Statement for the Record
of
Jamil N. Jaffer[1]
on the
Bipartisan Review of 9/11 Commission Report
before the
House Permanent Select Committee on Intelligence
of the
United States House of Representatives

May 20, 2026

I. Introduction

Committee Chairman Crawford, Committee Ranking Member Himes, Review Chairwoman Stefanik, Review Co-Chairman Gottheimer, and Members of the Committee: thank you for inviting me here today to discuss the very real and ongoing threat of terrorism facing our nation today and what tools, techniques, and authorities we might best utilize to combat this threat.

It is a testimony to the leadership of Chairman Crawford and Ranking Member Himes that over eight months ago—in what everyone can reasonably acknowledge was and remains a challenging political environment for our nation—they were able to announce the establishment of a bipartisan review by the House Permanent Select Committee on Intelligence (HPSCI) of the recommendations of the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission).[2] It is likewise a testimony to Chairwoman Stefanik's and Co-Chairman Gottheimer's leadership that they have been able to conduct a thorough bipartisan review of these matters to date, including holding: (1) a joint closed briefing with the House Committee on Homeland Security featuring Intelligence Community (IC) leaders from the National

[1] Jamil N. Jaffer currently serves as Founder & Executive Director of the National Security Institute and the NSI Cyber & Tech Center, and as an Assistant Professor of Law, Director of the National Security Law & Policy Program, and Director of the Cyber, Intelligence, and National Security LLM program at the Antonin Scalia Law School at George Mason University. Mr. Jaffer is also a Venture Partner at Paladin Capital Group, a leading global multi-stage investor that identifies, supports, and invests in innovative dual-use companies that develop promising, early-stage technologies to protect the national and economic security of the United States and our allies. Mr. Jaffer serves on a variety of public and private boards of directors and advisory boards and recently served as a member of the Virginia Governor's Task Force on Artificial Intelligence. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, Senior Counsel to the House Permanent Select Committee on Intelligence, Associate Counsel to President George W. Bush in the White House, and Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice, as well as more recently as a member of the Cyber Safety Review Board at the Department of Homeland Security. Mr. Jaffer is testifying before this Subcommittee in his personal and individual capacity and is not testifying on behalf of any organization or entity, including but not limited to any current or former employer or public or private entity.

[2] *See* House Permanent Select Committee on Intelligence, *House Intelligence Committee Stands Up Bipartisan Review of 9/11 Intelligence Recommendations* (Sept. 11, 2025), *available online at* <https://intelligence.house.gov/2025/09/11/house-intelligence-committee-stands-up-bipartisan-review-of-9-11-intelligence-recommendations/>; *see also* National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (July 22, 2005), *available online at* <https://govinfo.library.unt.edu/911/report/911Report.pdf>.

Counterterrorism Center (NCTC), the Federal Bureau of Investigation (FBI), the Defense Intelligence Agency (DIA), and the Department of Homeland Security (DHS) discussing the "current U.S. counterterrorism mission across the United States and the globe and…how the intelligence reforms implemented post-9/11 are working today";[3] (2) a closed briefing on counterterrorism threats with the Central Intelligence Agency (CIA) to "receive an update on the IC's counterterrorism (CT) mission amid the current CT threat landscape…[and] lessons learned from the intelligence community's perspective;[4] and (3) most recently, a closed briefing with the FBI's Counterterrorism Division (CTD) on a set of recent terrorist attacks conducted in the United States to provide "insight into the trends the FBI is seeing around recent attempts to carry out terror attacks and how the threat landscape, and therefore [the FBI's] response to detect and deter, has evolved since September 11, 2001."[5]

As the members of the Committee are aware, this review is designed to understand the "current status of the IC's adoption of the [9/11] Commission's recommendations…[and] as how the IC is equipped to counter the threats the United States will face over the next 25 years," to evaluate the "progress made on the [Commission's] intelligence-related recommendations" and to "identify possible gaps or areas of improvement."[6] The questions the review has been called upon to address could not be more important given the increasingly dangerous and varied threat environment we face today. As such, the Committee's decision to launch this bipartisan review comes at exactly the right moment.

Two generations of Americans have grown up in the post-9/11 environment, with children born after 9/11 having now reached post-college age and moved on to their careers or graduate school. These generations have lived in the shadows of the attacks, dealing with the decisions made in the days, weeks, and months that followed, but many will never remember sheer pain that our nation went through on that fateful day, nor the deep national resolve that was formed as then-President George W. Bush stood on a pile of rubble at the site of the Twin Towers, and said, "I can hear you. The rest of the world hears you. And the people who knocked these buildings down will hear all of us soon."[7]

The 9/11 generation—which includes all of the witnesses sitting at this table and all of the members on the dais, I believe—understands all too well exactly what those words meant back then and what they mean today. That generation deeply feels the commitment to protecting our nation and its people and preventing anything like that day from ever happening again.

---

[3] *See* HPSCI, *House Intel Committee Holds Joint Briefing with Homeland Security Committee in 9/11 Intel Recommendations Review* (Dec. 17, 2025), available online at <https://intelligence.house.gov/2025/12/17/house-intel-committee-holds-joint-briefing-with-homeland-security-committee-in-9-11-intel-recommendations-review/>.

[4] *See* HPSCI, *House Intelligence Committee Holds Briefing on Counterterrorism Threats as Part of 9/11 Review Effort* (Feb 12, 2026), *available online at* <https://intelligence.house.gov/2026/02/12/house-intelligence-committee-holds-briefing-on-counterterrorism-threats-as-part-of-9-11-review-effort/>.

[5] See HPSCI, *House Intelligence Committee Holds Briefing with FBI on Recent Terror Attacks as Part of 9/11 Review Effort* (May 15, 2026), *available online at* <https://intelligence.house.gov/2026/05/15/house-intelligence-committee-holds-briefing-with-fbi-on-recent-terror-attacks-as-part-of-9-11-review-effort/>.

[6] *See HPSCI Review*, *supra* n. 2.

[7] *See* George W. Bush Presidential Library, *Featured Artifact*, *available online at* <https://www.georgewbushlibrary.gov/explore/galleries/featured-artifact>.

My goal in this testimony, therefore, is to briefly discuss the current nature of the terrorist and other key threats facing our nation, identify some of the areas covered by the 9/11 Commission's recommendations that still need more work, discuss adjacent areas that are relevant to the modern threat environment to prevent another such attack and to protection our national security, and make a handful of actionable recommendations that I believe will help better position the IC to detect, deter, and defeat the threats that confront us today and therefore protect our nation in the near term.

II. The Modern Threat Environment

The threat environment facing the United States today is perhaps more serious and complicated than any time in recent memory. First, it bears noting that the threat of al Qaeda, its affiliates, and its various offshoots, including ISIS, while "significantly weaker than at their respective peaks during the early 2000s and mid-2010s…persist in efforts to rebuild and threaten the U.S. Homeland and our global interests."[8] These groups include, but are not limited to al-Qaeda in the Arabian Peninsula (AQAP), ISIS-Khorasan in South Asia, and ISIS in Syria, which are the three the IC assesses are most likely to conduct attacks overseas.[9] The IC believes that al Qaeda likely has between 15,000 and 28,000 members worldwide, while ISIS has between 12,000 and 18,000 members.[10] In 2023, Gen. Erik Kurilla, then-the US CENTCOM Commander, publicly cautioned that ISIS-K could conduct an "external operation against U.S. or Western interests abroad in as little as six months, with little to no warning," a warning he repeated in similar form in June 2025 as well. And the DNI has noted that "[i]n recent years, al-Qa'ida and ISIS plotters intent on targeting the Homeland have focused more on virtually recruiting U.S.-based aspirants to encourage and enable potential attacks," and that "[w]hile al-Qa'ida and ISIS maintain the intent to launch operations targeting the U.S., the most likely terrorist attack scenario in the Homeland involves U.S.-based lone offenders," including young people motivated by terrorist messaging and networks on social media."[11]

Moreover, with the recent U.S. strikes and the (and ongoing) conflict in Iran, including Operation Midnight Hammer, Operation Epic Fury, and Project Freedom, the possibility of terrorist attacks by Iranian-affiliated or supported groups—including Hizballah, Palestinian Islamic Jihad, Hamas, the Houthis, and various Iran-backed Shia militias in Iraq—remains heightened even above the historic and long-standing threat posed by such groups and despite the significant pressure placed on these groups by the United States and Israel.[12] Indeed, the United States government has long understood the capability and interest of Iranian-related threat actors to conduct operations in the

[8] *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 2026), at 7-8, *available online at* <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf>.
[9] *Id*. at 8, 10.
[10] *Id*. at 10.
[11] *Id*. at 8-9.
[12] Id. at 8, 10, 30-31.

United States, whether through terrorist plots targeting former American senior officials[13] or foreign diplomats,[14] or through potential direct action against Americans in the United States.[15]

Indeed, the recent charges brought against Mohammad Baqer Saad Dawood Al-Saadi—an Iraqi national, senior member of Kataib Hizballah (an Iran-backed Shia militia responsible for the deaths of hundreds of American soldiers in Iraq), and an operative for Iran's Islamic Revolutionary Guard Corps (IRGC)—related to his "involvement in nearly 20 attacks and attempted attacks throughout Europe and the United States," including a plot in March and April of this year to carry out terrorist attacks in the United States involving the targeting of a "prominent Jewish synagogue located in New York…[and] two additional U.S.-based Jewish institutions in Los Angeles, California, and Scottsdale, Arizona."[16]

This is particularly concerning given the DNI's recent assessment that the United States faces "an enduring challenge of detecting individuals who might seek to commit acts of terror after entering the Homeland… during the past few years."[17] The DNI noted that while "[s]ince January, U.S. officials have only had a handful of encounters at our southern or northern borders with individuals associated with terrorist groups with a strategic intent to attack the Homeland, such as al-Qa'ida and ISIS…[the United States] need[s] to continue efforts to identify, locate, and remove suspected foreign terrorists who have exploited border vulnerabilities during the last five years."[18] This, of course, is not an idle concern. The 9/11 Commission itself flagged the importance of terrorists exploiting such avenues to travel to the United States.[19]

And beyond the terrorist threat, it is worth noting that the IC assesses that "[t]he global security landscape is volatile and complex, with armed conflict growing more common and posing potential threats to U.S. interests" and that "[s]trategic competition and regional and smaller powers becoming more willing to use force to pursue their interests [also] heighten the risk of conflict."[20] Moreover, the DNI has flagged a range of threats to the United States posed by adversary nations, including China, Russia, Iran, and North Korea, as well as by transnational criminal gangs and drug traffickers. For example, the IC projects that by 2035, more than 16,000 missiles will be able to reach the United States, up from the current figure of more than 3,000 such missiles, a more-than 5x increase.[21] Likewise, the DNI has noted that "[t]he space domain is

---

[13] *See* Mike Wendling, *FBI warns about Iranian spy allegedly plotting to kill US officials*, BBC (Mar. 5, 2024), *available online at* <https://www.bbc.com/news/world-us-canada-68471252>.

[14] *See* U.S. Department of Justice, *Two Men Charged in Alleged Plot to Assassinate Saudi Arabian Ambassador to the United States* (Oct. 11, 2011), *available online at* <https://www.justice.gov/archives/opa/pr/two-men-charged-alleged-plot-assassinate-saudi-arabian-ambassador-united-states>.

[15] *See, e.g.*, Rebecca Schneid, *The Iran-Backed Militia Behind a Terror Plot Against American Jews*, Time (May 16, 2026), *available online at* <https://time.com/article/2026/05/16/kataib-hezbollah-terror-plot-synagogue/>.

[16] U.S. Department of Justice, Iraqi National Arrested and Charged with Providing Material Support to Iranian-Backed Terrorist Organizations and Directing Attacks Targeting U.S. Citizens and Interests (May 15, 2026), available online at <https://www.justice.gov/opa/pr/iraqi-national-arrested-and-charged-providing-material-support-iranian-backed-terrorist>.

[17] *See Annual Threat Assessment*, *supra* n. 8 at 8.

[18] *Id*.

[19] *See 9/11 Commission Report*, *supra* n. 2 at 383-85.

[20] *See Annual Threat Assessment*, *supra* n. 8 at 14.

[21] *Id*. at 10

becoming increasingly contested, with China and Russia developing counterspace capabilities to challenge our own space efforts and U.S. dominance more generally" and that "[t]he threats of nuclear proliferation and chemical and biological warfare capabilities continue to grow."[22]

Perhaps most prominently, the DNI has argued that global armed conflict presents a serious threat to the United States, with "61 active state-based conflicts across the world, the highest number since the end of World War II…result[ing] in about 129,000 battle-related deaths, the fourth highest of any year since the end of the Cold War…superseded only by 2021, 2022, and 2023."[23] The DNI notes that this risk of conflict is "heightened by major power competition…[because] Beijing and Moscow view Washington and its allies and partners as aggressors, and hostile toward their interests in Europe and the Asia-Pacific region" and that "[e]ven if the great powers refrain from conflict, many regional and smaller powers are growing much more willing to use force to pursue their interests."[24]

Countries are using "deniable, coercive, or violent approaches below the threshold of war…includ[ing] acts of sabotage, assassinations, detentions, [and] non-lethal attacks,"[25] as well as increasingly conducting operations in the cyber domain as well.[26] These trends, when combined with the changes we've seen in battlefield technology the Ukraine war, make it clear that the IC is spot on in assessing that "[f]uture warfare will require rapid adaptation, both on the offense and defense," and "a balance between quality and quantity…[where] [e]xquisite, high-end capabilities…cannot be continually replenished at scale in a lengthy, high-intensity conflict."[27] Indeed, the use of unmanned aerial systems for warfare—a trend the United States fundamentally built in the aftermath of the 9/11 attacks—can now also present a significant asymmetric threat, as the Ukraine's Operation Spiderweb vividly demonstrated in June 2025, with systems pre-positioned deep within an adversary's territory being used to inflict billions of dollars in strategic damage on otherwise hardened military targets.

Likewise, the IC is exactly right in assessing that "[i]ntelligence and information will continue to be important to military success," with "[u]ncrewed systems…mak[ing] real-time surveillance and targeting achievable for many militaries, particularly when teamed with commercial imagery and AI or machine learning systems."[28]

Moreover, when these trends are combined with the advent and rapidly increasing adoption of AI globally, including the proliferation of highly capable open-weight models by China (although this trend may be changing), as well as the role that advanced AI capabilities like Mythos and ChatGPT 5.5 Cyber can play in identifying and exploiting new and novel vulnerabilities (as well as addressing them at scale),[29] we are likely to see a broader proliferation of more sophisticated

---

[22] *Id*. at 14.
[23] *Id*.
[24] *Id*.
[25] *Id*.
[26] *Id*. at 16-17
[27] *See Annual Threat Assessment*, *supra* n. 8 at 15.
[28] *Id.*
[29] *See, e.g.*, Hugh Son & Sam Sabin, *Anthropic's Mythos Set Off a Cybersecurity 'Hysteria.' Experts Say the Threat was Already Here*, CNBC (May 8, 2026), *available online at* <https://www.cnbc.com/2026/05/08/anthropic-mythos-ai-cybersecurity-banks.html>.

influence operations, advanced biological design work, malware and exploit development, and intelligence collection at scale.

Earlier assessments of this broad range of threats, led then-FBI Director Christopher Wray to say in 2024 in Congressional testimony that he'd be "hard pressed to think of a time when so many threats to our public safety and national security were so elevated all at once."[30] This echoes, in many ways, "the system was blinking red" concerns expressed by then-CIA Director George Tenet describing the threat profile facing our nation in the summer of 2001.[31]

Against this rapidly evolving threat picture, the key question for this Committee and the Review is whether the legal, institutional, and operational architectures that we built in the aftermath of 9/11—including institutions like the Office of the Director of National Intelligence, the National Counterterrorism Center, the National Counterintelligence and Security Center, the Joint Terrorism Task Forces, the Department of Homeland Security, the Justice Department's National Security Division, FBI's National Security Branch, and legislation like the USA PATRIOT Act and the FISA Amendments Act—are fit for purpose for the next twenty-five years.

In my view, the answer to that question is essentially yes, although I would encourage certain changes to extend our capabilities into the future and caution strongly against making changes that would take our eyes off the ball and unnecessarily give our adversaries an advantage.

III. The Fight Over Section 702

As this Committee well knows, Section 702 of the Foreign Intelligence Surveillance Act—which permits the collection of foreign intelligence from non-United States persons reasonably believed to be located outside the United States (i.e., those individuals who are not U.S. citizens or lawful permanent residents and are reasonably believed to be outside the U.S.)—is the single most valuable intelligence collection authority available to the government. Indeed, as of 2024, 60% of the articles in the President's Daily Brief (PDB) contained Section 702 information.[32]

The wide range of critical intelligence topics covered by Section 702 collection, and the nature and quality of foreign intelligence obtained is hard to overstate. Specifically, according to the Office of the Director of National Intelligence, using Section 702 collected data "is how the Intelligence Community generates crucial information to protect the United States from threats, including terrorism, cyber-attacks, narcotics trafficking, and weapons proliferation."[33]

Indeed, just looking at recent declassified overseas counterterrorism successes alone, Section 702 was used in 2023 to has been used to "identif[y] a threat from foreign terrorists against multiple

---

[30] *See* Federal Bureau of Investigation, *Director Wray's Opening Statement to the House Appropriations Committee* (Apr. 11, 2024), *available online at* <https://www.fbi.gov/news/speeches-and-testimony/director-wrays-opening-statement-to-the-house-appropriations-committee-041124>.

[31] *See 9/11 Commission Report*, *supra* n. 2 at 259.

[32] Office of the Director of National Intelligence, *FISA Section 702 Value* (Feb. 14, 2024), at 1, *available online at* <https://www.intelligence.gov/assets/documents/702-documents/FISA_Section_702_Vignettes-20240214_Final.pdf>.

[33] *Id*.

U.S. military installations overseas inspired by the Israel-Gaza conflict" and in 2020 to "identify members of a terrorist cell that was planning an attack on a U.S. facility in a Middle Eastern country" and to disrupt that attack.[34] Likewise, Section 702 data "informed planning for the February 2022 U.S. military operation that resulted in the death in Syria of Hajji 'Abdallah, the leader of ISIS…[by] contribut[ing] to the U.S. assessment of the ISIS leader's presence in Syria[, which]…provided military planners and senior policy makers confidence in their decision to send U.S. troops on the mission."[35] And Section 702 "contributed to the United States' successful operation against Ayman al-Zawahiri in 2022."[36]

Moreover, Section 702 was used in 2023 to "disrupt[] a potentially imminent attack by a terrorist who had researched and identified specific critical infrastructure sites inside the United States, less than a month after he was first identified and subsequently queried against Section 702 information."[37] This is a particularly important matter because in that case, "the results of a U.S. person query provided important intelligence that contributed to the additional investigation of the U.S. person terrorist."[38] Specifically, the FBI "used iterative U.S. person queries to stay ahead of the terrorist's plans as his plot developed and he shifted communications platforms," which allowed the FBI to "stay ahead of the threat and ensure [the government was] not missing important intelligence on the plot."[39]

In 2022, the Section 702 allowed the government in 2022 to "discover that state-supported hackers had infiltrated computer systems on utilities in several locations in the U.S….and…warn the systems' operators, help them expel the hackers from their systems, and monitor other infrastructure for further victims."[40] Section 702 also played a critical role in 2021 in the U.S. government's response to the cyberattack on Colonial Pipeline; in that case, the IC "acquired information that verified the identity of the hacker, as well as information that enabled U.S. government efforts to recover most of the ransom."[41] Likewise, Section 702 has played a key role in defending against Iran-state sponsored hackers and both Russian and Iranian ransomware actors.[42]

Section 702 has also helped "uncover gruesome atrocities committed by Russia in Ukraine—including the murder of noncombatants, the forced relocation of children from Russian-occupied Ukraine to the Russian Federation, and the detention of refugees fleeing violence by Russian personnel"[43] and it was also used to disrupt a foreign state actor's effort to "gain[] access to sensitive technology that is used around the world."[44]

---

[34] *Id*.
[35] *Id*. at 2.
[36] *Id*.
[37] *Id.*
[38] *Id*.
[39] *Id*.
[40] *Id*. at 2-3.
[41] *Id*. at 3.
[42] *Id*.
[43] *Id*. at 4.
[44] *Id*.

And finally, as in the terrorism plot, in another case, the FBI used "U.S. person queries against Section 702 acquired information helped FBI to identify intrusion efforts against a transportation hub in the United States…[and specifically to] help[] FBI to identify where the Chinese hackers had achieved successful compromises of network infrastructure[,]…enabl[ing] FBI to alert the network operators so they could take action to mitigate the intrusions."[45]

What these facts demonstrate is not only that Section 702 is a massively valuable tool, but that U.S. person queries of the data—done consistent with the relevant law and procedures—are a critical part of protecting the safety and security of Americans and our critical infrastructure. And these examples only represent a relatively small subset of declassified information that has been made available—and a tiny fraction of the highly valuable intelligence collected in nearly two decades that Section 702 has been in place.

To be fair, there has been some controversy around Section 702, specifically around the issue of U.S. person queries. There has also been some misplaced controversy about the relationship between Section 702 and the admittedly problematic failures that took place during the Crossfire Hurricane investigation. To be clear, on the latter issue, there is **no connection** between Section 702 surveillance which, by its very terms, can never be used to target Americans anywhere in the world or anyone in the United States, and traditional (so-called) Title I FISA, which is explicitly intended to be used in the United States, based on an individualized probable cause finding made by a Senate-confirmed federal district judge (similar to a traditional wiretap).

In the Crossfire Hurricane matter, an individual FBI attorney, Kevin Clinesmith, illegally altered an email from another government agency to indicate that Carter Page—a one-time staffer on President Donald Trump's campaign—to insert the words "not a source" and then forwarded that email to a senior FBI official signing a traditional Title I FISA renewal application (not a Section 702 authorization) against Mr. Page.[46] Clinesmith pled guilty to making a false statement within the jurisdiction of the executive and judicial branches and was sentenced to 12 months probation and 400 hours of community service but served no prison time.[47] This situation—which was hugely problematic—first, had nothing to do with Section 702, and second, is an example of a well-brought prosecution that ultimately should have led to a much stiffer penalty against Mr. Clinesmith, including significant jail time and a major fine.

In order to deter such behavior in the future, Congress should consider specifically criminalizing the type of conduct at issue here—the knowing and willful misrepresentation of a material fact in any application, certification, or filing before the FISC—and providing a stiff penalty, potentially including a mandatory minimum so where the target of surveillance is a U.S person. While this reform is important, it is worth noting once again that the underlying matter has nothing to do with Section 702.

---

[45] *Id*. at 3.

[46] *See* District of Columbia Court of Appeals, *In the Matter of Kevin E. Clinesmith*, D.C. App. No. 21-BG-018, *Report and Recommendation Approving Petition for Negotiated Discipline* (Aug. 11, 2021), *available online at* <https://www.dcbar.org/ServeFile/GetDisciplinaryActionFile?fileName=HCKevinEClinesmith21ND004.pdf>.

[47] Department of Justice, *FBI Attorney Admits Altering Email Used for FISA Application During "Crossfire Hurricane" Investigation* (Aug. 19, 2020), *available online at* <https://www.justice.gov/usao-ct/pr/fbi-attorney-admits-altering-email-used-fisa-application-during-crossfire-hurricane>.

With respect to the debate over the use of U.S. person queries in the Section 702 database, there are a few things to be said. First, as noted above, U.S. person queries are often quite helpful in cases that are designed to protect the safety and security of American citizens and critical infrastructure organizations. Second, requiring the government to get a federal court order to search a database of lawfully collected information already in its possession—a database consisting of information obtained by targeting foreigners located overseas for the collection of foreign intelligence information—would undermine the very purpose of one of the key the post-9/11 reforms, namely deconstructing the "wall" between foreign intelligence and law enforcement work that had grown up—due to a series of internal Department of Justice and FBI guidelines and a misreading of the original 1978 FISA statute—prior to the 9/11 attacks.[48]

It was this notional "wall," and key misunderstandings about it, that the 9/11 Commission and later reviews determined were a key factor in why information lawfully in the possession of the CIA relating to two of the future 9/11 hijackers (Khalid al-Mihdhar and Nawaf al-Hazmi)—namely that they were al Qaeda operatives with visas to travel to the United States—was not passed on to the FBI in time to track them down living in San Diego, California (in their true names) for over a year leading up to the 9/11 attacks.[49] Just as the conceptual "wall" make the CIA unsure as to whether it could—or should—pass along the data about Mihdhar and Hazmi to the FBI until it was too late, so too would the imposition of a requirement that the government get a court order to search lawfully collected data hamper the ability to identify individuals talking to foreign terrorists.

Imposing a warrant requirement for a U.S. person query, it would make it well neigh impossible for the government to demonstrate to a federal judge that it had the requisite probable cause because it would not have access to the very data that could provide just such probable cause. This was not the goal of the Section 702 reforms. To the contrary, the Section 702 reforms were specifically designed to allow the government to identify when a foreign intelligence target was talking to someone in the United States.[50] Indeed, imposing a warrant requirement on such queries would, in effect, require the FBI to obtain a court order before it can ask its own database whether a known foreign-intelligence target may have been in contact with a U.S. person. Cutting off access to that information would be robbing the government of access to already lawfully collected information at the very time it needs it: namely when an overseas foreign intelligence may well be contacting a domestic compatriot to give the "go order" to conduct an attack.

Such a limitation is not a privacy protection in any meaningful sense because the underlying communications have already been lawfully acquired, under FISA court-approved procedures, against a non-U.S. target abroad. Instead, it is simply a procedural barrier to connecting the dots—a failure similar in kind to the very mistakes that the 9/11 Commission identified as key blockers to stopping September 11 attacks. It would truly be a shame if, twenty-five years after the 9/11 attacks, we forgot those lessons and recreated the very same wall that the 9/11 Commission and others specifically encouraged us to dismantle.

---

[48] *See 9/11 Commission Report*, *supra* n. 2 at 78-80.

[49] *Id*. at 81-82.

[50] *See, e.g.*, Kenneth L. Wainstein, *Statement for the Record Concerning the Foreign Intelligence Surveillance Act*, House Permanent Select Committee on Intelligence (Sept. 20, 2007), at 14-16, *available online at* <https://www.justice.gov/archive/nsd/2007/wainstein-HPSCI-statement-9-20-07.pdf>.

This is, of course, not the first time a warrant requirement has been proposed, but it has been defeated each time, including as recently as in 2024. Instead, Congress has chosen, multiple times (including in 2024) to put in place reforms, including training, better oversight, more senior approval requirements, and certain limited restrictions on queries not likely to return foreign intelligence information.[51] These reforms have now had time to work and, as we can see from the Annual Statistical Transparency Reports from the two years since Reforming Intelligence and Securing America Act (RISAA) was enacted, U.S. person queries by the FBI are down significantly from pre-reform numbers (which themselves were apparently inflated by efforts to protect U.S. person victims from nation-state cyber hackers),[52] and compliance error rates are also down.[53] Indeed, it is worth noting that the compliance issues that have existed in the past with respect to Section 702 have been carefully looked at by both the Privacy and Civil Liberties Oversight Board on multiple occasions and by the President's Review Group on Intelligence and Communications Technologies in 2014 and these reviews have repeatedly found that the vast majority of such instances have been unintentional, self-identified, self-reported, and almost always fixed through the existing executive branch and judicial oversight mechanisms.[54]

Given all this, there is little doubt in my mind that not only should a clean Section 702 reauthorization should be an easy call, Congress should categorically reject any proposal to impose a warrant requirement on Section 702 queries, and perhaps most importantly, Congress should make Section 702 permanent.

Having served on Capitol Hill in three different jobs for nearly a half-dozen years, I realize that isn't where we are today as a political matter. But the fact of the matter is that the current ritual of reauthorizing Section 702 every few years—often punctuated by short-term extensions and threats of lapse (as we are now experiencing)—is, respectfully, a form of political brinksmanship that imposes real operational costs on the IC and offers little to no privacy benefit in return.

The many substantive privacy protections built into Section 702 both from the outset as well as based on reforms put in place over the last nearly two decades, including the foreign-targeting

---

[51] *See* Andreas Kuersten, *FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act* (July 8, 2025), Congressional Research Service, R48592, *available online at* <https://www.congress.gov/crs_external_products/R/PDF/R48592/R48592.2.pdf>.

[52] *See* Office of the Director of National Intelligence, *The Value of U.S. Person Queries of Section 702* (Mar. 17, 2026), *available online at* <https://www.intel.gov/assets/documents/702-documents/US_Person_Queries_FISA_Section_702-FINAL.pdf>.

[53] *See* Office of the Director of National Intelligence, *Annual Statistical Transparency Report (ASTR) Regarding the Intelligence Community's (IC) Use of National Security Surveillance Authorities for Calendar Year 2025* (Apr. 1, 2026), *available online at* <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2026/4149-astr-cy25>; Office of the Director of National Intelligence, *Annual Statistical Transparency Report (ASTR) Regarding the Intelligence Community's (IC) Use of National Security Surveillance Authorities for Calendar Year 2024* (May 5, 2025), *available online at* <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2025/4071-astr-cy24>.

[54] *See, e.g.*, Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Staff Report (Apr. 2, 2026), *available online at* <https://documents.pclob.gov/prod/Documents/OversightReport/315fe19c-07f3-4cc6-986a-ff199ce5b616/Unclassified%20PCLOB%20702%20Report%202026.pdf>

requirement, the foreign-location requirement, the foreign intelligence purpose requirement, the FISC-approved targeting and minimization procedures, the FISC-approved querying procedures, the prohibition on reverse targeting, the PCLOB, congressional intelligence committee, and inspector generals' oversight, as well as the compliance reporting regime, and now the pre-RISAA and post-RISAA querying rules, taken together, are more than sufficient to do the job. And if they are not, Congress can always legislate. Congress need not recreate the current statutory Sword of Damocles hanging over itself and the IC in order to conduct robust oversight and change the law as needed.

Indeed, sunset provisions like the one in Section 702 actually often do the opposite of what their defenders argue. By creating a fear of lapse, they hamper the IC's ability to do its work, and in the actual case of lapse (which has happened occasionally), they have resulted in telecommunications companies limiting their compliance with existing directives.[55] Such provisions also unnecessarily politicize a national-security authority focused on foreigners overseas that has repeatedly been found to operate consistent with the Fourth Amendment and statutory law. And—perhaps most importantly—they offer foreign adversaries a periodic gift: a window during which our enemies know, with some confidence, that U.S. intelligence collection against them may be operationally degraded.

Over the past two decades, Congress has permanently reauthorized the overwhelming majority of the post-9/11 authorities that had sunsets, including 13 of 16 provisions of the USA PATRIOT Act, and the surviving three—Section 215 business records, roving wiretaps, and the IRTPA "lone wolf" authority—were repeatedly extended on short timelines until their 2020 lapse, which many publicly described as a significant national-security mistake.[56] Section 702 is no different. The right answer, in my view, is to make Section 702 permanent and avoid the possibility of a temporary lapse in this critically important authority. If Congress wishes to retain a mechanism for periodic recalibration, the appropriate vehicle is regular oversight and the normal legislative process, not panic button threat of a recurring sunset.

IV. Addressing the Hot Pursuit and the Non-U.S. Person Questions

In addition to making Section 702 permanent, there are two other statutory changes that Congress ought consider with respect to the Foreign Intelligence Surveillance Act. First, Congress ought consider addressing the situation in which the Intelligence Community is lawfully conducting Section 702 or equivalent foreign-intelligence collection against a non-U.S. person reasonably believed to be located abroad, and the target physically enters the United States.

Under current law, the moment a foreign surveillance target crosses into U.S. territory, Section 702 targeting must be discontinued because the target is no longer reasonably believed to be located outside the United States. To continue collection, the Intelligence Community must, in practice, obtain a traditional Title I FISA order, predicated on a showing of probable cause to

---

[55] *See* Department of Justice, *Letter to Congressional Leaders on Reauthorization of Section 702 and Potential Lapse* (Apr. 5, 2025), at 1-2, *available online at* <https://www.justice.gov/nsd/media/1346981/dl?inline=>.

[56] *See, e.g.*, Jamil N. Jaffer, *Prepared Statement on Reauthorizing the USA FREEDOM Act of 2015*, Senate Committee on the Judiciary (Nov. 6, 2019), *available online at* <https://www.judiciary.senate.gov/imo/media/doc/Jaffer%20Testimony.pdf>.

believe that the target is a foreign power or an agent of a foreign power, supported by minimization procedures, and approved by the FISC. The Title I process can take days to weeks and, while there are emergency authorizations available to the Attorney General, because the penalties of not obtaining a later court order are so severe (e.g., reporting the fact of surveillance to the target), in practice such EAs can be fairly slow as well. The result is an operationally problematic seam in our surveillance authorities: at exactly the moment that a known foreign terror suspect or foreign intelligence officer enters the United States—the very moment when the public-safety and national security risk is at its highest— the IC must stop collecting against that target.

To address this issue, Congress might consider enacting statutory hot-pursuit authority that would permit the Intelligence Community to continue Section 702 targeting of a non-U.S. person that has entered the United States for a time-limited initial period—perhaps 72 to 120 hours (*i.e.*, 3-5 days) so long as (a) the target was lawfully targeted under Section 702 immediately prior to entry; (b) the foreign-intelligence purpose and the no-reverse-targeting prohibitions remain in force; (c) the Attorney General, Deputy Attorney General, or Assistant Attorney General for National Security certifies the need for continuation; and (d) the FISC is notified within twenty-four hours of such certification. Likewise, Congress might also consider an expedited FISC review mechanism for the conversion of such hot-pursuit collection into a traditional Title I order but without the use of the aggressive penalty provisions currently applicable to traditional EAs.

A properly calibrated hot-pursuit authority would close an intelligence gap that, today, is addressed only by operational improvisation and working through legal constructs designed for an entirely different era.

Another approach Congress ought consider when looking at the overall FISA construct, including Section 702, is whether it is time to look at the question of what constitutional rights with respect to government surveillance foreign national present in the United States might have (i.e., not a U.S. citizen or legal permanent resident who have the full protection of the Constitution and the right to a Title I FISA order globally under existing law). In doing so, Congress might consider whether a court would assess such rights in the context of whether such an individually has come here legally (e.g., on a visa, etc.) or illegally. Having looked at that question, and depending on what rights such an individual is assessed to have, Congress might reasonably consider whether the current statutory regime is the right one (where physical presence in the United States is a primary consideration for the protection of FISA) or whether such individuals ought have more limited rights either as a condition of their visa or as a result of having arrived in the United States illegally. Such a regime, if properly conceived, might remove the question of the location of the target as a key metric and instead focus on the status of the individual. Of course, appropriate consideration would have to be given to how a court would examine this question, particularly in a scenario where information collected under any such new authority might be used in the criminal context. Such a framework does seem to fit closely, however, with the original construct of FISA, which was designed to safeguard the constitutional rights of Americans and provide appropriate privacy and civil liberties protections for American citizens and lawful permanent residents, not principally to protect foreign nationals, whether in the United States or abroad.

V. Getting on the Offense on Collection, Counterterrorism, and Counterintelligence

One of the biggest challenges the IC has faced in the recent post-9/11 environment has been how to pivot ourselves from the largely defensive posture we are in today to more of a forward leaning approach on counterterrorism. To be sure, in the immediate aftermath of 9/11, we were certainly on the offense overseas, whether in Afghanistan or elsewhere around the globe under the rubric of the Global War on Terror. For a solid two decades, we kept a strong version of that pressure up, primarily limiting our operations domestically to defense while staying on the offense abroad. This effort was largely successful and kept us relatively safe at home with AQ and ISIS largely on the run overseas. However, as the war in Afghanistan wore on, and given the ups-and-downs in the Iraq theatre from the successful initial intervention, through the Shia and Sunni militias, and the rise of ISIS (and the fall of its notional Caliphate), as well the activities of AQIM, Boko Haram, and al Shabab in Africa, and the rise and growth of the AQAP and the Houthis in Yemen, the U.S. public over time has appeared to tire of these operations and the political system has responded with withdrawals of forces and a seeming reduction in offensive operations.

However, in today's increasingly multipolar world, as noted above, we face a broad range of threats from not just from terrorists, but from nations like China, Russia, Iran, North Korea, and a wide range of non-state actors (some at the behest or with the sponsorship of nation-states, admittedly) seeking to degrade American interests and our security across the physical, economic, cyber, and information domains. If we are to stay ahead of the counterterrorism threat and other national security threats, we must remain on the offense, even if we have largely tired of the Global War on Terror because, without a doubt, our enemies are watching and waiting for us to let our guard down.

To that end, in my view, there is value at this juncture, nearly 25 years removed from the 9/11 attacks, to consider providing the IC with new authorities and resources to: (1) engage in more proactive collection against emerging terrorist organizations and adversary intelligence services, including in places and against targets where we might otherwise have been more cautious in the past; (2) impose significant costs on aggressive adversary intelligence services through sanctions designations, public exposure, cyber operations under one or both of Titles 10 and 50, targeted expulsions and indictments, and asset seizures; (3) affirmatively degrade adversary capability including Chinese, Russian, Iranian, North Korean, and terrorist capabilities in the cyber, AI, biotech, UAS, and HUMINT domains through a portfolio of actions that may include offensive cyber operations, supply-chain interdiction, financial-sector pressure, and HUMINT-enabled denial and disruption; (4) shape the global information environment in ways that disadvantage adversary narratives; and (5) integrate defense, diplomacy, intelligence, law enforcement, economic, and informational efforts in order to achieve these goals.

VI. Counter-Intelligence Programs

Specifically, on counterintelligence, it is worth noting we face a significant and ongoing threat here at home. The Chinese government is actively operating against our government in the United States through a range of mechanisms, from classic espionage to cyber-enabled operations, including IP theft costing the United States trillions in lost research and development dollars. Back in 2022, then-FBI Director Chris Wray noted the "Chinese government steals staggering volumes

of information and causes deep, job-destroying damage across a wide range of industries" requiring the FBI to open a new China-related counterintelligence case approximately every twelve hours.[57] Likewise, we know that the Russian[58] and Iranian[59] intelligence services continue to operate against the United States, including through cutouts and proxies, and smaller players like Cuba are effectively getting in the game as well.[60]

The combined effect of these CI threats makes them of a potentially larger magnitude than we have faced since the Cold War. The Chinese government's efforts alone—including their efforts targeting Chinese nationals here through police stations and using their students as assets—are massive.[61]

The challenge that our counterintelligence enterprise faces is that, having made the decision to place our principal CI authorities and operational capabilities in the FBI's Counterintelligence Division, we have largely isolated them from the bulk of the U.S. national-security apparatus. This was, in part, intentional to protect the security of those investigations. However, that separation is less effective in a world of deep and broad-based CI threats. While the National Counterintelligence and Security Center (NCSC) today performs a coordination, analysis, and policy function, it could do more. Our approach to CI today is perhaps too reactive, identifying and prosecuting assets, but taking place principally after the damage has already been done, in much the same boat as our counterterrorism posture was pre-9/11.

As the Committee looks deeper into this issue, it may make sense to have the NCSC stand up a (more) robust National Counterintelligence Operations Center, with FBI, DOW, State, DHS, CIA, and DOJ all co-located at senior levels to better coordinate efforts; under this construct, FBI would remain in the lead, but NCSC would serve in a coordinating and convening function. It might also make sense to take a page from the NCTC and assign NCSC a stronger role in strategic operational planning on CI issues across the government, and to work with key stakeholders to create potential campaign plans using a range of authorities and resources from across the government.

It may also make sense to embed more FBI, DoD, IC, and State Department CI officers in the National Vetting Center and in the screening enterprise more broadly, given that the immigration and visa screening functions are critical CI-enabling activities, and because the current

---

[57] *See* Christopher Wray, *Countering Threats Posed by the Chinese Government Inside the U.S.* (Jan. 31, 2022), *available online at* <https://www.fbi.gov/news/speeches-and-testimony/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122>.

[58] *See, e.g.*, Immigrations & Customs Enforcement, *Russian Citizen Arrested After HSI Investigation into Illegal Exportation of US-Sourced Microelectronics* (Sept. 17, 2024), *available online at* <https://www.ice.gov/news/releases/russian-citizen-arrested-after-hsi-investigation-illegal-exportation-us-sourced>.

[59] *See, e.g.*, Peter D'Abrosca, *Air Force intel vet Monica Witt allegedly spiraled into Iran's terror underworld*, New York Post (May 17, 2026), *available online at* <https://nypost.com/2026/05/17/us-news/air-force-intel-vet-allegedly-spiraled-into-irans-terror-underworld/>.

[60] *See, e.g.*, David C. Adams, *The Puzzling Story of Manuel Rocha, U.S. Diplomat and Secret Agent for Cuba*, Foreign Service Journal (Mar. 2025), *available online at* <https://afsa.org/puzzling-story-manuel-rocha-us-diplomat-and-secret-agent-cuba>.

[61] *See, e.g.*, Brit McCandless Farmer, *How China recruits its spies in the U.S.*, CBS News (Aug. 31, 2025), a*vailable online at* <https://www.cbsnews.com/news/how-china-recruits-its-spies-in-the-us-60-minutes/>.

organizational approach to screening may not adequately address CI concerns. Non-American travelers, students, researchers, businesspersons, and other entrants who present elevated CI risk should also be flagged through real-time screening processes that can operate at scale.

Finally, it may make sense to allocate significantly more funding to the CI enterprise, including but not limited to at the FBI, and to ensure that a significant portion of these new resources are going to ensuring that we have enough cleared CI agents at both the FBI and other relevant government agencies. Likewise, some of this funding should be specifically allocated to ensuring the FBI is deepening intelligence sharing relationships on CI issues with state and local law enforcement, critical-infrastructure owners and operators, major research universities, and key critical U.S. private-sector entities, particularly in the technology sector.

VI. AI & the Intelligence Community

In my view, the AI revolution—that has primarily been focused here in the United States—is creating a massive set of opportunities for Americans and our allies, and if we create the kind of security capabilities around it that give Americans and our industry the confidence to broadly adopt, it has the potential to be a massively transformative opportunity for our nation writ large, serving as a tide that raises all boats, creating new innovation and capabilities, upskilling workers across a broad range of industries, and freeing innovators create even more productive tools into the future.

This opportunity is also available to our national security community, including the IC, and it is my view that we should sprint towards that opportunity. Specifically, the potential for AI-enabled technology and tools to provide for significantly better detection of potential terrorist plots is massive. The IC has, over the course of decades, accumulated vast quantities of foreign-intelligence information, far more than any group of human analysts could possibly process or correlate. This data comes in a variety of forms, from SIGINT, IMINT, GEOINT, HUMINT, MASINT, and OSINT, to name just a few. Overcoming the key bottleneck of processing, analysis, and dissemination to consolidate and analyze all this data is a critical challenge that that cutting-edge AI capabilities are well-positioned to address.

Specifically, AI capabilities can enhance our ability to analyze signals and other intelligence gathered through a range of sources and can potentially provide the ability to take highly classified information—even compartmented data—and derive insights that can be delivered at varying levels of classification without revealing sources and methods.

To do effectively, however, it will be critical for the IC to work directly with the investors, innovators, companies, organizations, and academics that are on the cutting edge of these innovations to help ensure that we are baking in the kind of trust and security capabilities that will provide confidence to use such tools in highly classified environments at scale; this includes ensuring that tools to be used by the IC are built using secure-by-design principles, implemented in a fully auditable manner, and take advantage of the latest capabilities in AI security and explainability.

XI. The Right Way to Think About Intelligence Appropriations

In looking at Congressional reform, the 9/11 Commission recommended Congress consider establishing either a joint bicameral committee for intelligence or individual House and Senate committee with both authorizing and appropriations authorities.[62] While neither of these approaches was implemented at the time, it may be worth once again looking at this issue, particularly given the unique "select" nature of both the House and Senate Intelligence Committees and the success these committees have enjoyed in creating an expert cadre of members focused on intelligence issues.

A third approach that might also be worth considering is establishing an Intelligence Appropriations Subcommittee under the existing Appropriations Committee structures in the House and Senate, respectively. Such a structure would have benefit of maintaining the separation of authorizations and appropriations as for other government programs, as well as maintaining the relative status quo of the current committee structure but simply separating out intelligence programs from defense. Given that the top line intelligence budget is often declassified, this should not present significant classification issues as the committee could simply submit its appropriations amounts and programs in classified for, like the budgetary portion of the intelligence authorization bill. Under such a structure, strong consideration should be given to drawing the leadership and members of such an appropriations subcommittee solely or principally from HPSCI and SSCI membership.

XII. Conclusion

Thank you for the opportunity to testify before this Committee's critically important bipartisan 9/11 Commission Review. I look forward to the opportunity to answer your questions.

[62] *See 9/11 Commission Report*, *supra* n. 2 at 419-20.