verification Service*, DHS/CBP/PIA-056, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf; and GAO, *Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues*, GAO-22-106154, July 27, 2022, https://www.gao.gov/assets/gao-22-106154.pdf; email communication from CBP to CRS on April 12, 2023.

Notes: Sea entry and exit refers to cruise passengers, not crewmembers. For information on crewmembers, see DHS, *Traveler Verification Service*, p. 42.

a. As of July 2022, the biometric air exit system was approximately 80% complete and it is continuing to be implemented nationwide.

There have been several legislative actions, preceding and following the 9/11 Commission's recommendations, to implement an integrated biometric entry-exit screening system for foreign nationals wishing to travel to the United States. Prior to the release of the Report, Congress had attempted to implement an automated entry-exit system to vet and adequately record the movement of noncitizens in and out of the United States—most notably with the passage of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) and later amendments to it.[126] The data collection at the time was foremost focused on gathering biographical data of noncitizens, such as names, descriptions, and countries of origin. The 9/11 attacks prompted new calls for increasing screening capabilities by collecting biometrics, such as fingerprints, iris scans, or facial recognition technology, which are much harder to falsify than biographic data.

Shortly after the September 11th attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act). The USA PATRIOT Act required the Attorney General to implement the biographical portion of the IIRIRA's entry-exit system "with all deliberate speed."[127] The IIRIRA entry-exit system was also further directed to utilize biometric technology and promote tamper-resistant identification documents.[128] Additionally, the USA PATRIOT Act mandated increased entry-exit information sharing with law enforcement databases—an attempt at deconstructing the wall between intelligence and law enforcement—to better detect individuals from entering the country who pose a threat to national security.[129]

The following year, Congress passed the Enhanced Border Security and Visa Entry Reform Act of 2002, requiring the Attorney General to establish integrated arrival and departure databases in line with the technological standards of the USA PATRIOT Act entry-exit system.[130] An additional provision focused on improving interoperability among all security databases to determine the admissibility of noncitizens into the United States.[131] Additionally, two years later, Congress tasked the Department of Homeland Security (DHS) with developing a plan to accelerate the implementation of an automated biometric entry-exit system,[132] and built on prior legislation requiring a fully automated entry-exit system to collect arrival and departure records for travelers under the Visa Waiver Program at sea and air POEs.[133] In 2008, Congress included a provision in annual appropriations legislation to withhold funds until DHS demonstrated a path toward implementation.[134] In 2015 and 2018, Congress authorized temporary fee increases on employer petitions for L-1 and H-1B worker visas to help fund the a biometric exit system;[135] this system was further buttressed in the 2025 budget reconciliation package.[136]

The executive branch has also taken steps to implement a biometric entry-exit system. In March 2017, President Donald J. Trump directed DHS to "expedite the completion and implementation of a biometric entry-exit tracking system for all travelers to the United States, as recommended by the National Commission on Terrorist Attacks Upon the United States."[137] In October 2025, CBP amended its regulations to allow DHS to require photographs from all noncitizens arriving and departing the United States; DHS previously only fielded biometric exit pilot programs at 15 air or seaports.[138]

In March 2025, CBP announced a new pilot program to collect facial images from certain noncitizens upon exit as part of its initiatives to create a comprehensive biometrics entry-exit system.[139] Under this program, eligible participants, via a CBP application, would photograph themselves after exiting.[140] The application employs geolocation services to confirm the participant left the United States and uses software to ascertain that it is a live photo.[141]

These actions have steadily improved U.S. screening capabilities toward a comprehensive biometric entry-exit system. Today, air and sea points of entry, as well as pedestrian land points of entry, all have fully implemented biometric systems.[142] Challenges remain with collecting land-entry biometrics on incoming vehicles, but CBP is currently piloting facial recognition technology for travelers entering the U.S. in personally owned or commercial vehicles.[143] Conversely, *exit* systems have historically proven especially difficult to implement, and the U.S. has not fully implemented a biometric exit screening system at any point of entry category.[144]

Recommendations in the Rearview

The Committee believes the 9/11 Commission's recommendation to establish a fully automated biometric entry-exit screening system is of utmost importance. Twenty-five years after the 9/11 attacks occurred, few issues have garnered as much national—and international—attention as mass migration—authorized and unauthorized, temporary or permanent. In recent years, adversaries have sought to take advantage of the United States' immigration and visa posture., This includes members of foreign terrorist organizations (FTOs), special interest aliens

from hostile foreign countries,, and agents of foreign adversaries traveling under business or student covers, all to undermine our national security.

Today, the State Department routinely denies foreign nationals' visa applications on national security grounds. According to recent available data, hundreds of immigrant and nonimmigrant visa applications are refused on security-related grounds every year.[145] At the southern and northern borders, hundreds of foreign nationals have been encountered that appear on the Terrorist Screening Dataset (TSDS).[146] This number has recently grown to the thousands,[147] most likely because of the recent designation of international cartels as foreign terrorist organizations in 2025.[148] While CBP has stated that "terrorism-related encounters at our borders represent an extremely small portion of total border encounters,"[149] we must remember that an extremely small number of terrorists perpetrated the 9/11 attacks. In both the visa application review process and encounters at our national borders, our biometric and biographic entry-exit system capabilities play a vital role in denying dangerous foreign nationals from entering our country or apprehending them if they do succeed at gaining entry.

Since the 9/11 Commission proposed to upgrade the American screening system from a biographic entry-exit system to an automated biometric entry-exit system, Congress and the executive branch have taken affirmative steps to implement the recommendations. Despite efforts by Congress and the executive branch, the current biometric entry-exit system has not been fully implemented, largely due to infrastructure and practical challenges. Consequently, there remains a gap between the current biographic entry-exit system and the biometric entry-exit system envisioned by the 9/11 Commission.

While challenges remain in fully implementing a biometric entry-exit system, primarily with regards to biometric exit data collection, technological progress over the last two and a half decades presents an opportunity to close the gap. What can be achieved today, especially with the introduction of new technologies such as artificial intelligence, far exceeds what was possible in 2004. In the context of improving biometric screening of foreign nationals traveling in and out of the United States, our nation is far better positioned today to achieve the aims of the 9/11 Commission's recommendation. Moreover, the Committee recognizes that screening and vetting is a highly intelligence-dependent enterprise. Without sufficient foreign intelligence collection on terrorism, the information about potential terrorist suspects who require further scrutiny will not exist to be added to the relevant screening and vetting databases. Without effective intelligence, the capabilities of a successful screening and vetting enterprise are not nearly as useful in protecting Americans from harm.

The Committee cannot fail to recognize the role intelligence plays in addressing the issue of unauthorized travel into the homeland—and visa overstays—by dangerous foreign nationals. The Intelligence Community, federal law enforcement, and state and local partners must be capable of locating, tracking, interdicting, or denying entry to those who pose a threat to the homeland. The current system fails to sufficiently allow for effective identification and removal of foreign terrorist or intelligence operatives. In the 21st century, the lack of a fully automated biometric entry/exit system impedes efforts to address this issue.

Reccomendations in the Rearview: Summary

From a macro perspective, the Committee believes the Report's recommendations, to the extent they have been adopted, have largely proven successful in achieving their primary objective, namely to help prevent a terrorist attack of similar magnitude to September 11th on American soil. While testifying before this Committee on May 20, 2026, Dr. Hoffman concluded:

> This is a towering achievement. During the dark and fearful days following 9/11 and the early years of the war on terror, such a result was then a matter of faith and hope and was far from certain. It is proof how important the 9/11 Commission's recommendations and [the] 2004 Intelligence Reform and Terrorism Prevention Act have been in keeping our country safe from another massive terrorist attack.[150]

Of course, implementation of the Report's recommendations is not the sole reason that another 9/11-like attack has not been perpetrated against the United States. There are many reasons terrorist plots are foiled, such as luck, swift action by vigilant citizens, or assistance from global law enforcement partners. Some amalgam of these factors, combined with the adopted reforms, have thus far prevented another significant intelligence failure and subsequent large-scale terror attack. Nevertheless, shortcomings emerged in the post-Report era that warranted attention from Congress and the Executive Branch.

Moreover, while the Report recommendations that were adopted have been largely effective in achieving their objectives, there are concerns that have emerged regarding whether the post-9/11 structure of the Intelligence Community is appropriate considering new threats that have emerged.

Some of the gaps highlighted in this section have only been exacerbated by a world that has evolved dramatically since the publishing of the 9/11 Commission Report in 2004. Rapid technology developments and the return of great power competition have significantly changed the threat landscape.

In a hearing before the Committee on July 21, 2026, HPSCI Chairman Rick Crawford addressed the new and emerging threat landscape we now face:

> Twenty-five years since the September 11th attacks, one thing has become abundantly clear: The post-9/11 intelligence challenges have expanded far beyond counterterrorism coordination. While our fight against terrorism remains a high priority, we now face a broader and more complex security environment. To be sure, the 9/11 Commission's core lessons of improved information sharing and coordination within the IC and law enforcement remain as critical as ever. But the threat landscape has evolved significantly over the last 25 years. Consider technological advancements in AI, quantum computing, drones, cyber and bio threats. Consider our country's renewed focus on competition and conflict with great powers and strategic rivals, asymmetric and irregular warfare, foreign malign influence, economic warfare, espionage, and gray zone aggression, all increasingly common threat streams. We've seen China and Russia exploit domestic security

> gaps and take advantage of our counterintelligence vulnerabilities. The list of new threats could go on.[151]

These issues are the focus of the following section.

How Has the Threat Landscape Evolved?

The current threat landscape has evolved in ways that extend far beyond the Report's counterterrorism-centered framework. While foreign terrorist organizations remain a significant concern, the United States now faces a broader and more complex security environment shaped by strategic competition, cyber operations, coercive economic practices, and nuclear proliferation, as well as asymmetric and irregular warfare. In addition, many of the examples outlined in this section are not new threat streams. What has changed is how these threats have evolved given technological advancements and geopolitical shifts.

The post-9/11 threat environment is no longer defined primarily by hierarchical terrorist organizations planning large-scale attacks from overseas safe havens. Instead, threats now emerge from both state and non-state actors operating across multiple domains and have created the conditions in which adversaries increasingly combine conventional, unconventional, and technological tools. The result is a more ambiguous and multidimensional threat landscape, one that requires intelligence agencies to identify strategic competition, technological vulnerabilities, and adversarial influence across public and private sectors.

The following sections examine key categories of emerging threats that define the transformed security environment the United States faces today.

Great Power Competition

The return of our nation's focus on competition and conflict between great powers and strategic rivals represents one of the most important changes in the security environment since the Report. Counterterrorism, counterinsurgency, and stabilization operations dominated the post-9/11 era. Today, U.S. national security strategy is increasingly shaped by competition with the People's Republic of China (PRC) and Russia, both of which possess advanced military capabilities, nuclear forces, cyber capabilities, hybrid commercial cover mechanisms, sophisticated intelligence services, and global strategic ambitions. These two countries, often in partnership with each other, North Korea, and Iran, pose a geopolitical challenge our nation has not confronted since the Cold War.

The Chinese Communist Party (CCP), led by President Xi Jinping, is widely viewed as the most comprehensive long-term strategic competitor to the U.S. Under Xi's leadership, the PRC has adopted a culture that uses a whole of society approach in challenging the U.S. and is positioning itself to become the new global hegemon. U.S. intelligence has described China as the leading military and cyber threat, with capabilities including conventional strike systems, cyber operations against infrastructure, and the space domain, as well as ambitions to lead in artificial intelligence.[152] Beyond the military sphere, China has been able to challenge the U.S. through economic influence, technological competition, diplomatic pressure, transnational repression of its diaspora dissidents, and efforts to reshape international norms. China has also employed various tools to expand its global presence and generate leverage over poorer nations by creating debt traps or overpromising on critical infrastructure needs, including through its Belt and Road Initiative.[153]

Russia also remains a major military and intelligence threat, particularly because of its nuclear arsenal, cyber capabilities, war in Ukraine (and subsequent destabilization of Europe), and willingness to use covert and irregular tools.[154] President Vladimir Putin has attempted to expand the Russian Federation and recapture influence over former republics of the Soviet Union. Russia has a larger presence than any country in the Arctic and has exerted significant control over shipping lanes in the region.[155] Regardless of the motivation for President Putin's aggressive moves toward expansion, or the means of achieving it, the Russian Federation is shrewdly looking outward and this threat will continue to metastasize.

Further exacerbating the threats posed by China and Russia is how these two nations have not only aligned themselves when it is convenient for their respective strategic interests, but also how both nations have utilized Iran and North Korea to also challenge the West.[156] Russia has utilized North Korean troops on the front lines in its conflict in Ukraine. This has solved Russia's issues associated with casualty troop attrition rates.[157] In recent years, China has provided Iran with significant economic, technological, and diplomatic support.[158] In exchange, China has been able to benefit from cheap, sanctioned oil that fuels its economy.[159]

At a recent Committee hearing, former National Security Advisor to the President H.R. McMaster highlighted in his prepared remarks the threats posed by the connections these countries have formed and the implication of these threats to the United States. He has called these relationships "the axis of aggressors" and urged in his testimony that the Intelligence Community "must organize to identify and counter those threats, exploit vulnerabilities, and isolate the axis from sources of mutual support."[160]

As highlighted above, the evolving strategic landscape has forced the Intelligence Community to adapt in order to balance the threats strategic competition poses and better understand how these impact the United States' national security interest.

Counterintelligence Threats to the United States

With great power competition, counterintelligence has reemerged as a significant challenge facing the United States. In the immediate aftermath of 9/11, intelligence reform focused heavily on improving the government's ability to detect, disrupt, and prevent terrorist attacks, surging resources to support the counterterrorism mission. While counterterrorism efforts should remain a high priority for the Intelligence Community, the United States must not lose sight of other threat vectors. Some argue that our nation's overfocus on counterterrorism threats has caused our government to develop tunnel vision and lose sight of our nation's counterintelligence mission in the domestic space, a vulnerability that nations like China and Russia are more than willing to exploit.

Foreign intelligence threats have remained a persistent threat to our nation's security, reaching its apex with attention and resourcing during the Cold War. That era focused primarily on preventing the Soviet Union from usurping the West militarily, subverting our nation from within, and spreading communism abroad. With the conclusion of the Cold War in the early 1990s, attention and resourcing for the counterintelligence mission diminished and then dropped with the advent of the Global War on Terror (GWOT).

For two decades, while the U.S. was focused on GWOT, resourcing of the counterintelligence mission failed to keep pace as adversary states advanced strategic objectives to penetrate U.S. institutions, steal sensitive information, manipulate decision-making, and exploit the openness of American society. These threats are not limited to traditional espionage against government agencies—harkening back to the Cold War era, they extend to universities, research laboratories, the defense industrial base, technology firms, state and local governments, and private-sector critical infrastructure providers. Our nation is under persistent attack by foreign actors seeking to undermine our national security and the American way of life.

The unfortunate reality is that our nation's counterintelligence posture is outdated and outmatched by the scope and scale of threats presented by hostile foreign powers. Today's counterintelligence threat landscape is vastly more complex and expansive than the threats presented during the Cold War. Yet our current counterintelligence approach is reactive rather than proactive. It focuses on identifying and prosecuting spies—or other acts of espionage or subterfuge—after the damage is done. The system measures success by incentivizing and prioritizing investigations, indictments and prosecutions, rather than proactive disruptions of adversary operations. Given the scale of foreign intelligence targeting of U.S. interests, a reactive posture inhibits strategic deterrence by having a minimal effect on an adversary's risk-gain calculus, resulting in more malign operations, not fewer. In other words, our counterintelligence posture can be categorized as "too little too late." Our adversaries masterfully exploit this vulnerability and have gained significant strategic advantages as a result.

Stepping into this vulnerability gap is China, which currently presents the greatest counterintelligence threat our nation faces. In a recent interview, FBI Director Kash Patel stated:

> The CCP engage[s] in the greatest level of espionage against the United States of America. And particularly troubling is how they acquire land and real estate in and around military bases. Particularly troubling…is Salt Typhoon and Volt Typhoon where there is penetration of our telecommunication infrastructure. Particularly troubling is how the Chinese are going after our critical infrastructure systems, our water, our energy, and our electrical grid infrastructure systems. We know they've penetrated them…We need a whole-of-government approach. We need to work with the interagency…and harden our infrastructure.[161]

Further underscoring the persistent challenge posed by China, former FBI Director Christopher Wray testified in 2020 that the FBI opens a new counterintelligence case related to China approximately every 10 hours.[162] Similarly, Mr. Nicholas Eftimiades, a homeland security professor at the Penn State Harrisburg School of Public Affairs, stated at a HPSCI Roundtable in June 2026:

> The FBI opens one case related to China every 12 hours. That's two cases a day times 365, [which is] 730 cases a year. I have been in counterintelligence and done investigations. Each one takes months to resolve or could take months to resolve. So [the FBI] are thousands of cases in arrears with absolutely no hope of gaining on this.[163]

The Chinese intelligence enterprise—traditional services and, most especially, non-traditional collectors—seek to penetrate and exploit many facets of our country. These efforts include cyber intrusions, talent recruitment programs, exploitation of academic partnerships, targeting of cleared personnel, and attempts to acquire dual-use technologies. China has obfuscated its illegal activity within legitimate commercial, academic, or diplomatic activity, complicating detection and response. China has also stalked and harassed dissidents across the globe, a practice known as transnational repression.

Russia also remains a major counterintelligence threat. Russian intelligence services have long relied on human intelligence, cyber operations, disinformation, and covert influence to collect sensitive information and undermine Western institutions. Like China, Russia has engaged in transnational repression schemes, stalking and harassing dissidents across the globe. The Russians, either directly or via contracted hires, have successfully assassinated many individuals perceived to pose a threat to the Russian government. Lastly, like China, Russia enlists surrogates and proxies, hires private investigators, and recruits youth and criminals online to conduct surveillance and sabotage activities.[164] Despite the war in Ukraine, the Kremlin remains determined to use all its tools in its arsenal to maintain a constant cadence of counterintelligence threats to Western interests.

Lastly, Iran has remained a persistent counterintelligence threat to our nation. Iran has built sophisticated capabilities through the Islamic Revolutionary Guard Corps (IRGC) and its clandestine paramilitary wing, the Quds Force. Both have played critical roles in sponsoring, training, and equipping various proxy groups across the globe for the Iranian regime. In addition, the IRGC and Quds Force have targeted President Trump and current and former officials as retribution for the 2020 strikes that killed former Quds Force Commander Qasem Soleimani. These lethal plots remain a threat today and have only intensified since the beginning of targeted military strikes on Iran's nuclear weapons facilities and government leadership, including former Iranian Supreme Leader Ayatollah Ali Khamenei.

Iran is uniquely able to utilize its various proxy networks to conduct military and intelligence operations on its behalf. This enables the regime to conduct global terror operations while maintaining some level of plausible deniability. Further exacerbating this threat is the fact that the Iranian regime has also used transnational criminal networks in recent years to target or kill dissidents, such as attempts to kidnap and kill Iranian American human rights activist, Masih Alinejad.[165] The threats posed by Iran will continue to grow in size and scope if an effective deterrent is not established.

Modern counterintelligence threats are persistent, dispersed, and embedded in routine interactions among governments, businesses, universities, and digital platforms. We need to rethink how we impose costs on our adversaries to drive back foreign intelligence operations that undermine our nation's security, while preserving civil liberties. Mr. Jaffer highlighted the need to recalibrate how we tackle counterintelligence challenges when he said in his testimony that "[w]e need to get on the offense, not just against terrorists, but against counterintelligence threats here in the homeland, to include but not limited to China and Russia."[166] The current counterintelligence posture must improve to address the proliferation of threats driven by hostile foreign powers.

As a society, we are at a critical crossroads in our nation's history as it pertains to counterintelligence. Our adversaries have employed imaginative ways to conduct intelligence operations within the homeland. The nation's current counterintelligence posture is eerily similar to the counterterrorism posture our nation had prior to 9/11. Our government must work to address these issues before it is too late. HPSCI Chairman Crawford has repeatedly emphasized this point and has stated in the past that "We cannot risk waiting for the counterintelligence version of September 11th to make the reforms needed to strategically disable, disrupt, and neutralize foreign intelligence entities' activities against the U.S."[167]

Asymmetric and Irregular Warfare

Asymmetric and irregular warfare have become central components for adversaries seeking to challenge the United States and exploit its vulnerabilities without engaging in direct conventional conflict. In recent years, this has come to be known as "gray zone aggression," and includes proxy warfare, covert action, disinformation, cyber operations, economic coercion, and sabotage.[168] In his written testimony before the Committee, Dr. Seth Jones, President of the Defense and Security Department at the Center for Strategic and International Studies, stated that countries may use these tactics as an effort because:

> [T]hey allow military and intelligence agencies to conduct coercive activities below a level that is likely to trigger a costly or risky conventional war. Second, irregular and gray zone activity is relatively inexpensive for perpetrators. Unlike conventional war, these activities generally do not require vast sums of money or cause the perpetrator to suffer substantial casualties. Some of these actions—such as offensive cyber and influence operations—can also be done from a state's own territory, a third country, or virtual networks that lie far from the target country. Third, these actions are often deniable and difficult to attribute. Targeted governments are frequently cautious about attributing them because they fear escalation or want to protect intelligence sources and methods. Fourth, actions below the threshold of conflict can impose costs on targeted countries.[169]

Adversaries may seek incremental gains that individually appear limited but cumulatively alter the strategic environment. The reasons outlined in Dr. Jones' testimony highlight the difficulties the IC has in confronting this particular evolving challenge. Counterintelligence offices have historically been responsible for countering such threats, but CI has remained under-resourced and focused elsewhere.

For intelligence agencies, asymmetric warfare requires a shift from event-based warning to pattern-based analysis. The challenge is not simply identifying a single attack but understanding how multiple low-level actions may serve a larger strategic campaign and adopting an anticipatory approach which lowers the bar on evidentiary proof of a foreign government's expressed plans or intentions. This requires deeper integration among military intelligence, cyber intelligence, financial intelligence, diplomatic reporting, and open-source analysis.

New and Emerging Technologies

New and emerging technologies are reshaping the post-9/11 threat landscape, presenting novel threats and challenges for today's policymakers. While terrorist organizations and hostile nation states continue to rely on traditional tools of violence, espionage, and coercion, rapid technological advancement has lowered the barriers to entry for a broader range of actors. Capabilities that once required state sponsorship, specialized training, or significant infrastructure are increasingly available through commercial markets, open-source platforms, and widely accessible digital tools. As Mr. McMaster pointed out in his written testimony, hostile states and nonstate actors are striving to weaponize those technologies against the United States and other nations.[170]

Artificial intelligence (AI) presents one of the most significant emerging challenges. Given the rapid evolution of this technology, Dr. Benjamin Buchanan, a professor at the Johns Hopkins School of Advanced International Studies, highlighted in his testimony that there is a lack of urgency amongst policymakers to address the challenges associated with AI when he stated:

> [T]he 9/11 Commission famously concluded that the attacks revealed a failure of imagination. The government's inability to take seriously a threat that did not fit existing categories and to connect information scattered across institutional seams led to devastating strategic surprise. Twenty-five years later, AI presents, in its own way, a similar kind of challenge. The technology is advancing faster than our institutions are adapting, and the most important data points come from outside government, in private companies.[171]

As the world has seen over the last few years, AI tools have enabled our adversaries to conduct their operations more efficiently and empowered them to achieve their desired goals. These actions include but are not limited to conducting sophisticated cyber operations, rapidly producing propaganda, and gathering information in a matter of minutes with little to no cost or training. Together, these capabilities highlight Dr. Buchanan's point that policymakers and the Intelligence Community must move at the speed of relevancy to stay ahead of AI-enabled threats. Beyond defending against these threats, the Committee believes the IC must also invest in adopting advanced AI capabilities of its own—so that the United States maintains its edge over its adversaries who are rapidly integrating AI into their own operations.

At the same hearing, 9/11 Commission Review Task Force Co-Chair Representative Elise Stefanik examined the growing role of artificial intelligence in enabling cyber operations by hostile actors and the steps necessary to strengthen the nation's preparedness for these emerging threats.[172] In response, Dr. Buchanan underscored that advances in AI are increasing the sophistication and effectiveness of both offensive and defensive cyber capabilities of hostile actors.[173] Dr. Buchanan also stated that this reality is one of the many reasons why our nation should make it a bipartisan priority to maintain the United States' lead in "investing and deploying AI systems and making sure we do everything in our power to deny China these capabilities."[174]

Biotechnology also presents a growing national security concern. Mr. McMaster stated in his testimony before the Committee that one of the biggest takeaways from the COVID-19 Pandemic is his belief that the virus came "from the lab at Wuhan" and that "[w]e know that our adversaries are developing these kinds of capabilities."[175] The point made by Mr. McMaster is that advances in biotechnology paired with AI offer enormous opportunities in areas ranging from agriculture to medicine, but they also introduce potential dual-use risks.[176] Knowledge and techniques that can support vaccine development, disease detection, and medical innovation may also be misused by hostile states or non-state actors seeking to develop, modify, or disseminate harmful biological agents. The expanding availability of biological data, laboratory automation, and commercial research tools increases the importance of strong oversight, privacy protections, early-warning systems, and coordination between the Intelligence Community, public health agencies, law enforcement, academia, and the private sector.

Other emerging technologies further complicate the threat landscape. The proliferation of drones, publicly and commercially available information, and encrypted communications gives adversaries new ways to surveil targets, evade detection, disrupt critical infrastructure, and challenge U.S. technological advantages. As these capabilities become cheaper and more widely available, the line between state and non-state actors, and the capabilities they possess, will continue to blur, requiring policymakers to modernize legal authorities, increase technical expertise, and improve interagency coordination to keep pace with rapidly evolving threats. Lastly, the U.S. must take a leadership role in how these technologies are developed and deployed. 9/11 Commission Review Task Force Co-Chair Representative Josh Gottheimer rightly emphasized this at a HPSCI Committee hearing by stating that "America, not Beijing, sets the rules for this critical technology."[177]

Foreign Terrorist Organizations

Many recommendations from the original 9/11 Commission Report have led to reforms that have helped U.S. counterterrorism operations degrade leadership structures of al Qaeda and the Islamic State (ISIS), reduce their ability to hold territory, and disrupt many external operations networks. Although significant progress has been made, foreign terrorist organizations remain an enduring threat, and their structure, capabilities, and operational methods have changed significantly since 9/11. These groups have adapted by decentralizing, relying on regional affiliates, encrypted communications, and online propaganda that drives self-radicalized attackers.

ISIS, al Qaeda, and their affiliates continue to exploit instability in regions such as the Middle East, Africa, and South Asia. These organizations have developed more disparate franchises and increasingly encouraged affiliated groups and inspired individuals in the West and beyond to conduct attacks using easily accessible resources. This decentralized model complicates intelligence collection efforts and reduces the effectiveness of strategies targeting leadership and financial networks.

Within our own hemisphere, cartels operating in Central and South America threaten our national security and law enforcement interests. Foreign adversaries and their agents employ cartels to launder illicit funds, traffic ill-intentioned individuals across our borders, and smuggle weapons into the homeland. While there are arguments for and against categorizing cartels as foreign terrorist organizations, it is undeniable that such organizations are purveyors of destruction: they undermine democracy in Central and South America, creating instability; are willing partners of U.S. adversaries and opponents of a thriving, healthy West; and facilitate death and despair that cross national boundaries. By adopting new tactics, techniques, and procedures, cartels present a pernicious threat for our intelligence and law enforcement communities to address.

This evolution demonstrates both progress and limitations in post-9/11 reforms. Our nation's Intelligence Community has become far better at identifying foreign terrorist networks and disrupting large-scale plots, but the threat has shifted toward smaller, less detectable operations. The IC has been forced to adapt its focus to monitoring regional affiliates and proxies, online recruitment pipelines, and economic and political instability that creates the environment for terrorist groups to regenerate.

Homegrown Violent Extremists

Homegrown violent extremists (HVEs) present one of the more difficult challenges in the post-9/11 era. Unlike foreign terrorist operatives, who may travel internationally, communicate with overseas handlers, or rely on identifiable networks, HVEs are most likely to radicalize largely within the United States, typically in isolation, acting with little or no direct organizational support from foreign terrorist organizations, which creates challenges when using traditional intelligence collection methods.

Over the last decade, self-radicalization has increasingly occurred through online communities, social media platforms, encrypted messaging applications, and algorithm-driven content networks. Oftentimes, disenfranchised individuals consume extensive amounts of extremist material, develop grievances, and commit violence without ever formally joining an organization.

The ideological, philosophical, and motivational influences driving homegrown violent extremism are broad. They include jihadist-inspired extremism, nihilistic violent extremism, extreme anti-religious violence, racially or ethnically motivated violent extremism, anti-government extremism, and other forms of grievance-based violence. Some acts of terrorism stem from delusions of heroic grandeur. Recent examples include the politically motivated assassination attempts on President Donald Trump; the assassinations of political activist Charlie Kirk, Minnesota state lawmaker Melissa Hortman, and United Healthcare CEO Brian Thompson; and the attack on Pennsylvania Governor Josh Shapiro. There have been other deadly attacks perpetrated against religious institutions. In addition, antisemitic attacks have risen sharply after the October 7th attacks in Israel. Many of these attacks were perpetrated by homegrown violent extremists who were self-radicalized by content denigrating the Jewish community.

These threats challenge the framework established after 9/11 because many intelligence reforms were designed to identify connections among foreign actors, travel patterns, communications, and networks. Homegrown violent extremists often do not exhibit those indicators, and their attacks may involve lawful activity, such as acquiring firearms, vehicles, knives, or licit material to build improvised explosive devices; require minimal planning; and leave little to no warning. As a result, prevention depends heavily on cooperation among federal agencies and state and local law enforcement, community reporting, and behavioral threat assessments, all while Americans' civil liberties are protected.

This form of terrorism places a heavy burden on local authorities and communities to harden their defenses. As seen in the recent attack on the synagogue in West Bloomfield Township, Michigan, many "soft targets" have begun hiring armed security guards to neutralize potential attackers.[178]

Drones and Unmanned Systems

Since World War II, air superiority has been a critical factor in assessing which side has the greater capacity to win a war. The father of the United States Air Force, Army General William "Billy" Mitchell, stated, "Great contests for control of the air will be the rule in the future. Once supremacy of the air has been established, airplanes can fly over a hostile country at will."[179] Historically, no nation has been able to compete with the United States' ability to establish control and command of the skies during conflict and maintain air superiority. However, drones and other unmanned systems are quickly challenging our ability to maintain domestic air control. The proliferation of these systems represents a major technological shift in the threat environment. Commercially available drones can be used for surveillance, targeting, smuggling, disruption of public events, attacks on critical infrastructure, or delivery of explosives. Capabilities once limited to advanced militaries are now available to all states and interested non-state actors at relatively low cost.

As observed in nearly every conflict since the counter-ISIS campaign, readily available and relatively cheap drones have transformed the battlefield by enabling persistent surveillance, precision strikes, and low-cost attacks against more expensive platforms. Non-state actors have used drones for reconnaissance and improvised attacks, while state actors are developing more advanced unmanned systems, including autonomous platforms and drone swarms. Swarming technology presents a significant concern due to the large numbers of small drones that could overwhelm existing air defense systems or create confusion in crowded airspace.

Drones create difficult detection and response problems within the homeland. They can fly at low altitudes, operate near airports or sensitive facilities, and be modified for malicious purposes. Yet because drones also have legitimate commercial, recreational, and public safety uses, regulation must balance security needs with innovation and lawful activity. From an intelligence perspective, drones and unmanned systems illustrate how emerging technologies can rapidly create new vulnerabilities before government institutions have fully adapted.

Cyberattacks

Cyberattacks have become one of the defining threats of the present-day national security environment and are likely to accelerate given advances in AI-enabled capabilities. State actors, criminal groups, and hybrid actors now routinely target U.S. government systems across all levels of government, water and power infrastructure, financial institutions, healthcare networks, defense contractors, and other private companies. Cyberattacks can produce effects from data theft to physical disruption. Ransomware incidents can interrupt hospitals, schools, pipelines, and municipal services. Supply-chain compromises can infiltrate software used across government and industry. Cyber-enabled espionage can extract sensitive defense, commercial, and personal data on an enormous scale.

Cyber threats blur the line between intelligence collection and warfare. Cyber operations allow state and non-state adversaries to lay dormant for months, and in some cases years, before remotely conducting espionage, disruptions, acts of sabotage, theft, and influence campaigns. A cyber intrusion may also begin as espionage but create access that could later be used for disruption or destruction during a crisis. This ambiguity complicates deterrence, attribution, and response. The Intelligence Community must therefore integrate technical cyber indicators with geopolitical analysis, private-sector reporting, and law enforcement investigations to anticipate, disrupt, deter, and mitigate cyber-attacks.

The PRC's cyber threat actors Salt Typhoon and Volt Typhoon conducted dangerous technical penetrations of our critical infrastructure and went undetected for years by the government.[180] These cyber-attacks—constituting potential pre-positioning by the PRC—could lead to catastrophic effects.

Similarly, the Solar Winds hack by Russian intelligence went undetected for a year and led to significant disruptions. The Russians are also known to enlist politically motivated individuals known as "hacktivists" to conduct hacking operations and ransomware attacks, which can have major destabilizing effects on sectors they target.[181]

Foreign Malign Influence

Foreign malign influence is a form of cognitive warfare that has become a major tool for both state and non-state actors in today's threat environment, targeting the political, social, and informational foundations of Western societies. Representative Stefanik warned at the Committee's July 21, 2026 hearing that U.S. adversaries are working to "inject divisive and destructive topics into public discourse" including through influence campaigns on college campuses, online, and in the media.[182] Dr. Jones agreed, specifically describing the threats posed by China as "pervasive inside of the United States" and pointing to PRC efforts ranging from technology theft and cyber operations to pressure on American companies and influence activities conducted by the United Front Work Department.[183] 9/11 Commission Review Task Force Co-Chair Representative Gottheimer followed-up on that exchange in the same hearing and highlighted how this issue is not exclusive to just China and is exacerbated by advancements in AI when he said:

> Since 2023, Iran, China, and Russia have run covert operations to divide our country. We know that. Funding of crime groups, flooding of social media, and targeting our college campuses, especially with anti-American and decisive rhetoric. AI super charges all of it. A single adversary can now generate fake voices and fake videos and millions of fake messages.[184]

State actors such as China, Russia, and Iran use influence operations to shape public opinion, exploit social divisions, weaken trust in democratic institutions, and manipulate policy debates in ways favorable to their strategic interests. China utilizes social media networks, most notably ByteDance's TikTok, to conduct influence campaigns on a variety of topics designed to sow division and create distrust throughout the West.[185] Russia has utilized Telegram and bots to accomplish similar objectives.[186] According to public reporting,[187] both China and Russia may now be conducting malign influence efforts to exploit and exacerbate preexisting and legitimate debates within the United States about building new AI data centers. These foreign malign influence campaigns seek to exploit legitimate concerns about the costs and shortcomings of expanding AI data centers, widen differences in public discourse, and ultimately foil efforts to reach sensible compromises that preserve America's AI edge over China.

These types of operations are also not limited to state-actors. After the October 7th attacks perpetrated by Hamas, the online platforms were flooded with doctored videos and misinformation related to the ensuing conflict in Gaza by non-state actors, such as Hamas, Hezbollah, and other terror networks, looking to exploit the conflict to shape public debate, fundraise, and exert international political pressure on Israel. Similar efforts have had success shaping public opinion about the United States and the Western world more broadly.

During a Committee hearing, Dr. Jones highlighted how foreign influence campaigns often combine overt propaganda, covert media manipulation, cyber-enabled information operations, state-controlled media, fake social media accounts, proxy organizations, and selective amplification of divisive narratives.[188] The objective is not always to persuade audiences of a specific false narrative. Often, the goal is simply to create confusion, demoralize the public, intensify polarization, and reduce confidence in the U.S. government.

Foreign malign influence operations differ from other aspects of espionage and statecraft because they often take place in the open information environment. These operations often blend covert manipulation with lawful speech, making response especially difficult in a constitutional democracy. Social media amplifies this threat exponentially by allowing adversaries to target specific audiences, rapidly spread disinformation, and exploit existing grievances. Frank Cilluffo, Director of the McCrary Institute for Cyber and Critical Infrastructure at Auburn University, highlighted at a HPSCI hearing that AI and other synthetic media will likely increase the scale and sophistication of these operations.[189]

The threats posed by foreign malign influence are especially relevant to a review of post-9/11 intelligence reform because they demonstrate how the intelligence problem has moved beyond detecting discrete plots. Influence campaigns are continuous, adaptive, and sometimes difficult to trace. These attacks may accompany cyber intrusions, economic coercion, election interference, or diplomatic pressure. Countering them requires cooperation among intelligence agencies, law enforcement agencies at every level, and the public. In confronting these threats, the Intelligence Community must be cognizant of protecting First Amendment rights.

Economic Warfare and Espionage

Countering economic warfare and espionage has become an increasingly important dimension of national security. Definitions of economic warfare and economic espionage can vary widely depending on the context. For the purposes of this report, "economic warfare" is defined as "a nation-state's ability to use economic tools to weaken an adversary's ability to generate and use power." This report defines "economic espionage" as "a nation-state's ability to steal sensitive economic, commercial, or technological information to advance the aggressor's interests or strategic goals." Clearly defining these terms is important given rising tensions between the United States and its adversaries.

Adversaries, mainly China, use economic tools to gain leverage, weaken U.S. competitiveness, shape political choices, and reduce the resilience of American institutions. These tools may include coercive trade practices, sanctions evasion, strategic investment, supply-chain manipulation, debt diplomacy, currency manipulation, and cyber-enabled theft. Dr. Jones stated in his written testimony that "China is increasingly engaged in the threat or imposition of economic costs and inducements to influence decision-making and popular support across the globe to gain a competitive advantage."[190]

Economic espionage has proven to be a significant challenge for the U.S. to overcome. These hostile actions are especially significant because they target the foundation of U.S. technological and industrial power. Sensitive sectors such as defense, biotechnology, energy, AI, quantum computing, and semiconductors are attractive targets for foreign intelligence services. The FBI has warned that "economic espionage costs the American economy hundreds of billions of dollars per year."[191]

These types of threats show how national security and economic security have become deeply interconnected. During the immediate post-9/11 period, intelligence reform focused on preventing terrorist attacks and improving information sharing among federal agencies. Today, intelligence agencies must also help identify vulnerabilities in supply chains, foreign investment, research partnerships, and critical industries. The private sector is therefore no longer merely a stakeholder in security; it is often the primary target.

Intellectual property theft is a major subset of economic espionage and a central concern in strategic competition. Foreign actors seek trade secrets, proprietary technologies, research data, source code, defense designs, pharmaceutical research, and advanced manufacturing techniques. Theft can occur through cyber intrusions, insider threats, joint ventures, front companies, academic collaborations, and forced technology transfer. The FBI also assesses that China accounts for roughly $225-$600 billion in intellectual property theft annually.[192]

The damage caused by intellectual property theft is both economic and strategic. Economically, it deprives U.S. companies and researchers of the benefits of innovation. Strategically, it allows adversaries to accelerate military modernization, strengthen their own domestic industries, and reduce dependence on Western technology. In his testimony, Mr. McMaster discussed how the U.S. did not take the steps necessary to protect its economy after China integrated into the global market. Specifically, he stated:

> And, at the same time, we are opening our economy to them, and we are being infiltrated by PLA scientists and others who are there to extract intellectual property, to extract know-how, apply it to gain commercial advantage but, importantly, to gain military advantage.[193]

Economic warfare and espionage present difficult challenges because many of the threat indicators exist outside classified government systems. Universities, start-ups, laboratories, contractors, and multinational firms often hold the most valuable research. Protecting intellectual property therefore requires stronger coordination among intelligence agencies, law enforcement, and the private and public sectors. Combatting this challenge also requires avoiding overly broad measures that could damage legitimate scientific collaboration or economic growth.

Lessons Learned and Implications for Post-9/11 Intelligence Reform

The hybrid threat landscape shows that the post-9/11 intelligence challenge has expanded beyond traditional counterterrorism coordination to detecting and mitigating threats across multiple domains. While the 9/11 Commission's core lesson—improving information sharing, synthesis, and anticipation—remains relevant, today's threat landscape is broader and more complex.

The threats highlighted throughout this section often overlap, as adversaries combine cyber operations, influence campaigns, economic pressure, and military posturing into coordinated strategies. Although post-9/11 reforms improved coordination and established enhanced information-sharing frameworks, primarily in the counterterrorism space, intelligence agencies must continue adapting by strengthening public-private partnerships, expanding open-source and technical capabilities, and improving analysis of both immediate plots and long-term strategic risks. Modern intelligence must be integrated, adaptive, and capable of detecting threats across multiple domains while continuing to safeguard Americans' civil liberties.

Furthermore, the IC must adapt to include more cross-jurisdictional collaboration and foster an environment in which its various elements bring their expertise to a joint fight. These current threats call for the same degree of reform and integration as was necessary after 9/11.

Vulnerabilities Exposed in Today's Threat Environment

Breaking Silos: From an Agency-Centric Mindset to Mission-Centric Intelligence Culture

While every agency within the IC has unique authorities, capabilities, and expertise, the dangers facing our nation are complex and often exceed a single agency's ability to detect, understand, and address the threat. Threat streams, such as computer network attacks and espionage campaigns, foreign malign influence campaigns, economic espionage, and counterintelligence efforts require agencies to collaborate so policymakers receive a holistic understanding of an issue and possible solutions. Post-9/11 reforms improved some of these efforts toward coordination and information sharing.

Despite the progress over the course of the last twenty-five years, most elements within the IC still operate within agency-centric cultures rather than as part, or in support, of interagency mission-specific teams. This agency-centric culture that exists within some elements of the IC and law enforcement components may create stovepipes leading to intelligence failures that allow the next catastrophic attack on the United States. The IC must reform its existing architecture and support interagency collaboration as a matter of course.

Adopting a joint force mindset will require the IC to do more than routine coordination or information sharing. ODNI must incentivize agencies to combine resources on overlapping mission sets and improve how agencies communicate with one another. In addition, ODNI should evaluate effectiveness by mission success as opposed to which agency can claim credit. To be successful, the IC components must accord appropriate weight and respect to the DNI's leadership and role as integrator of the IC. Lastly, analysts, collectors, and operators should be encouraged and proficient at working across the various agencies. These steps will help reduce bureaucratical barriers that prevent collaboration and integrate intelligence disciplines.

This cultural shift is paramount in the current era. Our nation's adversaries are leveraging whole-of-society approaches using every tool at their disposal to advance their strategic objectives. The IC, and more importantly our country, cannot afford fragmented approaches that create gaps between agencies, limit full-scope detection and analysis, or create delays in recognizing threat indicators. By promoting a mission-first mindset, this cultural change would help the IC better detect emerging threats, reduce duplicative missions, and provide more actionable intelligence to policymakers. The IC's success is dependent on the willingness to promote interagency coordination that crosses traditional agency boundaries.

Strengthening ODNI as the IC's Strategic Integrator

To create a more unified, interagency mindset, ODNI must be empowered as the IC's chief strategic integrator. ODNI was created to address the fragmentation, information-sharing failures, and agency stovepipes that limited the government's ability to identify and disrupt threats prior to 9/11. As mentioned in the previous section, elements within the IC still often operate within an agency-centric structure. The DNI's role must be strengthened to ensure that the IC can align collection, analysis, operations, and resources to match the highest priority

threats our nation faces while bringing to bear integrated authorities. Congress must examine the DNI's role and the current architecture of the IC, and provide legislative solutions designed to help build an IC that is more agile, accountable, and prepared for the complex threat environment unfolding before us.

A significant step that can be taken to achieve this goal is to give ODNI greater budget authority across the IC. Without meaningful control over budget decisions, the DNI remains limited in what it can achieve in terms of driving integration, reducing duplicative actions, and enforcing community-wide priorities and standards. Full budget authority would allow the DNI—at the direction of the President of the United States—to better align resource allocations with national intelligence priorities, incentivize the IC to be force multipliers within a joint structure, and ensure that agencies are not protecting legacy programs or institutional status quos. In addition, stronger budget authorities would also help the DNI identify current gaps, shift resources to new and emerging threats, and hold the IC elements accountable for contributing to shared mission outcomes.

Congress should examine expanding the use of interagency mission centers and task forces focused on specific threat streams or national security challenges. These centers can help organize the IC around problem sets as opposed to focusing on individual agencies. This shift would help bring together analysts, collectors, operators, technologists, and policy support elements from across the IC. The structures would focus on issues that reflect the National Intelligence Policy Framework (NIPF) and ensure the proper expertise and capabilities are integrated at the front end of the mission, not after agencies have already established separate approaches to a problem set.

Most importantly, these models would facilitate a joint mindset throughout the IC to tackle our nation's most pressing national security challenges. Throughout the DOD, the joint warfare culture is not a mechanism to coordinate among the services; it is a mindset that places overall mission success above institutional preference. It is important to note that many in the military resisted the shift to joint models, requiring Congressional action through the implementation of the Goldwater-Nichols Act of 1986.

To combat the rising threats posed by great power competition, the IC should adopt an operational approach like the DOD's use of functional and regional combatant commands. Mission centers paired with stronger budget authority for ODNI would greatly incentivize agencies to contribute their best capabilities and brightest talents to the shared objectives, construct cross-agency teams, and develop leaders that have the skills and knowledge to comfortably operate across institutional boundaries. These centers should provide agencies with specific collection requirements, set analytic priorities, manage intelligence activities based on the NIPF, and hold agencies accountable for achieving milestones within those goals.

Ultimately, reforms to strengthen ODNI should avoid adding bureaucracy. Instead, reforms should be targeted towards ensuring that the IC can act as a unified enterprise directed against strategic threats that do not align neatly with specific agency and department lines but rather operate within jurisdictional and authorities' seams, giving an advantage to our adversaries.

Ever Increasing Need for Analytic Expertise

As the world becomes more complicated, it is that much more important that the Intelligence Community be comprised of deeply serious, knowledgeable civil servants committed to objective, rigorous analysis.

Throughout its report, the Commission highlighted the importance of subject matter expertise, acknowledging that it was both a valuable and not easily replaceable commodity. During the Cold War, the Report detailed, "[A]nalysts could safely invest time and resources in basic research, detailed and reflective…they could draw on a deep base of knowledge."[194] Conversely, there was insufficient familiarity with Islamist terrorism before September 11th. That which did exist was finite, as the report warned: "The limited pool of critical experts—for example, skilled counterterrorism analysts and linguists—is being depleted. Expanding these capabilities will require not just money, but time."[195]

Today, in addition to still needing that counterterrorism expertise, the IC also requires deep understanding of Russia and China, proficiency in emerging technologies, and familiarity with rapidly proliferating modern weapons systems, while not turning its back on potential future hot spots all around the globe.

Beyond *what* intelligence analysts know, the Report offered suggestions for *how* they could improve their craft. It was "crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination."[196] This included conducting red-team analysis, developing sets of indicators and warnings for potential attacks, and otherwise considering previously unseen threats. Such exercises also needed to be combined with rigorous analysis and context.

The Report highlighted the importance of intelligence analysts sticking to their conclusions, especially when they were not necessarily supportive of policy.[197] The Commission was concerned with political chilling effects on analysts; for instance, it detailed:

> [A]fter the Cole attack and for the remainder of the Clinton administration, analysts stopped distributing written reports about who was responsible. The topic was obviously sensitive...CIA analysts in Washington presumed that the government did not want reports circulating around the agencies that might become public, impeding law enforcement actions or backing the President into a corner.[198]

Political pressure on intelligence assessments is a longstanding problem, echoed in CIA's comments on its failure to predict the 1979 Iranian revolution[199] and former CIA and NSA Director retired Air Force General Michael Hayden's reflections on administrative incentives to link Saddam Hussein's regime with al Qaeda.[200] We must continue to guard against groupthink, bias, or political pressure in the analytic process.

Adopting a "Whole of Society" Approach to Strategic Competition

As previously stated in this report, China employs a "whole-of-government" approach to advance its national strategic objectives. The CCP uses every instrument of national power—

including military, economic, diplomatic, technological, and societal tools—to challenge the existing international order and try to establish China as the world's leading power. These efforts have enabled China to expand its influence around the globe and bend the rules-based international order to benefit its national interests, ultimately diminishing the ability of democratic institutions to thrive. In an exchange with Rep. Scott Perry at a Committee hearing, Dr. Jones highlighted how China deploys every tool that is available to advance its strategic advantage when he discussed various ways China uses this approach:

> There are far too many [examples] to go through in detail for this testimony unless we added another four hours, but they range from everything from influence operations, most recently, the influence operations inside the United States about AI data centers, to discourage the building of AI centers across the United States. We've seen the Chinese Communist Party involved in activity in cities in the United States to pressure, in some cases to try to seize individuals from China that are conducting actions on social media platforms that the Chinese Communist Party does not like. There's espionage on university campuses. There's offensive cyber operations, the Volt Typhoons and the Salt Typhoons that we've talked about. Those are just examples. Those are just a couple of examples.[201]

This is not an abstract threat; it has reached our shores. The CCP has weaponized the openness of American society and exploited vulnerabilities and loopholes within the U.S. legal and economic systems to establish influence across various sectors. For far too long, the United States and its Western allies neglected this reality. In turn, the U.S. would be remiss if it did not attempt to adopt a "whole-of-society" approach to counter this present—and growing—threat, including leveraging every appropriate tool at the federal government's disposal.

The private sector must also play an active role by developing a collaborative relationship with the government. Concurrently, the government must provide timely and actionable intelligence to help the private sector address these challenges, while federal agencies must make themselves accessible and responsive to industry stakeholders.[1] For instance, the Cybersecurity and Infrastructure Security Agency (CISA), a critical component of the Department of Homeland Security, was established in part to "provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators."[202] Mr. McMaster suggested at a Committee hearing that the government, with support from the IC, should "identify the most critical technologies and intelligence prospects, establish security standards, and mobilize public and private efforts to protect them from espionage."[203]

[1] Through Chairman Crawford's "SCALE UP" initiative, HPSCI convenes federal, congressional, local, and industry leaders for classified briefings and broader unclassified discussions that strengthen government-industry coordination. These engagements seek to build the bottom-up cooperation and whole-of-society commitment necessary to address national security challenges.

Unlike China, our republican form of government requires buy-in from the ground up—not dictated on high from a central planning committee. The government must take the necessary actions to foster the whole-of-society cultural change the country must embrace.

The Public-Private Partnership Gap

Private industry, rather than the IC, is leading the development of paradigm-shifting technologies—including artificial intelligence, quantum computing, and drones—and private-public cooperation is paramount to our nation's success in maintaining our strategic advantage. Arguably one of the most pressing challenges in dealing with new and emerging technologies is building and maintaining partnerships that balance national security interests with the commercial interests of U.S. technology companies. Furthermore, the technology industry has been particularly susceptible to counterintelligence risks due to the companies' collaborative nature and the fact that many of them lack the sophisticated vetting processes needed to detect foreign intelligence or foreign actors looking to circumvent export controls.

The nature of these technologies presents an unprecedented regulatory challenge. The same technology that serves entirely benign civilian purposes can, with minimal or no modification, become an instrument capable of great harm. Because the gap between benign and nefarious applications is small or nonexistent, national security interests will frequently and unavoidably conflict with commercial ones. Balancing these competing interests is challenging. Mr. Jaffer described the challenge at an HPSCI hearing on May 20, 2026:

> If we were to let the technology community in the door and we were to partner tightly with them, and by the way, expect more of them – all too often we see technology companies say, we're global companies when it comes time to work with the U.S. Government. When it comes time for them to take advantage of the U.S. Government and benefit from our technology, our national security capabilities, or threats they're facing, oh, now they're an American company.[204]

This inconsistency is untenable. The United States must pursue stronger partnerships with U.S. technology companies to ensure corporate interests do not undermine national security endeavors.

As Mr. McMaster recommended, the IC should "develop private sector partnerships where declassified information can be shared with relevant stakeholders, particularly technology firms directly targeted by Chinese economic aggression. The Intelligence Community should simultaneously be learning from their private sector partners about Chinese tactics and emerging vulnerabilities."[205]

Open-Source Intelligence: New Threats and New Opportunities

The IC must significantly improve its use of Open-Source Intelligence (OSINT), intelligence derived exclusively from commercially or publicly available information that addresses specific intelligence priorities, requirements, or gaps. OSINT helps drive other intelligence disciplines and delivers unique intelligence value on its own. As the open-source environment continues to expand and evolve, and as private-sector industries that are developing dual-use technologies—such as artificial intelligence and quantum computing—continue to grow, open-source data will become increasingly important. In fact, OSINT is so instrumental to the IC's success that 20 percent of the President's Daily Brief is derived from OSINT reports.[206]

Despite OSINT being more widely incorporated, vast quantities of publicly and commercially available information remain underused. This disparity represents a significant and largely low-cost intelligence gap that adversaries are already exploiting. Historically, OSINT has been treated as a secondary intelligence discipline, one that has not always received the same respect or distinction as more traditional disciplines such as human intelligence, signals intelligence, and geospatial intelligence. This mindset, which has often prioritized exquisite collection methods, could cost the IC a tremendous amount of money.

Dr. Hoffman illustrated the value of OSINT and how adversaries are exploiting this information at a HPSCI hearing on May 20, 2026:

> [A]nyone in the public eye now, for $0.99, individuals can get all their personal details, their home address, Social Security numbers, cell phone numbers, and so on, which facilitates the attacks on persons or threats and harassment being directed against them.[207]

Even more troubling, nonstate actors are increasingly using OSINT to conduct operational planning and gather information on targets. Terrorist attacks, such as the 2025 New Year's Day vehicular attack in New Orleans, illustrate the grave dangers posed by the availability of cheap and open-source materials, which allow relatively weak terrorist group franchises to amplify their operational capacity. Dr. Hoffman further explained at the May 20, 2026 HPSCI hearing:

> Clearly, all kinds of technology, from things like the New Orleans vehicular attack using Google Glasses to carry out surveillance, for example, and record surreptitiously.[2] So, he wasn't holding up his iPhone or holding up a camera. He just had eyeglasses that he could use. Certainly, the power that artificial intelligence, but just the availability of open-source material to carry out intelligence and reconnaissance in a detailed fashion from one's desktop, is enhanced appreciably.[208]

[2] Although the witness's testimony described the technology of the New Orleans terrorist as "Google Glasses," the terrorist used Meta glasses to carry out his attack on Bourbon Street.

The capabilities of foreign powers, terrorist groups and their sympathizers, and lone wolfs are greatly enhanced by open-source data, hardware, and services. Consider as an example a foreign intelligence agency looking up who publicly discloses that they hold a security clearance on their social media or business websites to support targeting. The United States can help close this gap by better utilizing OSINT and elevating it as a core intelligence discipline.

Closing the Gaps in Information Sharing

While interagency information sharing has improved meaningfully since the failures exposed by the September 11th attacks, critical gaps remain, particularly between the federal government and state and local partners. The architecture of our national security enterprise must continue to evolve to create genuine "connective tissue" between non-IC agencies and the broader homeland security community.

Threats that emerged in the post-9/11 world often require specialized expertise that remains siloed because of clearance barriers and uneven access to classified information. Agencies with relevant knowledge and expertise must be empowered to share it, and, where appropriate, more of those agencies should be brought into the fold of classified information sharing. Expanding the cleared workforce in a deliberate, vetted manner would reduce bottlenecks in information flow and improve the government's collective ability to identify, assess, and respond to threats.

Foreign partners and allies also play a critical role in providing valuable insights and intelligence. Mr. Cilluffo testified in a July 21, 2026 HPSCI hearing:

> One of America's greatest strategic advantages is its network of trusted partners, particularly the Five Eyes and our closest NATO and bilateral allies. Our adversaries often seek to exploit seams between countries, agencies, sectors, and authorities. We should respond by deepening the trusted relationships that permit earlier warning, shared situational awareness, coordinated action, and collective resilience.[209]

The overclassification of information has emerged as a potential obstacle in ensuring timely and actionable intelligence on various threat streams reaches state and local law enforcement and stakeholders.

Furthermore, in some cases, jurisdictional battles between various agencies have led these agencies to create alternative controls and compartments that mitigate who has insight into the information they are collecting. This practice continues to cause information gaps across the IC and has prevented progress on combatting certain threat streams. This form of gatekeeping and territorial culture was a key issue that the original 9/11 Commission Report sought to eliminate. The fact that these issues associated with information sharing are still apparent after twenty-five years should set off major alarms for the American people. In addition, leaks of classified information and the lack of accountability for those who disclose classified information have contributed greatly to creating information barriers by incentivizing restrictions.

There are multiple ways to address issues associated with information sharing, such as better coordination and integration with state and local fusion centers; using OSINT on threat streams to disseminate information to the public; creating greater accountability measures, including tougher criminal penalties, for unlawful disclosures; or conducting an IC-wide assessment on the criteria needed to classify information at certain levels.

Reauthorizing and Reforming the Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act's (FISA) Section 702 enables the U.S. government—through the compelled cooperation of U.S. electronic communication service providers—to collect emails, text messages, and other electronic communications of foreign nationals, who are located overseas, and who are reasonably believed to possess certain types of foreign intelligence information, including terrorism-related information.

Congress established the FISA Section 702 program in 2008 and reauthorized it in 2012, 2018, and in 2024 with the Reforming Intelligence and Securing America Act. Each reauthorization has contained a sunset provision, requiring Congress to periodically debate whether to renew the program and what reforms to make. The most recent law renewed the program for only two years, until April 2026; at the time of this writing, the statutory authorization for the 702 program has expired, though the Foreign Intelligence Surveillance Court has recertified the program through mid-March 2027.

Given that over 60 percent of the articles in the President's Daily Brief are derived at least partly from intelligence acquired under Section 702,[210] it is essential Congress reauthorize Section 702, while making all necessary reforms to give the American people comfort that this powerful surveillance tool is not being used for illegal or improper purposes. In the past, compliance failures by FBI have raised bipartisan concerns in Congress, and the recent reauthorization act made numerous reforms designed to prevent such compliance failures and to ensure appropriate accountability for employees who do not follow the program's strict rules.

COMMITTEE RECOMMENDATIONS

In the course of evaluating the implementation and efficacy of the 9/11 Commission's recommendations, the Committee developed recommendations of its own born out of the reforms that have and have not been fully implemented since 2001. The overriding principles of these recommendations are that the modern threat environment requires whole-of-government cooperation, strong congressional oversight, and a well-equipped Intelligence Community that is both effective and accountable. As threats and challenges to U.S. national security have evolved since 2001, the IC has evolved as well, but there are indisputably areas that can be improved, both to confront current threats and to anticipate and address new ones. The recommendations below are offered in that spirit, highlighting areas of improvement drawing from the oversight activities of the Committee.

Perhaps the most important principle guiding these recommendations is the shared belief by all HPSCI Members that safeguarding the privacy and civil liberties of Americans is imperative.

The United States need not—and must not—replicate the surveillance architectures employed by totalitarian and authoritarian regimes. Nor should the IC measure its effectiveness by its ability to imitate the coercive systems or practices of America's adversaries. Such systems are anathema to the character of our nation, its constitutional traditions, and its commitment to protecting the rights and liberties of its citizens.

Accordingly, any recommendation in this report intended to reduce unnecessary barriers between intelligence collection and law enforcement must be accompanied by rigorous oversight, appropriate safeguards, and a heightened sensitivity to the privacy, rights, and civil liberties of Americans.

Recommendations

1. ***Establish Mission-centered and Task Force-based Intelligence Integration as an IC-Wide Standard –***

   In the years following 9/11, joint interagency task forces and mission centers have become the gold standard in combatting terrorism. The Committee recommends applying best practices from these models to additional mission sets across the IC. Specifically, the Committee recommends that ODNI identify additional new mechanisms and establish a formal IC-wide standard requiring agencies to organize key intelligence activities around mission sets rather than agency ownership. These standards and mechanisms should prioritize integrated teams, shared responsibility, and mission outcomes over institutional credit. ODNI should review any policies, classification practices, and internal procedures that unnecessarily limit collaboration across agencies.

2. ***Professionalize Open-Source Intelligence Collection and Analysis –***

The Committee believes that open-source intelligence (OSINT) is underutilized and underfunded across the IC, and while OSINT utilization has improved, progress has been uneven and slow. The Committee therefore recommends that the DNI continue taking steps to formally recognize OSINT as a primary intelligence discipline.

Specifically, the Committee recommends the DNI create a line item for OSINT activities in each agency's budget, update IC policy to include OSINT, establish training standards, and create a formalized job code for OSINT practitioners. The Committee also recommends greater integration of commercially offered technological solutions to leverage OSINT data for insight and improved integration with classified tools. The Committee believes these steps will help change the IC's culture to recognize OSINT as the "-int of first resort."

3. ***Fully Implement Biometric Entry-Exit System –***

The United States should complete its implementation of a biometric entry-exit system for foreign nationals traveling in and out of the country. Similar to the Schengen Area in Europe, foreign nationals traveling to the United States should pass control booths at points of entry at admission and departure, enabling the U.S. to track who is in the country, for how long, why, and when they leave. Technological advancements make collecting biometric data at points of entry relatively quick and easy. As much as practically possible, U.S. borders should be secured to ensure foreign nationals seeking land exits to pass through land points of entry so CBP can collect biometrics and build profiles.

4. ***Build Interoperable Information-Sharing Systems Across the IC*** –

The Committee recommends that the IC should prioritize interoperable technology platforms that integrate artificial intelligence capabilities from trusted vendors that enable agencies to share relevant intelligence, data, and threat indicators in real time. These systems should be designed to reduce unnecessary barriers between agencies while preserving appropriate security controls.

The IC should also pursue technological developments in expanding information-sharing systems with key partners and allies. This will be critical in any efforts to expose or operate against our adversaries in a coordinated and sustained manner.[211]

5. ***Measure Success by Mission Outcomes, Not Agency Ownership –***

The Committee recommends the IC update performance metrics standards to reward collaboration, joint production, and successful mission outcomes. Agencies and personnel should be evaluated based on their contributions to shared national security objectives rather than whether a single agency can claim primary ownership of success. This includes cooperating on multi-agency assessments, contributing to communities of interest, undertaking joint duty assignments, or volunteering for various crisis or other multiagency rotations. Likewise, seniors should be rewarded for supporting maximum participation in cross-agency efforts among their employees.

6. ***Develop and Expand Joint Training and Career Incentives Across the IC –***

The Committee recommends that the IC expand joint training opportunities that expose analysts, collectors, and operators to other intelligence disciplines and agencies. Evaluations of IC officer performance should incorporate preferences for service in cross-agency assignments, mission centers, and integrated task forces.

7. ***Formally Establish Counterintelligence as a Career –***

There is currently no standardized career path established within the federal government that pertains to counterintelligence. The current architecture has created a patchwork of job series that is used to cover federal employees conducting counterintelligence functions. The Committee recommends the Office of Personnel Management establish a counterintelligence career field within the federal government.

In doing so, the IC will foster the necessary expertise needed to confront the evolving threats that we face today and in the future.

8. ***Review Current Classification Processes –***

Classification creates barriers to working across agencies, particularly sharing with state, local, tribal, and territorial law enforcement partners. The Committee recognizes the need to protect sources and methods, but judges that overclassification remains a durable problem within the IC. Therefore, the Committee recommends that ODNI look closely at current processes and procedures to determine if there are steps that can be taken to share intelligence at unclassified levels to improve coordination. As part of such review, the Committee recommends evaluating whether artificial intelligence can play a role in addressing overclassification.

9. ***Strengthen Partnerships with State, Local, Tribal, and Territorial Law Enforcement Agencies and Fusion Centers –***

The Committee recommends that the DNI explore avenues for all IC components to expand intelligence cooperation with state, local tribal, and territorial law enforcement agencies and local fusion centers. These expanded opportunities should focus efforts on areas that are priorities within the National Intelligence Priority Framework. In addition, these efforts could include greater intelligence sharing with these entities and integrating IC analysts who are subject matter experts in various fields within fusion centers.

10. ***IC Collaboration with the Private Sector –***

The Committee recommends that the IC expand efforts to communicate threat information and engage with the private sector. Leveraging new and existing mechanisms to engage with the private sector both to provide relevant threat reporting and to understand private sector perceptions of threats will improve the IC's efficacy across multiple mission sets. These engagements should go beyond areas of traditional cooperation and information sharing, such as critical infrastructure, and include sectors such as agriculture, technology, finance, water, and energy.

11. ***Address "Black Swan" Risks Posed by AI Advancement –***

The Committee believes the proliferation of advanced artificial intelligence models and the rapid advancement of this arena amplify existing risks, most prominently in the terrorism space. The 9/11 Commission emphasized the risk posed by terrorist access to weapons of mass destruction, whether nuclear, radiological, chemical or biological. Preventing terrorist groups from developing access to equipment and expertise necessary to build and use weapons of mass destruction has been a significant point of emphasis for the IC and the national security establishment since 9/11.

Frontier large language models have the possibility of making it significantly easier for any rogue actor, including terrorists, to develop and conduct more destructive attacks. While AI labs seek to prevent models from returning information that could assist a bad actor in, for example, building a bioweapon, the underlying capability of models is developing rapidly and such a use of a model is difficult to fully control.

While there is no single approach to address this threat, the Committee believes the IC and policymakers more broadly must carefully consider how to prevent AI tools from being leveraged for use by rogue actors, including terrorists. At the same time, the Committee believes the IC must accelerate its own responsible adoption of advanced AI capabilities so that the United States stays ahead of its adversaries. Investing in secure AI tools for collection, analysis, and warning paired with rigorous testing, human oversight, and strong privacy and civil liberties protections is essential to preparing the Intelligence Community for the next generation of threats. That same forward-looking posture must extend to other increasingly contested domains as well.

12. ***Reexamine Idea of National Intelligence Reserve Corps –***

In 2004, IRTPA afforded the DNI the authority to establish and train an intelligence reserve comprised of former IC employees to be called upon in emergencies. During the aftermath of 9/11 and war on terror that followed, the importance of longstanding subject matter expertise became readily apparent. Today, as the IC shifts substantial resources toward great power competition—coupled with a recent downsizing in intelligence officers—it runs the risk of atrophying expertise. Like Afghanistan after 9/11, Tunisia, Egypt and Libya during the Arab Spring, or Yemen after its civil war, there are many areas currently minimally examined that could erupt in importance. It would be invaluable for the IC to be able to call upon individuals with those regional or topical areas of expertise, who are already steeped in intelligence tradecraft and processes. Moreover, adding new blood in these instances could limit groupthink and bias toward longstanding analytic lines at a time when that is most vital.

13. ***Deepen IC Lessons Learned Program –***

While various IC agencies have processes to conduct postmortems, especially after intelligence failures, there is less structural examination that compares when and why those agencies had been correct. These examinations should draw from social sciences and go beyond the standardized – and important – tradecraft requirements to consider questions such as whether evidence existed to disconfirm a theory and how the same reports, if mapped onto a different scenario or country, would alter the intelligence assessments.

14. ***Require all Members of Congress, Senators, and Congressional Staff who Hold Clearances to Take Classified Material and Counterintelligence Training –***

Nation-state actors target lawmakers and their staff at all levels of government. In 2026, a staffer on the House Select Committee on the Chinese Communist Party was reportedly offered $10,000 to provide information on certain policy areas.[212] There have been numerous such cases prosecuted by the Department of Justice over the years.

Under current regulations, Members of Congress only undergo classified material handling and counterintelligence training during their new Member orientation. Staff likewise take this training only once. Conversely, such training is generally required annually in the IC. Given Capitol Hill is a prime target for counterintelligence actors, the Committee recommends Members of Congress and cleared staff be required to take classified information handling training at each new Congress.

15. ***Deepen Relationships Between IC Authorizers and Appropriators –***

As discussed above, the Commission recommended establishing a Subcommittee on Appropriations within HPSCI and SSCI, one of the most significant open recommendations. The Committee concurs that at the minimum, greater coordination between authorizers and appropriators would improve Congressional oversight. For example, because the National Intelligence Program budget request spans multiple appropriations subcommittees, oversight of NIP activities is necessarily more fragmented than it should be, making it harder for Congress to assess tradeoffs, identify duplication of effort, and ensure resources are aligned with national intelligence priorities.

16. ***Reauthorize FISA 702 and Extend the Periods of Reauthorization –***

FISA 702 has become the most important authority utilized within the IC for a range of national security imperatives, including counterterrorism. While the Committee recognizes the need to consider reforms to FISA, and has enacted numerous reforms in recent years, most recently to address unacceptable compliance issues within the FBI, the current pattern of short-term reauthorizations of the program creates risk to national security. At the time of this report, statutory authority for FISA 702 has sunset, with the possibility for a catastrophic loss of capability in the months to come. The trend towards short-term reauthorizations makes lapses of this sort more likely, creating uncertainty at best. Accordingly, the Committee reemphasizes the importance of reauthorization of FISA 702, and recommends that Congress consider longer terms of reauthorization, still providing opportunities for reform while lessening risk of a lapse.

17. ***Create a Statutory Definition for Counterintelligence –***

Varying definitions of the term "counterintelligence" have created ambiguity in roles, responsibilities, and what constitutes a counterintelligence threat. The Committee recommends that a statutory definition would solve this issue, taking into account the modern threat landscape in which nation-states utilize third-party individuals, co-optees, nontraditional collectors, and business relationships to exploit and gain an advantage in various sectors related to the United States.

18. ***Ensure the National Counterterrorism Center Remains the Lead Integrator for Counterterrorism Throughout the IC –***

Since being enacted into law, NCTC has played a vital role in coordinating the IC's mission. These efforts helped prevent large-scale terrorist attacks from happening over the last twenty-five years. The center's structure within ODNI has also helped coordinate efforts across agencies and eliminate stovepipes. The Committee recommends NCTC remain the lead integrator for counterterrorism efforts throughout the IC and remain nested in ODNI. The Committee also recommends that NCTC remain properly resourced and funded by Congress to ensure the center's short and long-term success.

19. ***Support IC Elements Sharing Counterintelligence Information with the National Counterintelligence and Security Center –***

There is no current obligation for any IC element to share counterintelligence information with the NCSC. As mentioned previously, the lack of coordination has created stovepipes that have led to insufficient information sharing related to the counterintelligence threat. After the 9/11 Report was released, Congress established NCTC, which incorporated intelligence related to counterterrorism from across the IC, paying dividends in our nation's counterterrorism fight. This same lesson should be applied to counterintelligence. Therefore, the Committee recommends ODNI consider requiring each IC element to share counterintelligence information with the NCSC.

20. ***Expand Capability to Leverage Emerging Technology –***

The private sector plays a vital role in delivering new capabilities to the United States national security community. In today's threat environment, the IC should seek innovative solutions to capability gaps throughout the private sector—especially as it relates to counter-unmanned aerial systems (CUAS), counterintelligence, cyber, AI, quantum computing, and biotechnologies.

To achieve this, Congress should approve additional funding for organizations like In-Q-Tel, the Defense Innovation Unit, the Intelligence Advanced Research Projects Activity, CIA labs, NSA's Research Directorate, and other entities within the IC charged with identifying, developing, and leveraging critical technologies. Congress should also provide funding to establish the Intelligence Community Innovation Unit to expand and synchronize the IC's engagement with the private sector while creating a public-facing entry point for companies seeking to partner with the IC.

Likewise, the IC should expand its outreach to these critical sectors. This move would bring entrepreneurs, growth companies, researchers, and venture capitalists to the table to develop creative solutions where government innovation tends to lag. By creating new financial incentives, the private sector will increasingly engage with government to solve complex security challenges.

Conclusion

This year, as our country has celebrated its 250th anniversary, Americans have been reminded of the many chapters that comprise our national story. Throughout our Nation's history, we have endured tremendous adversity and achieved great triumphs. The American people have weathered storms and overcome seemingly unsurmountable obstacles.

The pages of American history tell an amazing story, yet at the outset of each chapter, success was never guaranteed. From earning independence in the American Revolution, to preserving the Union through a devastating Civil War. From emerging from the unprecedented economic collapse of the Great Depression, to rising victoriously at the end of two World Wars and defeating communism after a decades-long Cold War.

September 11, 2001, marked the beginning of another chapter in our Nation's history. Twenty-five years ago, from scenes of smoldering rubble in New York City, fiery wreckage in Arlington, Virginia, and scattered debris in a field in Shanksville, Pennsylvania, the American people were once again confronted by an extraordinary challenge. Like the generations before them, the American people—bowed but not broken—rose to the occasion and girded themselves for the fight ahead.

At the time, the immediate threat was Islamist terrorism. In the far-flung corners of the world, a new kind of enemy was forming against us, with aims to destroy the United States of America, and indeed, the Western world.

In 2004, the 9/11 Commission illuminated the path forward in confronting this threat with the release of its Report. The recommendations contained within the Report were thorough, adequate, and necessary. The American people and our elected officials needed a roadmap. In a united effort, the 9/11 Commission provided it. In the years following the release of the 9/11 Commission Report, Congress made significant progress in implementing many of its recommendations.

The Committee Report before you today has outlined and discussed the Commission's recommendations relating to the Intelligence Community. It has examined which recommendations have been adopted, wholly, partially, or not at all.

Our Committee Report has also reviewed new and emerging threats that were not present at the time of the September 11th attacks. Indeed, many of these threats were not conceived of at the time of the attacks. The threat landscape today has evolved and expanded significantly since the 9/11 Commission was chartered. We have endeavored to describe some of the most pressing threats our nation faces today.

Our Committee has done this because we believe there is a disparity between what the 9/11 Commission sought to achieve and where our nation stands today. To be sure, in the twenty-five years since the 9/11 attacks, Congress and the Intelligence Community have made great strides in fortifying our country, including pursuing innovative ideas and strategies to stay

abreast of many threats to help keep our country safe. We applaud these efforts. However, gaps remain in our intelligence and national security architecture. These gaps have only widened with the introduction of new technologies and adversarial nations' increased willingness to exploit them.

For this reason, the Committee believes the United States faces a threat environment as complex and dangerous as any since September 11, 2001. Serious gaps remain in our ability to confront and address these vulnerabilities. We are not adequately prepared to confront and address our vulnerabilities. Mr. Cilluffo underscored this point in his testimony before the Committee with a stark warning:

> The strategic warning lights are blinking red. History may not repeat itself, but it tends to rhyme. There's a whole lot of rhyming going on right now. Volt Typhoon, Flax Typhoon, Salt Typhoon, Russian sabotage, Iranian proxies, the extraordinary lessons emerging from Ukraine about drones, autonomy, and precision strike, viewed collectively, they reveal coordinated campaigns designed to shape the strategic environment long before the first shot was ever fired. Individually they are storms. Collectively they become the perfect storm. Too often we investigate incidents. Our adversaries conduct campaigns. Too often we look at the world through our boxes and org charts: cyber over here, counterintelligence over there, critical infrastructure somewhere else. Our adversaries don't organize around our bureaucracies. They organize around our vulnerabilities.[213]

As was the case before 9/11, our nation risks forgetting that it was our failure of imagination that allowed al Qaeda to envision and execute the use of commercial airliners as weapons. As discussed, adversaries across the threat landscape are employing new and innovative tactics to target U.S. interests and undermine our security. We must not lose sight of this reality—or lose our capacity to imagine and prepare for the worst.

In today's age, an attack on our nation might not come by aerial bombing campaigns. It might not come with fiery assaults on civilian or military infrastructure, inflicting mass casualties. A new kind of attack may come quickly and quietly with debilitating consequences for the security and prosperity of our country. The next 9/11 might not look like 9/11, but its impact could be just as grave. The nation should not wait for another attack on the scale of September 11th to act on the vulnerabilities identified in this report.

Now is the time to act before it is too late. Below we offer recommendations that we believe will help secure the next chapter of American history by closing current security gaps and placing the American people on better footing in the face of new threats and determined adversaries.

We offer these recommendations in the spirit of the 9/11 Commission's work. At every point throughout compiling this Report, we have kept the victims of 9/11 and their families in mind. Every day, we worked to honor their sacrifice.

Our Committee's aim is simple: keeping the American people safe and secure, from threats foreign and domestic, while defending the cherished liberties so many generations of Americans have fought to preserve. Twenty-five years after 9/11, this objective is more urgent than ever.

Endnotes:

[1] 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, at 363, https://govinfo.library.unt.edu/911/report/911Report.pdf [hereinafter *The 9/11 Commission Report*].
[2] *Id*. at 399.
[3] *Id*. at 399-400.
[4] David Smith, *'The attack would have been prevented': co-author of 9/11 report reflects on missed opportunities*, THE GUARDIAN, Sep. 9, 2021, https://www.theguardian.com/us-news/2021/sep/09/thomas-kean-september-11-commission-report.
[5] *The 9/11 Commission Report*, at 399.
[6] *Id.* at 403.
[7] *Id.* at 404.
[8] *Id*.
[9] *Id.*
[10] *Id*. At 405.
[11] Exec. Order No. 13354, *National Counterterrorism Center*, 27 August 2004.
[12] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3672.
[13] *Id*. at 118 Stat. 3673.
[14] *Id*. at 3673.
[15] *The 9/11 Commission Report*, at 403–404.
[16] Pub. L. No. 108-458, 118 Stat. 3674.
[17] Thomas Ferraro, *Senate to press ahead with probe into Fort Hood*, REUTERS, Nov. 18, 2009, available at https://www.reuters.com/article/world/senate-to-press-ahead-with-probe-into-fort-hood-idUSTRE5AH5YG/.
[18] Senate Homeland Security and Government Affairs Committee, *Senators Describe Goals of FT. Hood Investigation*, November 18, 2009, https://www.hsgac.senate.gov/media/reps/senators-describe-goals-of-ft-hood-investigation/.
[19] Carrie Johnson, Spencer S. Hsu and Ellen Nakashima, *Hasan had intensified contact with cleric*, NBC NEWS, Nov. 20, 2009, https://www.nbcnews.com/id/wbna34075908.
[20] White House, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Act*, January 7, 2010, 3, available at https://obamawhitehouse.archives.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf.
[21] President Barack Obama, *"The Urgency of Getting This Right"*, January 5, 2010, available at https://obamawhitehouse.archives.gov/blog/2010/01/05/urgency-getting-right.
[22] White House, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Act*, January 7, 2010, 6, available at https://obamawhitehouse.archives.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf.
[23] *Id*.
[24] Joint Press Release, *ODNI and DOJ updated guidelines for NCTC access, retention, use, and dissemination of information in datasets containing non-terrorism information*, Mar. 22,

2012, available at https://web.archive.org/web/20120928021735/http://www.dni.gov/index.php/newsroom/press-releases/96-press-releases-2012/528-odni-and-doj-update-guidelines-for-nctc-access,-retention,-use,-and-dissemination-of-information-in-datasets-containing-non-terrorism-information.

[25] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 35:00 – 35:20 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.

[26] *The 9/11 Commission Report*, at 365.

[27] *Id*.

[28] *Id*. at 399.

[29] *Id*. at 409.

[30] *Id*.

[31] *Id*. at 411–415.

[32] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3689-92.

[33] *Id.*

[34] *Id*. at 3652, 3655.

[35] George Tenet with Bill Harlow, *At the Center of the Storm: My Years at the CIA,* 501 (2007).

[36] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 34:20 – 34:48 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.

[37] *The 9/11 Commission Report*, at 414.

[38] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 53:15 – 53:55 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.

[39] *Id.* at 54:07–54:15.

[40] *Id*. at 54:34–55:11.

[41] Office of the Director of National Intelligence (ODNI), Fact Sheet: ODNI 2.0 Launch, at 1, Aug. 20, 2025, https://www.dni.gov/files/ODNI/documents/ODNI-20-Fact-Sheet.pdf.

[42] *Id.*

[43] *Id.*

[44] *Id*.

[45] *The 9/11 Commission Report*, at 416.

[46] *Id*.

[47] *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. No. 110-53, 121 Stat. 335.

[48] *DNI Releases Budget Figure for National Intelligence Program*, ODNI News Release No. 22-07, Oct. 30, 2007, https://irp.fas.org/news/2007/10/dni103007.pdf.

[49] *Intelligence Authorization Act of 2010*, Pub. L. No. 111-259, 124 Stat. 2702.

[50] *DOD Release Military Intelligence Program Top Line Budget for Fiscal Year 2007, 2008, 2009*, DOD News Release No. 199-11, Mar. 11, 2011, https://sgp.fas.org/news/2011/03/mip.html.
[51] DOS, *Fact Sheet: Usama bin Ladin*, Aug. 21, 1998, available at https://1997-2001.state.gov/regions/africa/fs_bin_ladin.html.
[52] *The 9/11 Commission Report*, at 69.
[53] *Id*. at 380.
[54] *Id*.
[55] *Id*.
[56] *Id*. at 380–81, 413.
[57] Exec. Order No. 13328, *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, available at https://www.presidency.ucsb.edu/documents/executive-order-13328-commission-the-intelligence-capabilities-the-united-states-regarding.
[58] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3672.
[59] *Intelligence Authorization Act for Fiscal Year 2022*, Pub. L. No. 117-103, 136 Stat. 973.
[60] *Id*. at 974.
[61] Office of the Director of National Intelligence (ODNI), Fact Sheet: ODNI 2.0 Launch, 2, Aug. 20, 2025, https://www.dni.gov/files/ODNI/documents/ODNI-20-Fact-Sheet.pdf.
[62] *Id*.
[63] *The 9/11 Commission Report*, at 423.
[64] *Id*.
[65] *Id.*
[66] *Id*.
[67] *Id*.
[68] *Id*.
[69] *Id*. at 424.
[70] *Id*.
[71] *Id*. at 425
[72] *Id*. at 425–26.
[73] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 1:46:38 – 1:46:51 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.
[74] *The 9/11 Commission Report*, at 415.
[75] *Id*.
[76] *Id*.
[77] *Id.*
[78] *Id*.
[79] Office of the Press Secretary, *Memorandum for the Secretary of State, The Secretary of Defense, The Attorney General, and The Director of Central Intelligence*, Nov. 23, 2004, available at https://georgewbush-whitehouse.archives.gov/news/releases/2004/11/text/20041123-8.html.

[80] Transcripts, Senate Select Committee on Intelligence, Subject: National Security Threats to the United States, Federal New Service, Feb. 16, 2005, at 67, https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-hearings-threats.pdf.
[81] Associated Press, *Rumsfeld, Goss oppose paramilitary transfer*, NBC NEWS, June 29, 2005, https://www.nbcnews.com/id/wbna8398092.
[82] *Id*.
[83] *Id*.
[84] *The 9/11 Commission Report*, at 417.
[85] *Id*. at 79.
[86] *Id*. at 417–418.
[87] *Id*.
[88] *Id.* at 88.
[89] *Id.* at 417.
[90] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3664–3665.
[91] *The 9/11 Commission Report,* at 268.
[92] *Id*. at 420.
[93] *Id.*
[94] *Id*. at p. 420-21.
[95] *Id*.
[96] *Id.*
[97] *Id*. at 421.
[98] *Id*.
[99] S.Res. 445, 108th Cong., 2nd sess. Oct. 9, 2004, https://www.congress.gov/bill/108th-congress/senate-resolution/445.
[100] *Id*.
[101] *Id*.
[102] *Id*.
[103] *Id*.
[104] H.Res. 35, 110th Cong. Jan. 9, 2007, https://www.congress.gov/bill/110th-congress/house-resolution/35.
[105] *Id*.
[106] *Id*.
[107] H.Res. 5, 112th Cong. Jan. 5, 2011, https://www.congress.gov/bill/112th-congress/house-resolution/5/text.
[108] *Chairman Rogers Announces Strategic Partnership with House Appropriators*, Press Release, Mar. 23, 2011, available at https://intelligence.house.gov/2011/03/23/chairman-rogers-announces-strategic-partnership-with-house-appropriators/.
[109] *Id*.
[110] *The 9/11 Commission Report*, at 419.
[111] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 43:15 – 43:33 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.
[112] *Id*. at 43:40 – 43:45.

[113] *Id*. at 1:15:00 – 1:16:20.
[114] *Id*. at 1:16:22 – 1:16:31.
[115] *Id*. at 1:16:22 – 1:17:01.
[116] *The 9/11 Commission Report,* at. 383-84.
[117] *Id*. at 385, 389.
[118] *Id*. at 384.
[119] *Id*.
[120] *Id*.
[121] *Id*.
[122] *Id*. at 385.
[123] *Id*.
[124] *Id*. at 387.
[125] *Id*. at 389.
[126] *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, Pub. L. No. 104-208, 110 Stat. 3009-558; *Omnibus Consolidated and Emergency Supplemental Appropriations Act,* Pub. L. No. 105-277, 112 Stat. 2681-68 (1998); *The Immigration and Naturalization Service Data Management Improvement Act of 2000*, Pub. L. No. 106-215, 114 Stat. 337-42.
[127] *USA PATRIOT Act*, Pub. L. No. 107-56, 115 Stat. 353 (2001).
[128] *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, Pub. L. No. 104-208, 110 Stat. 3009-662.
[129] *USA PATRIOT Act*, Pub. L. No. 107-56, 115 Stat. 354, 374 (2001).
[130] *Enhanced Border Security and Visa Entry Reform Act of 2002,* Pub. L. No. 107-173, 116 Stat. 552.
[131] *Id*.
[132] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3818.
[133] *Visa Waiver Permanent Program Act*, Pub. L. No. 106-396, 114 Stat. 1641 (2000).
[134] *Department of Homeland Security Appropriations Act*, Pub. L. No. 110-329, 122 Stat. 3669-70 (2009).
[135] *Consolidated Appropriations Act*, Pub. L. No. 114-113, 129 Stat. 3006 (2016); *Bipartisan Budget Act of 2018*, Pub. L. No 115-123, 132 Stat. 126.
[136] *An act to provide for reconciliation pursuant to title II of H. Con. Res. 14,* Pub. L. No 119-21, 139 Stat. 359 (2025).
[137] Exec. Order No. 13780, *Protecting the Nation From Foreign Terrorist Entry Into the United States*, Mar. 6, 2017, 82 Federal Register 13216.
[138] DHS, *Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States*, 90 Federal Register 48604, 48613, Oct. 27, 2025 [hereinafter *Collection of Biometrics*].
[139] CBP, *Voluntary Self-Reported Exit (VSRE) Pilot*, 90 Federal Register 12752, Mar. 19, 2025.
[140] *Id*. at p. 12755.
[141] *Id*.
[142] GAO, *Facial recognition Technology*, GAO-22-106154, at 3; CBP, *Biometrics: Environments*, "Where is CBP Using Biometrics Today?" https://www.cbp.gov/travel/biometrics/environments.

[143] *Collection of Biometrics*, at 48637; GAO, *Facial Recognition Technology*, GAO-22-106154, at 3.

[144] GAO, *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; DHS, CBP, *Fiscal Year 2020 Entry/Exit Overstay Report*, Sep. 30, 2021, 6.

[145] See, e.g., DOS, Report of the Visa Office*, Immigrant and Nonimmigrant Visa Ineligibilities (by Grounds for Refusal Under the Immigration and Nationality Act)*, FY2024.

[146] CBP, *CBP Enforcement Statistics*, "Terrorist Screening Data Set Encounters," https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics.

[147] *Id.*

[148] *See* DOS, *Designation of International Cartels*, Fact Sheet, Feb. 20, 2025, https://www.state.gov/designation-of-international-cartels; White House, *Secure the* Border, https://www.whitehouse.gov/priorities/border-immigration.

[149] CBP, *CBP Enforcement Statistics*, "Terrorist Screening Data Set Encounters," https://www.cbp.gov/newsroom/stats/cbp enforcement-statistics.

[150] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 33:28 – 33:54 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.

[151] *Open Full Committee Hearing to Discuss the Next-Generation of Threats 25 Years After September 11th*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 9:30 – 10:27 (July 21, 2026), https://www.youtube.com/live/GoJw15sB-fw.

[152] The Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community,* Mar. 2025*,* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[153] Seth Jones, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats: A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-JonesS-20260721.pdf.

[154] *Id.*

[155] Bohdan Ustymenko, *Putin's Arctic ambitions: Russia eyes natural resources and shipping routes*, ATLANTIC COUNCIL, Apr. 9, 2025, https://www.atlanticcouncil.org/blogs/ukrainealert/putins-arctic-ambitions-russia-eyes-natural-resources-and-shipping-routes/.

[156] John Erath, *North Korean Forces in Ukraine: What it Means and What to Do*, GEORGETOWN JOURNAL OF INTERNATIONAL AFFAIRS, Apr. 10, 2025, https://gjia.georgetown.edu/conflict-security/north-korean-forces-in-ukraine-what-it-means-and-what-to-do/.

[157] *Id.*

[158] U.S.-China Economic and Security Review Commission*, Enabling Iran: A Timeline of China's Role During and After Operation Epic Fury,* Aug. 6, 2026, https://www.uscc.gov/research/enabling-iran-timeline-chinas-role-during-and-after-operation-epic-fury.

[159] U.S.-China Economic and Security Review Commission, *China-Iran Fact Sheet: A Short Primer on the Relationship*, Mar. 16, 2026, https://www.uscc.gov/research/china-iran-fact-sheet-short-primer-relationship.

[160] H.R. McMaster, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats, A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-McMasterH-20260721.pdf.

[161] *FBI Director says China most significant counterintelligence threat to U.S.*, THE NATIONAL DESK (YouTube, Oct. 2, 2025), https://www.youtube.com/shorts/z634SdUsjRk.

[162] Christopher Wray, *Statement Before the Senate Homeland Security and Governmental Affairs Committee*, Worldwide Threats to the Homeland, Sep. 24, 2020, https://www.fbi.gov/news/speeches-and-testimony/worldwide-threats-to-the-homeland-092420.

[163] *Open Roundtable: Emerging Gray Zone Threats and a Contested Homeland before the H. Perm. Sel. Comm. on Intel (National Intelligence Enterprise Subcommittee)*, 119th Cong. 2, at 1:07:05 – 1:07:25 (Jun. 25, 2026), https://www.youtube.com/watch?v=aDF7LzM1L4Q.

[164] Shaun Walker, '*These people are disposable': how Russia is using online recruits for a campaign of sabotage in Europe*, THE GUARDIAN, May 4, 2020, *https://www.theguardian.com/world/ng-interactive/2025/may/04/these-people-are-disposable-how-russia-is-using-online-recruits-for-a-campaign-of-sabotage-in-europe*.

[165] Department of Justice, *Two Eastern European Organized Crime Leaders Convicted of Murder for Hire Targeting U.S.-Based Journalist on Behalf of Iranian Government*, Press Release, Mar. 21, 2025, https://www.justice.gov/opa/pr/two-eastern-european-organized-crime-leaders-convicted-murder-hire-targeting-us-based.

[166] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 43:15 – 43:33 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.

[167]Congressman Rick Crawford, *Chairman Crawford Joins Fox News to Discuss Current U.S. Counterintelligence Threats*, Press Release, Sep. 29, 2025, https://intelligence.house.gov/2025/09/29/chairman-crawford-joins-fox-news-to-discuss-current-u-s-counterintelligence-threats/.

[168] Seth Jones, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats: A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-JonesS-20260721.pdf.

[169] *Id.*

[170] H.R. McMaster, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats, A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-McMasterH-20260721.pdf.

[171] Benjamin Buchanan, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats, A Hearing before the H. Perm. Sel. Comm. on Intel*,

119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-BuchananB-20260721.pdf.

[172] *Open Full Committee Hearing to Discuss the Next-Generation of Threats 25 Years After September 11th*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 58:40 – 59:09 (July 21, 2026), https://www.youtube.com/live/GoJw15sB-fw.

[173] *Id.* at 1:01:05 – 1:01:20.

[174] *Id.*

[175] *Id.* at 1:42:45 – 1:43:34.

[176] *Id.*

[177] *Id.* at 21:48 – 21:55.

[178] Representative Josh Gottheimer, *Gottheimer Announces $2.1 Million in New Counterterrorism and Nonprofit Security Grants for Local Temples, Churches, Religious Schools & Organizations,* Press Release, June 26, 2021, https://gottheimer.house.gov/posts/release-gottheimer-announces-21-million-in-new-counterterrorism-and-nonprofit-security-grants-for-local-temples-churches-religious-schools-organizations.

[179] General William "Billy" Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power – Economic and Military*, G.P. Putnam's Sons, New York (1925), at 25-26.

[180] The Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community,* Mar. 2025*,* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[181] CISA, *CISA, FBI, and U.S. and Global Partners Urge Immediate Action to Defend Critical Infrastructure from Pro-Russia Hacktivist Threats*, Press Release, Dec. 9, 2025, https://www.cisa.gov/news-events/news/cisa-fbi-and-us-and-global-partners-urge-immediate-action-defend-critical-infrastructure-pro-russia.

[182] *Open Full Committee Hearing to Discuss the Next-Generation of Threats 25 Years After September 11th*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 57:04 – 57:13 (July 21, 2026), https://www.youtube.com/live/GoJw15sB-fw.

[183] *Id.* at 57:28 – 58:31.

[184] *Id.* at 1:01:30 – 1:02:03.

[185] The Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community,* Feb. 5, 2024, https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[186] Martha Stolze, *Information Laundering via Baltnews on Telegram: How Russian State-Sponsored Media Evade Sanctions and Narrate the War*, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/publications/information-laundering-via-baltnews-on-telegram-how-russian-state-sponsored-media-evade-sanctions-and-narrate-the-war/257.

[187] Stephen Lee Myers and Dustin Volz, *China, Russia and Others Seek to Inflame Debate Over A.I. Data Centers,* NEW YORK TIMES*,* July 9, 2026, https://www.nytimes.com/2026/07/09/business/china-russia-ai-data-centers.html.

[188] *Open Full Committee Hearing to Discuss the Next-Generation of Threats 25 Years After September 11th*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://www.youtube.com/live/GoJw15sB-fw.

[189] *Id.*

[190] Seth Jones, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats: A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-JonesS-20260721.pdf.

[191] The Federal Bureau of Investigation, *Counterintelligence and Espionage*, https://www.fbi.gov/investigate/counterintelligence.

[192] Federal Bureau of Investigation, *Executive Summary, China: The Risk to Corporate America*, https://www.fbi.gov/file-repository/counterintelligence/china-exec-summary-risk-to-corporate-america-2019.pdf/view.

[193] *Open Full Committee Hearing to Discuss the Next-Generation of Threats 25 Years After September 11th*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 43:20 – 43:38 (July 21, 2026), https://www.youtube.com/live/GoJw15sB-fw.

[194] *The 9/11 Commission Report,* at 91.

[195] *Id*. at 401.

[196] *Id*. at 344.

[197] *Id*. at 118.

[198] *Id.* at 193-94.

[199] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*, Cornell University Press (2010), at 112, 114, 116.

[200] Michael Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, Penguin Books (2016), at 48-49.

[201] *Open Full Committee Hearing to Discuss the Next-Generation of Threats 25 Years After September 11th*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 1:51:34 – 1:52:38 (July 21, 2026), https://www.youtube.com/live/GoJw15sB-fw.

[202] *Cybersecurity and Infrastructure Security Agency Act of 2018*, Pub. L. No. 115-278, 132 Stat. 4170.

[203] H.R. McMaster, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats, A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-McMasterH-20260721.pdf.

[204] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 59:04 – 59:23 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.

[205] H.R. McMaster, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats, A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-McMasterH-20260721.pdf.

[206] Justin Doubleday, *OSINT leaders see 'abundance of opportunity' in 2025*, Federal News Network, Mar. 4 2025, *https://federalnewsnetwork.com/fnn-25-anniversary/2025/03/osint-leaders-see-abundance-of-opportunity-in-2025/.*

[207] *Open Hearing to Review the 9/11 Commission Intelligence Recommendations' Impacts and Progress*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 1:30:33 – 1:30:52 (May 20, 2026), https://intelligence.house.gov/2026/05/20/chairman-crawford-rep-stefanik-open-full-committee-hearing-to-review-progress-on-9-11-commission-intel-recommendations/.

[208] *Id.* at 1:30:02 – 1:30:32

[209] Frank Cilluffo, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats, A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-CilluffoF-20260721.pdf.

[210] Eric McDaniel, *A key U.S. spy tool has lapsed – now what?*, NPR, 13 June 2026, https://www.npr.org/2026/06/12/nx-s1-5856291/fisa-702-surveillance-expiration-bill-pulte.

[211] *See* H.R. McMaster, Written Testimony, *Open Hearing on 25 Years After 9/11: Confronting the Next Generation of Threats, A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2 (July 21, 2026), https://docs.house.gov/meetings/IG/IG00/20260721/119472/HHRG-119-IG00-Wstate-McMasterH-20260721.pdf

[212] Dustin Volz, *He Offered a Lawmaker's Aide Quick Cash. Was He Spying for China?*, NEW YORK TIMES, May 9, 2026, https://www.nytimes.com/2026/05/09/us/politics/china-us-spy-congressional-aide.html?eafs_enabled=false.

[213] *Open Full Committee Hearing to Discuss the Next-Generation of Threats 25 Years After September 11th*: *A Hearing before the H. Perm. Sel. Comm. on Intel*, 119th Cong. 2, at 32:43 – 33:36 (July 21, 2026), https://www.youtube.com/live/GoJw15sB-fw.