TESTIMONY OF

Ken Wainstein
Under Secretary
Office of Intelligence and Analysis
U.S. Department of Homeland Security

BEFORE THE

U.S. House of Representatives
Committee on Homeland Security
Counterterrorism, Law Enforcement, and Intelligence Subcommittee

AT A HEARING ENTITLED

"Persistent Challenges: Oversight of the Department of Homeland Security's Office of Intelligence and Analysis"

June 26, 2024

Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the Subcommittee, thank you for the opportunity to discuss the current activities of the Office of Intelligence and Analysis (I&A) in the Department of Homeland Security (DHS or Department). It is an honor to share with you the hard work of I&A's dedicated employees, who tirelessly serve and protect our Nation.

For background, I have served as the Under Secretary for Intelligence and Analysis since June 2022. Prior to this role, I spent over 20 years in law enforcement and national security in the federal government, including as a federal prosecutor in both the Southern District of New York and the District of Columbia, as the Director of the Executive Office for U.S. Attorneys, as General Counsel and then as Chief of Staff of the Federal Bureau of Investigation (FBI), as the U.S. Attorney for the District of Columbia, as the first Assistant Attorney General for National Security, and as Homeland Security Advisor for President George W. Bush. I subsequently worked in private legal practice and served on the Bipartisan Commission on Biodefense before being given the opportunity to return to public service as the leader of I&A.

Today, I will provide an update to my last testimony before this Committee from December 2022, with a focus on the organizational improvements, mission prioritization, and functional adjustments that are driving progress at I&A. First, I find it is helpful to begin with a brief overview of I&A, its founding, and its core missions because that context clarifies why the changes we are making today are so critical. Then, I will walk through the three stages of our 360 Review—which is the top to bottom organizational assessment that we started shortly after I joined I&A.

Now more than ever, I&A is in a state of positive change. We are adapting to address the current threat environment while ensuring we always act with full respect for the privacy, civil rights, and civil liberties of the American people.

I. THE MISSION

I&A was established specifically to address the intelligence gaps exposed by the terrorist attacks of September 11, 2001 (9/11). As numerous experts and entities—like the 9/11 Commission—examined and diagnosed the gaps that allowed the attacks to happen, Congress undertook the task of building a federal apparatus to address those gaps and develop a stronger domestic intelligence capacity. I&A was established as a critical part of that apparatus and was tasked with developing a national intelligence network and sharing information with our federal and other homeland partners under authorities and limitations designed specifically for the sensitivities of conducting intelligence activities in the homeland.

In service of that goal, we at I&A serve three core missions:

- First, to build and maintain an intelligence program within the United States that can detect and prevent threats to the homeland.

- Second, to serve as an information-sharing bridge between federal law enforcement and intelligence agencies and our state, local, Tribal, territorial, and private sector partners (SLTTP).

- And third, to operate with an intensely focused regard for privacy and civil liberties, which is a mission that is completely on par with the other two.

We emphasize these missions with the recognition that homeland security can be achieved only in conjunction with the protection of privacy and civil liberties, and that both objectives can and must be pursued at the same time. As someone who spent the better part of 15 years as a federal prosecutor, this dual mission is not a foreign concept. Just as I had a sworn and equal duty as a prosecutor to both pursue conviction of the guilty and protect the rights of the accused, we at I&A have a sworn and equal duty to both prevent threats to homeland security and protect against incursions into our rights and freedoms. With that duty in mind, my I&A colleagues are building the foundational elements of transparency, civil liberties, and privacy into our intelligence tradecraft in the domestic operating environment.

II. 360 REVIEW AND ORGANIZATIONAL IMPROVEMENTS

Upon my confirmation, Secretary Mayorkas asked me to conduct a "360-degree review" of I&A and its operations, with a focus on privacy and civil liberties safeguards. We immediately undertook that comprehensive operational review, building on the work of my predecessor John Cohen, who had taken important steps to strengthen oversight functions after compliance concerns arose in 2020. We brought in four senior advisers with extensive backgrounds in intelligence and intelligence oversight—Central Intelligence Agency (CIA) and Hill veteran Steven Cash, former DHS General Counsel Stevan Bunnell, former National Counterterrorism Center Director Russ Travers, and, later, former DHS Inspector General John Roth. They helped me in consulting with both outside experts and internal I&A personnel to provide input on the direction of I&A. This 360-review has involved a rigorous and probing process to examine I&A's structure and mission, with the goal of providing mission clarity and ensuring we focus our operations and resources on areas that add the most value to the homeland security enterprise.

The 360-review encompassed three primary stages of prioritization, which I will explain in detail. They are (1) organizational prioritization, (2) topical prioritization, and (3) functional prioritization. All three stages have yielded structural and operational improvements that have significantly increased our ability to execute I&A's core missions.

Stage 1: Organizational Prioritization

This first stage of our 360-review focused on a reorganization of I&A's top-level structure. Through this process, we signaled our prioritization of certain critical operations with the creation of new organizational structures to lead and support them. This included (1) creating the Transparency and Oversight Program Office (TOPO), (2) separating the management of our collection and analysis operations, and (3) establishing the Intelligence Enterprise Program Office (IEPO) and reinvigorating the Department's counter threat coordination through the

Homeland Security Intelligence Council (HSIC) and the Counter Threats Advisory Board (CTAB).

1. Establishing the Transparency and Oversight Program Office

To lead our mission to protect privacy and civil liberties, and to signal the centrality of this mission to all our activities, we created a new Transparency and Oversight Program Office led by a highly respected veteran DHS attorney, Andy Fausett, who reports directly to me and the Principal Deputy Under Secretary for Intelligence and Analysis. This new office unites all the transparency and oversight functions that were previously dispersed throughout the organization—the eight members of the Privacy and Intelligence Oversight Branch, the personnel handling Freedom of Information Act (FOIA) requests, congressional oversight, and Government Accountability Office (GAO) and Inspector General inquiries, and the organizational ombuds—and elevates their role within I&A. We now have a strong voice for oversight and compliance in all our front office decision-making and policy conversations, which has been absolutely critical over the past year as we have considered and implemented additional changes and reforms to the organization.

a. Guidance Improvements Under TOPO:

TOPO has been heavily engaged in drafting guidance for our collectors and analysts. That guidance has been particularly important for our intelligence efforts directed at domestic violent extremists (DVEs) and homegrown violent extremists (HVEs) inspired by foreign terrorist organizations who have engaged in violence in reaction to recent sociopolitical and geopolitical events. The volume and frequency of threats to Americans, especially those in the Jewish, Arab American, and Muslim communities in the United States, have increased, raising the prospect that violent extremists and lone offenders could target these communities. It is critical for our intelligence professionals to examine these threats, and it is our job to give them the guidance to conduct this mission.

TOPO is focused on providing that clear guidance to our collectors and analysts on the handling of speech that may be constitutionally protected. This guidance is critical, especially in relation to threats like domestic terrorism, where so much of the information about potential violence comes from speech that fall squarely within the core protections of our First Amendment.

b. Oversight Improvements Under TOPO:

Former DHS Inspector General John Roth recently joined TOPO as a Senior Advisor for Compliance and Oversight. John is helping I&A strengthen its compliance and oversight programs to better ensure robust adherence to legal and policy requirements and best practices. This work will, in turn, enhance the quality and speed of I&A's responses to external oversight entities like the GAO and the Department's and Intelligence Community's (IC) Office of Inspector General.

c. Policy Improvements Under TOPO:

Due to TOPO's strong performance to date, we have recently decided to move I&A's policy coordination and oversight function to that office. Better tailored and more routinely updated policy is essential to the maturation and oversight of I&A's operations, and we believe TOPO is uniquely positioned to ensure that policy development is fair, transparent, thoughtful, and timely. The oversight from TOPO will ensure that all I&A intelligence policies, existing and future, fully protect privacy and civil liberties.

2. Establishing the Office of Collection and the Office of Analysis

As part of the organizational reprioritization, I&A separated the management of collection and analytic functions, establishing a Deputy Under Secretary for Collection to work alongside the Deputy Under Secretary for Analysis. This increased the supervisory attention dedicated to both disciplines, which require distinct methods of management and supervision, particularly with respect to the protection of privacy and civil liberties. I&A veteran Jim Dunlap has taken the helm of Analysis and, to lead Collection, we brought in a highly respected 20-year veteran from the CIA who has brought an increased level of rigor to those operations. With this new management structure in place, we now have the focused management we need both to enhance the utility and quality of our analysis and to provide constant, hands-on supervision of our collection activities, which so directly implicate privacy and civil liberties concerns in the Homeland.

3. Enhancing Coordination of the Intelligence Enterprise

As we re-examined the organizational structure of I&A, the Secretary directed the DHS Counterterrorism Coordinator, Nick Rasmussen, and me to assess the effectiveness of the mechanisms for coordinating threat intelligence and response across the Department's components and headquarters elements. That assessment resulted in several reforms to improve coordination and integration of the Department's intelligence activities as well as the threat policy and response functions that are informed by those activities.

a. Creating the Intelligence Enterprise Program Office:

We undertook to build a mechanism to strengthen, better coordinate, and oversee the efforts of the DHS Intelligence Enterprise, which is composed of the intelligence programs housed within the DHS components. In statute, the Under Secretary for Intelligence and Analysis—by way of their dual role as the DHS Chief Intelligence Officer (CINT)—has the authority to set policy for these offices and coordinate intelligence capabilities across DHS to enhance threat identification, mitigation, and response. In practice, I&A has not always had the resources, mandate, or organizational structure to fully execute this coordinating and strategic oversight role.

We created the Intelligence Enterprise Program Office (IEPO) to provide strategic, administrative, and functional support to the CINT and integrate intelligence policy making across DHS components. The office is led by Steve Cash and reports to the Under Secretary and

the Principal Deputy Under Secretary. IEPO is already having a significant impact. For example, IEPO has developed and implemented a budget request for the Intelligence Enterprise to improve resource management across the Department, as well as rigorous, repeatable, process for Enterprise-wide intelligence topic prioritizations. The latter process produces an annual document—the Intelligence Enterprise Intelligence Priorities Framework (IE-HIPF)—which will be modeled on the IC's National Intelligence Priorities Framework and uses the recently completed I&A priorities framework as a starting point. Our goal is to have the IE-HIPF in place to support Fiscal Year (FY) 2025 operations.

b. Enterprise Privacy and Civil Liberties Intelligence Product Reviews:

Working with TOPO, IEPO is sharing I&A's experience in the privacy and civil liberties space with the DHS Intelligence Enterprise. For over a decade, the DHS Office of the General Counsel (OGC), Privacy Office (PRIV), and Office for Civil Rights and Civil Liberties (CRCL) have reviewed I&A's finished analytic products disseminated outside DHS, ensuring compliance with applicable laws and addressing concerns related to the protection of privacy and civil liberties. This review process reflects the Department's commitment to protecting the American people while upholding our Nation's fundamental values. To build on the success of this model, the Secretary directed the creation of similar review processes for the external release of analytic products authored by other components in the broader DHS Intelligence Enterprise. While the specific process for review varies among the Component Intelligence Programs, each process ensures legal, privacy, and civil rights and civil liberties oversight.

c. Counter Threats Advisory Board:

At the direction of the Secretary, IEPO has worked with the Counterterrorism Coordinator to revise our approach to the Counter Threats Advisory Board (CTAB). First established and chartered by the Secretary as the Counterterrorism Advisory Board in 2010, the CTAB was reconstituted and renamed following the enactment of legislation in 2020 which, among other things, directed the USIA to Chair this advisory board comprised of the principals of all DHS components and headquarters entities. While the requirements of that legislation have since expired, the CTAB has endured with an expanded remit encompassing all threats within the Department's mission space, not just terrorism. To make the CTAB meetings more substantive and impactful, we have scaled back meetings to a quarterly schedule, while maintaining the ability to call snap meetings when warranted by a crisis or the emergence of a specific threat. As a result, the CTAB is now a more focused and directed forum for operational planning and decision-making on key issues, and has recently served as a critical coordinating force for the Department's response to threats such as transnational organized crime (TOC) and fentanyl.

d. Homeland Security Intelligence Council:

IEPO has also helped to reenergize the Homeland Security Intelligence Council (HSIC), which is composed of representatives from the intelligence elements of each DHS component, ie. each Component Intelligence Program (CIP). Within the HSIC are six functional boards: (1) Analysis & Production Board; (2) Counterintelligence & Security Board, (3) Career Force

Management Board; (4) Collection & Reporting Board, (5) Intelligence Systems Board, and (6) the Strategy, Planning & Resources Board, each of which is co-chaired by a representative from I&A and from a CIP.

IEPO's leadership has dramatically improved the operationalization of the HSIC, evolving it from a forum where components provided primarily rote updates to one for Enterprise coordination and actionable policy decision-making. Since October 2023, the HSIC has proposed plans to develop specific Intelligence Enterprise budget guidance; optimize and execute the Enterprise Homeland Security Intelligence Priorities Framework; standardize intelligence training; facilitate better access to originator-controlled information; and improve information sharing to combat counterintelligence threats to the Department, among other initiatives.

e. *Replacing the NTAS Bulletins:*

As a part of our reforms to the CTAB, we also reworked the National Terrorism Advisory System (NTAS), which was designed to communicate information about terrorist threats to the American public. NTAS reports were designed to describe DHS's assessment of the terrorist threat and the factors driving it, but in recent years, all the bulletins have stated that the terrorism level is "heightened." To increase its utility and value as a warning tool, we will henceforth reserve the NTAS system for situations where DHS needs to alert the public about a specific or imminent terrorism threat or a change in the threat level.

I&A will now provide a more general annual update on the threat environment—including the terrorism assessments that used to be conveyed through the NTAS—through the Homeland Threat Assessment (HTA). The HTA will serve as the homeland security counterpart to the Director of National Intelligence (DNI) Annual Threat Assessment, reflecting insights from across the Department, the IC, and other critical homeland security stakeholders to highlight the most direct, pressing threats to our Homeland during the next year.

Stage 2: Topical Prioritization - Homeland Security Intelligence Priorities Framework

The organizational reforms I have just outlined have created a solid foundation to refine the intelligence priorities that underpin I&A's mission.

The homeland security threat environment that we face today is arguably as complex and varied as it has ever been. With this diversity comes the additional challenge of triaging competing priorities and limited resources, to focus our efforts on those specific threats where I&A can uniquely contribute, whether that be through homeland-focused analysis, collection, or information sharing with SLTTP stakeholders.

For the first time in a decade, I&A produced last fall a Homeland Security Intelligence Priorities Framework (IA-HIPF)—a prioritized list of national and departmental intelligence topics that will serve as an overarching strategic document for all our intelligence operations. This is the product of an in-depth assessment of the missions where I&A provides unique contributions to the national and homeland security communities, and involved multiple "deep

dive" sessions with I&A managers; engagement with I&A's field personnel and SLTTP partners; and outreach to Congress. Guided by the priorities of the DNI, the Secretary of Homeland Security, and our homeland security partners, this engagement resulted in lists of threat topics within the homeland security mission space. We then then applied the following criteria to rank the topics:

1. *Priority 1:* These are topics for which no other department or agency provides intelligence support, or topics where I&A makes unique contributions distinct from the work of other departments and agencies. The Secretary's priorities are also a significant factor in determining whether a topic is critical.

2. *Priority 2*: These are topics receiving intelligence support from other departments or agencies, but not to the extent or in the manner needed by I&A's stakeholders.

3. *Priority 3*: These are topics receiving intelligence support from other departments and agencies where I&A's support would have only marginal additional value.

The IA-HIPF informs our Program of Analysis (POA) and Operating Directive (OD), the annual strategic documents that guide our analytic and collection efforts, respectively. Together, the IA-HIPF, the POA, and the OD focus our efforts on the most pressing threats and help our partners understand the threat areas where I&A is best positioned to provide unique contributions.

Specifically, the IA-HIPF has helped to clearly articulate the scope of our intelligence missions and activities; to seek, justify, and allocate resources; to ensure that our efforts match customer needs inside and outside of DHS; and to manage our workforce, direct action, and measure our performance. The IA-HIPF will be updated at least annually to reflect changes in the threat environment and national and departmental priorities.

As I previously mentioned, I&A is currently organizing a similar prioritization process for the DHS Intelligence Enterprise to better coordinate collection and analysis activities and align them with Departmental missions and objectives.

Stage 3: Functional Prioritization

The final step in our 360-review has been the prioritization of the functions we perform in the course of our intelligence work. This effort has included cataloguing all the duties we perform and examining their relevant importance to our mission against four operating principles that have guided our decision making throughout this process. Those principles are:

1. *Focus on servicing the intelligence needs of our SLTTP partners*: Congress made clear that we are the federal agency with primary responsibility to share intelligence with and among our SLTTP partners across the country. As such, our intelligence work should be primarily guided by the homeland security needs of those customers.

2. *Focus on producing strategic-level intelligence*: Our greatest value to the national intelligence enterprise is the delivery of strategic—as opposed to tactical—intelligence that provides decisional advantage to our SLTTP partners and helps them prepare for and meet the current homeland security threats in their areas of responsibility. That is the intelligence gap that I&A was established to fill. In the domestic context, the tactical intelligence work is better left to our federal, state, and local law enforcement partners whose investigative work focuses on individual threat actors. While it is inevitable that some of our intelligence work (especially on the collection side) will relate to tactical information about individual threat actors and their activities, we should focus on providing intelligence that illuminates the broader threat patterns and trends that our partners should be prepared to confront and doing so at the lowest classification level possible to maximize its accessibility and consumption by SLTTP partners.

3. *Focus on leveraging unique capabilities:* In prioritizing our functions, we endeavor to focus on areas where I&A and DHS can contribute unique capabilities and distinct operational advantages. It is for this reason, for example, that we prioritized topics in the IA-HIPF, POA, and OD based on how well we could collect on and analyze that topic relative to other agencies.

4. *Focus on building our internal management:* As a relatively young agency with a broad mission, it is critical that we continually focus on measures that enhance I&A's management capabilities, provide support to the workforce, and promote I&A's growth into a more mature and effective intelligence agency.

We applied these four principles in every stage of our functional reprioritization process, which has resulted in approximately 30 functional and organization initiatives across I&A, detailed in the April 9 memorandum entitled "Direction Regarding the Recommendations from the I&A 360 Review," which I&A shared with Congress. I will highlight some of the more significant initiatives here:

1. Field Realignment

I&A recently announced a realignment of its field posture to bolster management and connectivity with headquarters, to improve intelligence support to our SLTTP partners, and to enhance information sharing and integration with other components of DHS.

The realignment makes four key changes to I&A's Field Intelligence Directorate. Specifically, it will—

- Create four divisions within the Field Intelligence Directorate to provide leadership and oversight of I&A's field presence; increase connectivity across the directorate, I&A leadership, and other DHS Components; and relieve field staff of significant administrative, human resources, logistics, security, and information technology demands;

- Realign I&A's existing 12 field regions into 10 regions, consistent with the regional structure used by other DHS Components, and tailor the internal management structure to

provide consistent levels of supervision and oversight in each region;

- Clarify roles at the individual field officer level to improve mission focus, professional development, and accountability; and

- Add functional leaders and compliance staff to ensure field activities focus on the most pressing threats while adhering to IC and departmental policies and protecting individuals' privacy and civil liberties.

Importantly, the realignment will collocate I&A field offices with those of other DHS Components. Collocation of office space and secure workspace across DHS Components will increase collaboration and information sharing, and ultimately result in greater efficiency and cost savings in the long run.

2. Field-HQ Rotational Program

To promote cohesion between the field and headquarters and better integrate field personnel into overall I&A operations and strategy, we will initiate a program for bringing field personnel into I&A headquarters for details of varying lengths starting later this year. We plan to expand the program and require field personnel to serve such a detail beginning in fiscal year 2025. Simultaneously, we will develop a TDY program for headquarters analysts and collectors to complete rotations to the field to increase their exposure to and understanding of field operations.

3. Overt Human Intelligence Collection: Focusing on the Border

In our Overt Human Intelligence Collection (OHIC) Program, we have undertaken an in-depth review of its policies, rules, and procedures to ensure they provide the level of governance and oversight needed for such a sensitive area of operations, as well as an assessment of how the program can provide the most utility for the Department and our partners.

We found that the program has been exceptionally valuable for our mission at the border. Since 2021, I&A has provided intelligence support for CBP security operations, conducting over 200 overt, voluntary interviews of special interest migrants that have led to 1) a half-dozen referrals to the FBI Joint Terrorism Task Forces for further investigation, 2) the production of over 400 intelligence information reports, and 3) the initiation of several successful law enforcement operations against human smuggling networks.

To build on that success and leverage our relationship with DHS components with border enforcement responsibility, we will now largely focus our field interviews on individuals with information about border security-related threats (such as fentanyl supply chain networks, human trafficking and narcotics smuggling), and in particular on the interviews of detained migrants of homeland and national security interest that we conduct in coordination with CBP along the southwest border. Those interviews generate raw intelligence reporting that provides information about the illicit narcotics trade, human smuggling, TOC and other cross-border threats—reporting that is not conducted by any other intelligence agency outside DHS. While the field

may still submit operational proposals for other field interviews, the majority of this program will be focused on border-related issues.

4. Open-Source Intelligence

The I&A open-source intelligence (OSINT) collection program has also yielded valuable information in support of our national and departmental missions. For example, we have utilized OSINT capabilities to understand how human smugglers communicate with migrants on social media and to identify U.S. schools and businesses targeted by foreign governments for espionage or transnational repression activities.

a. Embedding Collectors in Analytic Mission Centers:

We have recently conducted a review of our OSINT program and identified several adjustments that we believe will increase the relevancy of collection to both analysts and SLTTP partners. First, we have decided to move our OSINT collection staff from their current office at the DHS St. Elizabeths campus to the Nebraska Avenue Complex (NAC) to work more closely with I&A's analysis and collection management personnel. And second, OSINT staff will functionally integrate within I&A's analytic mission centers to better align priorities and improve the utility of collection to finished intelligence production. Collection staff will continue reporting to the Deputy Under Secretary for Collection, but by eliminating physical and organizational silos, analysts and collectors will have more opportunities for collaboration and alignment.

b. Focusing on Strategic Intelligence:

Our goal is to recalibrate our open-source collection efforts to better support strategic intelligence analysis. In recent years, there has been movement toward more tactical-level open-source collection as we have increasingly tasked our collectors to report on unfolding threat situations. There have been numerous occasions where we have asked them to search, collect, and provide warnings about the possibility for violence developing around events of heightened tension, ranging from the January 6, 2021, attacks on the Capitol to the reaction to the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, and the mass gatherings in the aftermath of the October 7, 2023, Hamas attacks in Israel.

For a number of reasons, the OSI collectors are not well postured to perform that tactical warning function. First, they operate with strictly constrained authorities, in that they can only collect publicly available information and cannot misrepresent themselves to access certain chatrooms or types of communications. Second, OSI is a very small unit, and it lacks the manpower needed to conduct the kind of wide-ranging internet search that is often necessary to identify threats in a period of heightened tensions. Finally, OSI has now been further constrained in dealing with domestic terrorism threats as a result of language in the National Defense Authorization Act for FY 2024 (NDAA) that limited our open-source cadre collecting on the domestic terrorist threat to a handful of collectors.

On those occasions where OSI has been asked to do this tactical collection, it has done so in parallel with the FBI. The FBI is similarly called upon to provide warnings in times of heightened tensions, but unlike I&A, it has investigative collection authorities that permit more intrusive search techniques upon sufficient predication. In light of our limited authorities and the statutory limit on our manpower, we are simply not as well positioned to effectively perform tactical open-source threat reporting. Instead, we will focus our open-source collectors on collection that supports our strategic intelligence priorities as they embed in the analytic centers. To preserve some tactical-alert capability in support of internal DHS needs and requests, we will retain a group of contract open-source collectors—under an OSI supervisor and subject to OSI policies—with the Intelligence Watch at the St. Elizabeths campus.

While we will carry out our OSINT collection in the more limited fashion set out above, we maintain broader concerns about the government's ability to conduct the open-source collection that provides warning about looming threats. We therefore urge Congress to re-examine the allocation of resources and authorities for this critical function. This re-examination may ultimately call for a substantial enhancement of the government's OSINT effort, given its critical role in threat warning.

5. Analysis

a. Strengthening Analytic Production:

Our Analytic Advancement Division has already made significant strides in improving both the quality of our products and their utility to our consumers—and it shows in the feedback we receive on our products. To build on that progress, the Deputy Under Secretary for Analysis is implementing a new process to measure and establish benchmarks for our intelligence output and the feedback from our customers. We plan to leverage this data to reassess the allocation of our analysts within mission centers and ensure our posture is tailored to cover near-term Departmental priorities and needs.

As one example, I&A has clearly displayed the quality of its work and the agility of its operations in its response to the horrific attacks on October 7, 2023, and the ensuing conflict between Israel and Hamas. Through the New Year, I&A produced daily situational reports about the conflict and its homeland implications for DHS leadership and our partners to ensure homeland security stakeholders had accurate and timely information to make decisions, and we continue to produce similar weekly situational reports. I&A has also published several products jointly with the FBI and the National Counterterrorism Center (NCTC), including an initial Public Safety Notification on October 7, followed by a Liaison Information Report for private sector customers, a Public Service Announcement, and multiple Joint Intelligence Bulletins, the most recent of which focused on threats to Jewish communities in the United States and abroad. Our subject matter experts also participated with FBI and NCTC in national threat calls with state and local customers to communicate the state of the homeland threat environment from a variety of threat actors including foreign terrorist ideologies, violent extremists inspired by foreign terrorist organizations, domestic violent extremists, and cyber actors. I&A continues to partner with IC counterparts to anticipate potential threats stemming from the heightened tensions surrounding the conflict.

b. SLTTP Fellows Program:

To ensure our analysis is tailored to the needs of SLTTP stakeholders, we are reestablishing our SLTTP fellows program to create an analytic cell at I&A staffed by analysts detailed from our SLTTP partners. This cell will produce focused products to answer our partners' most pressing security questions, and work with other analysts at I&A to help them better understand our most critical audience. This effort will also help to ensure critical information at the classified level is reviewed by SLLTP stakeholders and tailored at the unclassified level for broader dissemination.

c. Leveraging Investigative Case Files:

Consistent with our reorientation toward strategic-level intelligence, we will focus on producing strategic intelligence products based on the investigative holdings of our law enforcement partner agencies. Although it has long been recognized that the information in criminal investigative files can be an important source of strategic intelligence about our homeland security, various historical obstacles have prevented that information from being fully leveraged for strategic intelligence purposes. To address that situation, we are now participating in two pilot programs that will have our analysts reviewing and generating intelligence products from the case files of our law enforcement agency partners. First, as part of the Department's counter-fentanyl campaign, our analysts and reports officers are working closely with Homeland Security Investigations (HSI) to review fentanyl investigation files and generate products with actionable intelligence for our federal and SLTT partners, while protecting sensitive investigative methods and information as well as individual privacy and civil liberties. In addition, we are developing a similar arrangement with the FBI, whereby our analysts will embed with FBI analysts, have access to FBI systems, and generate intelligence products regarding domestic terrorism-related patterns and trends under the strict controls necessary to protect such sensitive investigative information. With Congress prohibiting NCTC from producing analytic products about domestic terrorism threats that lack a foreign or international nexus, it is all the more important that we work with the FBI to make sure that the information in its domestic terrorism case files that could prevent or mitigate attacks is reviewed and turned into actionable strategic intelligence for our SLTTP partners.

6. <u>Improving Management and Supervision</u>

a. Training and Development:

I&A recognizes that any progress we achieve is due to the dedicated efforts of the hardworking individuals who make up our workforce, and that our most important job as leaders is to ensure our people have the resources, support, and direction to execute their role to the best of their ability. To that end, I&A is continuing to implement new initiatives to improve the support and supervision of our employees. For example, we are developing a comprehensive New Managers Orientation Program to develop foundational supervisory competencies and management best practices. In tandem, we are also creating a Future Leaders Roadmap to develop existing managers, an Aspiring Managers Program to prepare I&A's rising talent for

supervisory roles, and new mentorship programs to provide additional professional development at all levels of the workforce.

These programs expand upon our management team's strong work over the last two years. During that time, we established a New Hire Orientation Program and delivered the course to over 200 new employes; facilitated approximately 34,000 online trainings through our new Intelligence Learning Management System; and delivered over 150 additional courses to more than 3,500 students through I&A's Intelligence Training Academy. We also developed oversight training that covers I&A's authorities, the Intelligence Oversight Guidelines and whistleblower protections, and brought on two full time Ombuds to help our workforce raise concerns with management. To hear from our workforce directly, we also implemented an advanced analytic employee feedback survey about the management and work environment of I&A's centers and divisions.

b. Telework Policy Changes:

In response to the COVID-19 pandemic, I&A instituted a telework policy in 2021 that provided I&A staff with telework opportunities according to their work position and responsibilities. While this policy was an appropriate means of affording staff with locational flexibility, it exacted a cost in terms of workforce cohesion and the effectiveness of the supervision, training and mentoring that is often best carried out in person.

Pursuant to direction from the DHS Management Directorate, and after careful review of various considerations, in April we adopted a new telework policy for I&A that generally reduces the amount of time our workforce may telework. This change is already increasing collaboration across our personnel and improving supervisory support for our workforce. The new policy provides that designated Senior Telework Officials, consisting of I&A senior staff who report to the Under Secretary and the Principal Deputy Under Secretary for Intelligence and Analysis, will determine telework eligibility based on mission requirements, required access to classified information, collaboration and operational needs, position responsibilities, and other factors. Given their responsibility to support other staff, supervisors and those designated in leadership positions will generally be eligible for less telework than non-supervisory staff. This policy will also prohibit routine telework on the core days of Tuesdays and Thursdays each week, maximizing in-person collaboration across the entire I&A workforce on those days.

III. CONCLUSION

Around this time last year, we were engaged in a debate with lawmakers surrounding our collection authorities, and we are grateful to Congress for hearing out our concerns and working constructively with us to reach the agreement that was incorporated into the FY 2024 NDAA. Even before that law was passed, we immediately began issuing additional guidance for our workforce to address the concerns raised by Congress. And following the enactment of the NDAA, we have developed a series of new policies to ensure compliance with its restrictions and codify the best practices for our intelligence activities.

That is just one example of the many ways we have improved the rigor of our operations. Going forward, we want to continue engaging with Congress and developing solutions together. As I have said many times, I&A is in a state of positive change. Importantly, the workforce has proven itself very open to that change, and that is one of the many reasons I am proud to be part of I&A and counted among its professionals who do so much to protect our homeland security each and every day.

Thank you very much for the opportunity to appear before you today, and I look forward to answering your questions.