DEPARTMENT OF HOMELAND SECURITY

OFFICE *of* INTELLIGENCE *and* ANALYSIS

PROGRESS REPORT

2025

DEDICATION

IN MEMORIAM AND WITH APPRECIATION

Patrick M. Hughes

We dedicate this progress report to Lieutenant General Patrick M. Hughes, who passed away on October 5, 2024 after an illustrious and impactful career of public service. Pat grew up in a small Montana town before joining the Army in 1962 and serving in a variety of demanding assignments, including two combat tours to Vietnam at the height of that conflict, and earning numerous decorations and medals, including the Silver Star, multiple Bronze Stars for "V" Device for Valor, and a Purple Heart. After achieving the rank of lieutenant general, serving as the Director of the Defense Intelligence Agency, and then retiring after 37 years of Army service, Pat became the leader of the organization in DHS that ultimately became today's Office of Intelligence & Analysis (I&A). In 2003, he was appointed the Assistant Secretary for Information Analysis to oversee the Information Analysis and Infrastructure Protection Directorate, which was later named the Office of Intelligence & Analysis. Pat served with tremendous distinction in that role.

We are all indebted to Pat for his leadership during those critical years in I&A's history, and for his tireless efforts to build I&A into the strong organization that it is today. Even more importantly, we are indebted to him for the culture of selfless service that he personified and that he worked so hard to inculcate into the organization. Thanks to those efforts, duty and service are the enduring tenets of I&A's culture and we all continue to draw inspiration from the example that he set with his character and his passion for service.

MESSAGE FROM THE UNDER SECRETARY

I am proud to present this Progress Report for the Office of Intelligence & Analysis of the Department of Homeland Security. This report reviews I&A's efforts in furtherance of its mission to enhance intelligence sharing among our nation's federal, state, local, tribal, territorial, and private sector (SLTTP) partners. It traces the evolution of I&A since its inception in 2003, describes its current status, and explains where we are taking the organization in the future.

Since the Department was established in 2003, our Office has had the responsibility of sharing with leaders across our nation's states, cities, and industry sectors the intelligence about homeland threats that equips them to make critical security decisions in their jurisdictions. In the process of handling that responsibility over the years, I&A and its partners have built a domestic intelligence network where previously there was none, and have matured the concept of homeland security intelligence into what is now appreciated as a vital input to the larger national security picture.

In 2022, as we approached our twentieth anniversary, Secretary Alejandro Mayorkas asked us to conduct a "360 Review" of I&A with an eye toward considering any and all reforms that would better equip I&A to meet today's threats and the intelligence needs of our homeland security partners. We conducted that thorough review from 2022 to early 2024, and the result was a series of significant changes to I&A and its operations. As a first step, we clearly defined our organizational mission, which had been only vaguely described in our founding legislation and remained largely unclarified in the years since. With our mission clarified, we then undertook a comprehensive, three-stage process in which we fundamentally changed I&A's organizational scheme; reprioritized the threat areas we address in our intelligence operations; and revised our operational functions to better focus on our clarified mission. With that process complete, I&A is now better positioned to perform its domestic intelligence mission in defense of our homeland security.

Importantly, we perform that mission with an intensely focused regard for the principles of privacy and civil liberties, in recognition of the sensitivity around the conduct of intelligence activities within the United States. It is for this reason that much of our I&A 360 Review and the ensuing reform has been focused on building compliance and transparency into all facets of our operations. This organizational commitment to privacy and civil liberties is critical to the integrity of our operations and to building confidence among the American people that we uphold our obligation to protect both their safety and their rights.

I am extremely proud of the work of our organization and its dedicated staff over the past few years. Our objective with this Progress Report is to describe that exceptional work, highlight the progress I&A has made as an organization, and ultimately provide a clear assessment of I&A's capacity to meet today's homeland security challenges. We trust you will find that we achieve that objective in the following pages.

Kenneth L. Wainstein
Under Secretary for Intelligence and Analysis
Department of Homeland Security

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The mission of the Office of Intelligence and Analysis—to provide decisional advantage to homeland security leaders across the nation—evolved out of the 9/11 terrorist attacks. Our Office was established to fill the gaps in the nation's homeland intelligence capabilities that were laid bare by those tragic attacks and chronicled in various studies after the attacks. I&A was vested with three primary mandates:

- To build and maintain an intelligence network within the United States that can detect and prevent threats to the homeland;
- To serve as an information-sharing bridge between the federal law enforcement and intelligence agencies and our SLTTP partners; and
- To operate with an intensely focused regard for privacy and civil liberties, which is a responsibility that is completely on par with the other two.

I&A personnel have made remarkable progress in furtherance of this mission set since the organization's early days. In doing so, they demonstrated an impressive level of operational and bureaucratic ingenuity, often being called upon to develop and implement new tools, processes, and capabilities without any guiding precedent or applicable blueprints. The result has been significantly enhanced connectivity and intelligence sharing among our partners, which has, in turn, led to our significantly enhanced preparedness to meet threats to our homeland.

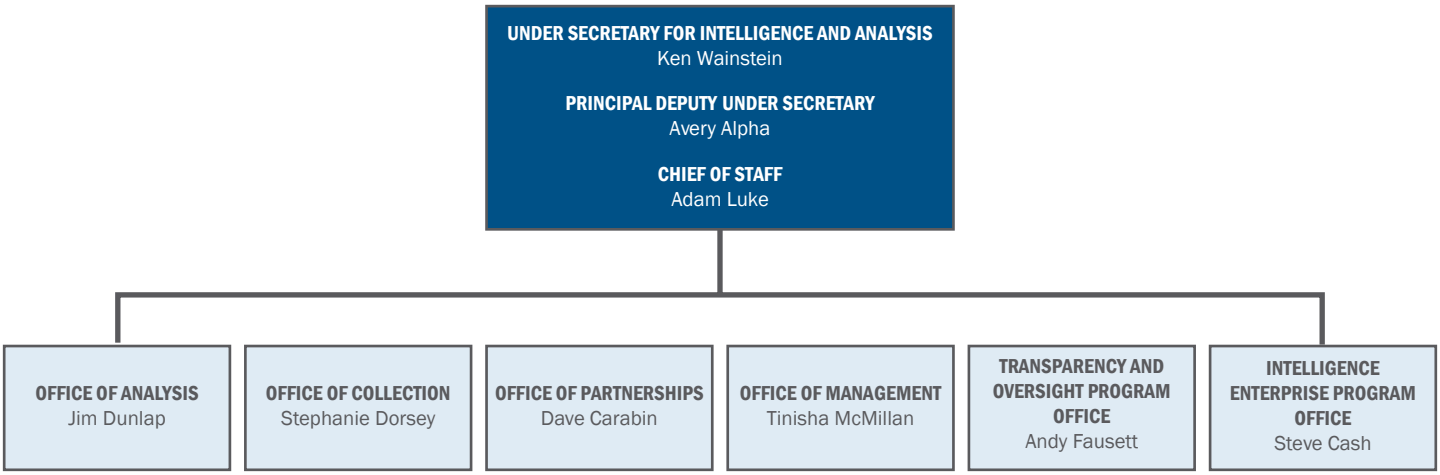
At the direction of Secretary Mayorkas, in 2022 we used the 20th anniversary of our organization as an opportunity to step back, reconsider our priorities, and reorient I&A's direction to better meet the threats of today and tomorrow. Over the last two and a half years, we methodically reviewed I&A's structural organization, our intelligence priorities, our oversight safeguards and compliance capabilities, and the functions we deliver in support of our homeland security missions. We looked hard at what has worked well, and harder at what has not; identified those operational areas where we are best positioned to contribute to the homeland security intelligence enterprise and those where other agencies might be better positioned; and strategized how we can continue strengthening our capabilities as new threats demand new strategies and approaches. Throughout that process, we sought input from our oversight entities in Congress and incorporated their direction. The result has been a series of fundamental reforms to our organization and operations that will maximize our effectiveness as a homeland intelligence agency.

Snapshot of I&A

Before diving into an overview of I&A's evolution and those reforms, it is important that the reader have some basic context about I&A's general mandate, its intelligence activities, and its current organizational structure. For that purpose, we provide this snapshot of the organization as it currently exists.

The Office of Intelligence and Analysis is the U.S. Intelligence Community agency statutorily charged with delivering intelligence to state, local, tribal, territorial, and private sector entities across the homeland. In carrying out this statutory charge, I&A executes all phases of the traditional intelligence cycle—setting intelligence requirements, collecting against those requirements, analyzing the collected intelligence, and then disseminating products based on that analysis. Unlike the other intelligence agencies, I&A tailors its intelligence operations to the needs of its SLTTP partners—establishing partnerships with SLTTP organizations across the homeland, integrating information from those partners with data and information from other elements of DHS and the Intelligence Community, and then drafting and disseminating intelligence products that inform partners' decision making.

As laid out in this organizational chart, I&A is composed of four primary elements—Analysis, Collection, Partnerships, and Management—and two smaller but vitally important offices—the Transparency and Oversight Program Office and the Intelligence Enterprise Program Office. The following are brief descriptions of the purpose and operations of those elements. Fuller descriptions of these elements and their supporting offices appear in the appendix.



Office of Intelligence and Analysis Organizational Chart

Office of Analysis

The Office of Analysis produces primarily strategic intelligence products for DHS stakeholders, including senior U.S. Government officials, federal partners, and state, local, tribal, territorial, and private sector entities. Its four analytical centers—the Counterterrorism Center, the Nation-State Threat Center, the Cyber Intelligence Center, and the Transborder Security Center—serve as the Department's centers of gravity for the analysis of the most critical areas of threat to the homeland.

Office of Collection

The Office of Collection collects information about homeland security threats and disseminates it in intelligence information reports to our partners. Our collectors focus primarily on open source and human intelligence collection, but also provide tactical services to the Department by supporting screening and vetting efforts and assisting U.S. Customs and Border Protection (CBP) with the exploitation of seized communications devices. Importantly, our collection activities are carefully circumscribed by our Attorney General Guidelines—which limit us to collecting information overtly or information that is publicly available.

Oversight Review of Analytic Production

Alongside the essential adherence to analytic tradecraft standards, it is vital that I&A's products also comply with all applicable laws and other guidelines and principles to ensure the protection of privacy and civil liberties. All of I&A's finished analytic products that are disseminated outside DHS are reviewed before publication by the I&A Privacy and Intelligence Oversight Branch, the DHS Office of the General Counsel, the DHS Privacy Office, and the DHS Office for Civil Rights and Civil Liberties to resolve any concerns regarding the treatment of personally identifiable information and constitutionally protected activity.

Enhancing Transparency and Building Public Trust

As one of its initial efforts to increase transparency into I&A's activities, the Transparency and Oversight Program Office reevaluated our policies and practices around the application of the Freedom of Information Act to unclassified information relating to sources and methods. That review resulted in the issuance of a new policy, which we coordinated with the Office of the Director of National Intelligence, that permits significantly greater disclosure of sources and methods information under the Freedom of Information Act. This new guidance supplanted the prior practice of largely withholding all material specifically referencing sources and methods and requires disclosure of such material unless its "disclosure would materially negate or impair the effectiveness of those sources and methods." The Transparency and Oversight Program Office now applies that new standard in recognition of the elevated importance of transparency for an organization operating in the domestic environment.

Office of Partnerships

The Office of Partnerships coordinates all of I&A's state, local, tribal, territorial, and private sector relationships, builds and nurtures the intelligence network among those partners, and oversees over 150 I&A intelligence officers who are deployed around the country to work with our partners.

Office of Management

The Office of Management provides the administrative support—technology and data services, financial management, human resources, etc.—that enables the successful execution of our intelligence missions.

Transparency and Oversight Program Office

The Transparency and Oversight Program Office ensures I&A's rigorous adherence to the principles of privacy, civil liberties, and transparency. With the office's creation in 2023, we consolidated all of the oversight and transparency functions that were previously dispersed throughout the organization—policy coordination; privacy and intelligence oversight; support to congressional oversight; the handling of Freedom of Information Act, Government Accountability Office, and Inspector General inquiries; internal controls; and the organizational ombuds—and thereby elevated the oversight and transparency mission within the organization. The office is led by a director who reports directly to the Under Secretary for Intelligence and Analysis (the Under Secretary), and its voice is now an important consideration in every decision we make.

Keeping the Congress Fully and Currently Informed

In carrying out its statutory obligation to keep the Congress "fully and currently informed" of its intelligence activities, I&A started to provide the House and Senate Intelligence and Homeland Security Committees with regular written updates of its activities. These updates include summaries of the impact of our field reporting and analytic products—including open source and critical incident products—that we disseminate to our SLTTP partners. We also include in these notifications highlights from our engagements with SLTTP partners as well as notifications about new policies and organizational guidance we put out, such as our recently issued Program of Analysis and Operating Directive.

Intelligence Enterprise Program Office

The Intelligence Enterprise Program Office coordinates with the intelligence programs of other DHS components, which collectively make up the DHS Intelligence Enterprise. The office provides strategic and administrative support to the Under Secretary in his role as the Department's Chief Intelligence Officer, by which he exercises leadership over intelligence policy making across DHS.

ORIGIN OF I&A

To understand and assess the state of the current organization, we need first to remind ourselves of I&A's origin. I&A was born out of the September 11, 2001 terrorist attacks on our nation. In the aftermath of those attacks, several commissions and other entities examined why we had been unable to prevent the attacks and reached the same conclusion: that the national security apparatus that had been designed for the Cold War was not well suited to the asymmetric threats that the country now faced. Structural, cultural, and legal limitations were hindering coordination and information sharing between law enforcement and intelligence agencies and between the federal government and its state, local, and private sector partners. There was a clear recognition that these entities needed to enhance coordination and information sharing to identify threats and connect the dots that would help prevent the next 9/11 attack.

Building a Robust Domestic Intelligence Network – The State and Local Intelligence Council

In 2016, I&A established a State and Local Intelligence Council (SLIC) to bring together practitioners from across law enforcement, public safety, and first responder communities to improve the multi-directional information sharing that was lacking prior to 9/11. The SLIC is a practitioner-level forum that routinely meets with I&A leadership to review policies and programs, as well as analytic and operational efforts, and provides feedback to enhance the sharing of information with state and local partners. It serves as the primary body to inform I&A leadership and guide integration between I&A and state and local partners across a wide range of homeland security threats.

In response, Congress took strong actions to build a new homeland security apparatus. It lowered the so-called "wall" that limited information sharing and coordination between the intelligence and law enforcement agencies, reorganized the Intelligence Community, and created DHS to consolidate many of the federal government elements with critical homeland security responsibilities into a single, coordinated entity. Congress also signaled the need for the Intelligence Community to expand its aperture beyond the traditional focus on "foreign intelligence" by codifying a new definition of intelligence—"national intelligence"—and thereby clarifying that the Intelligence Community needed to focus on homeland threats as well as foreign threats.

Finally, Congress set out to build the foundation of a national intelligence network that would meet the domestic needs of the Intelligence Community's revised "national intelligence" mission. The result of the ensuing bureaucratic overhaul was a federal apparatus that was more focused on integrating intelligence efforts across the spectrum of national security partners—from state officials to federal agencies and from private sector critical infrastructure owners to foreign counterparts overseas. A central element of this effort was the creation of a federal agency with the statutory mandate to share intelligence with the SLTTP part of that spectrum, or as Senator

Joseph Lieberman explained, "a new intelligence division focused on the threats to our homeland [and] equipped to truly connect the intelligence and law enforcement dots from Federal, State, and local agencies…." Congress then established I&A and tasked it to build relationships and establish an intelligence network among those partners across the United States.

EVOLUTION OF I&A

Over the past 21 years, I&A has done an admirable job of building that intelligence network and meeting the demands of a new intelligence agency in a new operational space. To meet those demands, I&A built an intelligence infrastructure largely from scratch—establishing frameworks for its operations, designing tools to integrate intelligence and drive information sharing, and establishing compliance mechanisms that ensure its activities strictly adhere to privacy and civil liberties requirements. Among those groundbreaking efforts that I&A undertook throughout its first two decades are the following:

Delivering Intelligence to DHS Partners: In 2008, DHS developed an unclassified platform—the Homeland Security Information Network (HSIN)—to facilitate information sharing among the Department's stakeholders. Within HSIN, the Department also created—and I&A manages—an intelligence-sharing platform, HSIN-Intel, to enable DHS, SLTT agencies, and other federal partners to share intelligence products directly. More than 5,000 HSIN-Intel users have shared over 60,000 products that received over 300,000 views in Fiscal Year 2024 alone from law enforcement and homeland security professionals across the country.

Building an Intelligence Enterprise Within DHS: As part of the 9/11 Commission Act of 2007, Congress tasked the Under Secretary for Intelligence and Analysis to serve as the Chief Intelligence Officer for DHS. In that statute, Congress required the Under Secretary to provide the Secretary with intelligence support for DHS missions, to make recommendations related

Information Sharing in Focus - Fusion Centers

Our participation in each of the nation's 80 fusion centers is critical to our development of and support for the domestic information-sharing network. Fusion centers are state-owned and operated facilities that serve as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information among SLTT, federal, and private sector partners. These centers contribute to the national information-sharing effort by receiving and analyzing threat analysis from the federal government in the context of their local environment; disseminating that information to local agencies; gathering tips and leads from local agencies and the public; and providing suspicious activity reporting back to the federal government. They also generate products about the prevailing national threats that reflect the particular circumstances and needs of their regions, thereby providing regional leaders with the tailored intelligence to make decisions and set policy in their jurisdictions.

to intelligence resources and policies, and to oversee the DHS Intelligence Enterprise. The assignment of this new role for the head of I&A came after DHS established the Homeland Security Intelligence Council, whose membership includes Key Intelligence Officers from DHS's operational components. The Under Secretary has used the Council to implement intelligence policies across the DHS Intelligence Enterprise, to prioritize components' efforts through mechanisms such as the Homeland Intelligence Priorities Framework, and to establish and oversee bidirectional information sharing between DHS and the Intelligence Community.

Developing Organic Collection Capabilities: In 2003, Congress added DHS to the Intelligence Community in an amendment to the National Security Act of 1947. In that same year, the President formally identified I&A's predecessor office—the Office of Information Analysis and Infrastructure Protection—as the designated DHS Intelligence Community element. Yet despite the Office's integration into the Intelligence Community, it did not have a specific program through which to conduct collection activities. In 2008, Executive Order 12,333 was revised to specifically cite and delineate I&A's collection authorities. Since then, I&A has developed significant collection capabilities through building out our Overt Human Intelligence Collection and Open Source Intelligence Collection programs. Importantly, I&A has established robust oversight mechanisms to help ensure the protection of privacy and civil liberties in the operation of those programs.

Organizing to Meet the Needs of SLTTP Partners: I&A has undergone numerous organizational changes, realignments, restructurings, and overhauls through the years. These changes have been primarily focused on enabling I&A to more effectively meet the needs of the intelligence consumers it was designed to support and enable—the more than one million law enforcement officers and almost five million fire safety personnel, emergency medical services personnel, and other emergency responders in the 16 critical infrastructure sectors across the United States.

I&A initially established a State and Local Program Office to provide direct support to these partners, with a specific focus on enabling a domestic intelligence and information-sharing architecture through the national network of state and major urban area fusion centers. The growth of I&A's State and Local Program Office aligned with the initial deployment of intelligence officers to fusion centers across the country. The State and Local Program Office was responsible for providing guidance and support to help build the intelligence capacity of our SLTT partners—establishing oversight mechanisms to handle information exchanges among those partners, DHS, and the Intelligence Community, and supporting the infrastructure necessary to provide those partners with access to classified and unclassified information. Collectively, these efforts were designed to enable a domestic intelligence and information-sharing environment capable of rapidly detecting and sharing threat-related information across all levels of government.

Collocation With Our SLTT Partners: In 2005, I&A deployed its first intelligence officer to a state and major urban area fusion center. By 2008, I&A had a presence in 22 fusion centers, and today there is an intelligence officer in each of the 80 state and major urban area fusion centers. I&A has also strategically deployed intelligence officers with other SLTT partners, including

those along the southwest border. Each year, these officers produce thousands of intelligence reports and provide intelligence directly to governors, homeland security advisors, fusion center directors, mayors, police chiefs, sheriffs, emergency managers, and many more homeland security consumers.

Private Sector Engagement in Focus – Corporate Security Program

The Private Sector Engagement Branch, in collaboration with the FBI and Cybersecurity and Infrastructure Security Agency (CISA), facilitates regular opportunities for public and private sector entities to engage with one another in the form of Corporate Security Symposia. These symposia are a series of regional, day-long conferences held around the country to generate discussion among public and private sector partners—including typically a large contingent of corporate security personnel—on current and emerging security threats to their businesses, infrastructure, and cybersecurity systems. Events feature prominent speakers from both the public and private sectors who shed light on issues ranging from cybersecurity to insider threats. These face-to-face events facilitate connections among a broad range of private sector stakeholders who share common security concerns.

Since the program's inception in 2011, the Private Sector Engagement Branch has put on 86 symposia and has reached more than 27,000 registered attendees, including all 16 critical infrastructure sectors. Participant feedback on these sessions has been glowing, with 97 percent of attendees agreeing that they found the symposium to be a valuable experience. In the last year alone, I&A hosted 10 symposia.

Building Connectivity With the Private Sector: Recognizing that private sector companies are on the front lines facing threats from our adversaries, I&A also focused on enhancing connectivity with our private sector partners. This has resulted in the establishment of the Private Sector Engagement Branch, which has developed and manages a number of novel public-private initiatives, such as the Corporate Security Symposia and the Public-Private Analytic Exchange.

Private Sector Engagement in Focus - Public-Private Analytic Exchange Program

I&A also facilitates the Public-Private Analytic Exchange Program on behalf of the Office of the Director of National Intelligence to promote connections between the private sector and experienced United States Government intelligence analysts. Each year, combined public and private analyst teams produce unclassified joint analytic products for both the private sector and the government on national security issues, helping to ensure that the private sector is fully integrated into the government's analysis and mitigation of the most pressing threats to homeland security.

Persistent Challenges

Despite this impressive record of progress over its first two decades, I&A has continued to face a number of persistent organizational challenges that have constrained its ability to execute its mission to the Office's fullest potential. It is important to understand these challenges in the context of this Progress Report, as they help to explain both I&A's journey to this point as well as the reasoning behind a number of the 360 Review changes that were designed to address these challenges.

The principal organizational challenges that I&A has faced are the following:

1) Broad Mission
2) Limited Resources for a Broad Mission
3) Overlapping Authorities With Other Agencies
4) Safeguarding Privacy and Civil Liberties

Broad Mission

The implementing legislation for I&A paints its mission in broad strokes. The Homeland Security Act assigns I&A responsibility to assess "terrorist [and] other threats to homeland security" without clearly defining the contours of that assignment. The statute also gives I&A the primary role in sharing information with state, local, and private sector entities without further specificity.

The result is a broad mandate that sweeps in virtually any threat that touches the homeland. This mandate has not been significantly clarified or limited by regulation or by practice in the years since, and it has been further complicated by the increasingly diverse threat environment within the homeland. While I&A's primary area of responsibility at the start was the post-9/11 threat from foreign terrorist groups such as Al Qaeda, it has since expanded to include a myriad of other pressing dangers ranging from domestic violent extremists to transnational criminal organizations and nation-state adversaries. Faced with that multiplicity of threats, I&A has often found itself overextended and pulled in too many directions.

Limited Resources for a Broad Mission

I&A's broad mission to develop a robust information-sharing network among our federal and SLTTP partners is resource intensive. While Congress provides significant resources for I&A, including support for I&A's recent efforts to expand its core analytic cadre and enhance its technology and oversight compliance capabilities, the demands of I&A's mission and the current threat environment have often outstripped the resources available to the Office.

Overlapping Authorities With Other Agencies

I&A's work is further complicated by the fact that other federal agencies, in particular, the FBI, share the operational space that was statutorily assigned to I&A. As both a domestic law

enforcement and domestic intelligence agency, the FBI has the same remit as I&A to share intelligence with SLTTP partners. While in practice the two agencies typically focus on different types of information sharing—with the FBI focusing on more tactical, investigative intelligence in keeping with its criminal investigative function and I&A focusing on strategic intelligence—there remains an overlap of responsibility for the SLTTP intelligence-sharing mission.

Although some level of operational overlap can be helpful among intelligence agencies, in this case that overlap, in conjunction with the vagueness of I&A's statutory mission, has clouded the contours of I&A's mission space and the delineation of its area of primacy among relevant agencies. In the absence of that clear delineation, I&A has often found itself subject to varying and shifting expectations from Congress and its stakeholders, making it more difficult to build the organization around a clear and coherent vision of its mission. We are now taking decisive steps to distinguish I&A's operational primacy from that of the FBI and to build toward that coherent vision.

Safeguarding Privacy and Civil Liberties

Conducting intelligence activities in the domestic environment can be particularly fraught, as it requires a heightened sensitivity to privacy and civil liberties concerns. We at I&A have a sworn and equal duty to both prevent threats to homeland security and protect against incursions into the rights and freedoms of the American people. This is particularly critical in relation to homeland security threats such as domestic terrorism, where so much of the violence arises from political thought and speech that lie squarely within the core protections of our First Amendment.

It requires a strong compliance infrastructure to operate in the domestic arena as an effective intelligence organization while diligently protecting civil liberties. Just like other newer, less mature companies and organizations, I&A has at times struggled with developing such an infrastructure while keeping pace with the operational demands arising from the daily threats and crises. As explained below, I&A has

Data Access Review Council

The Data Access Review Council (DARC) is DHS's coordinated oversight and governance body for activities involving the sharing of personally identifiable information through bulk data transfers in support of the Department's national and homeland security missions. The DARC is administered by I&A, and includes representatives from the Office of Strategy, Policy, and Plans; the Office of the General Counsel; the Privacy Office; and the Office for Civil Rights and Civil Liberties. The DARC coordinates departmental review of Information Sharing and Access Agreements with national security partners, ensuring compliance with applicable law and policy and protecting the rights of the individuals whose information is contained in those shared data holdings. The DARC has facilitated the execution of these agreements governing the responsible sharing of dozens of DHS data sets and has been cited as a best practice within the Intelligence Community for ensuring such agreements protect individuals' privacy, civil rights, and civil liberties.

now committed the time, attention, and resources to build and develop an effective compliance infrastructure and culture. It is still a work in progress, but with the new Transparency and Oversight Program Office up and running, we are now putting the necessary mechanisms in place to build a strong oversight capacity within I&A. These oversight enhancements all flow from our recognition that homeland security can be achieved only in conjunction with the protection of privacy and civil liberties. We must pursue both at the same time, and can have a truly secure country only if we safeguard the values that made our nation strong in the first place. For I&A, our tradecraft is built upon that premise.

INFLECTION POINT – 360 REVIEW

Recognizing these ongoing challenges and the evolving threat environment, the Secretary directed I&A leadership in 2022 to undertake a wholesale review of the organization, its priorities, and its operations—a process called the "I&A 360 Review." To guide that review, we first defined our mission with the clarity that was lacking in I&A's founding legislation. That effort resulted in our articulation of the following three-part mission:

- To build and maintain an intelligence network within the United States that can detect and prevent threats to the homeland;
- To serve as an information-sharing bridge between the federal law enforcement and intelligence agencies and our SLTTP partners; and
- To operate with an intensely focused regard for privacy and civil liberties, which is a responsibility that is completely on par with the other two.

With the mission clarified, we then launched into a methodical review of I&A's operational priorities, building on the preliminary organizational assessment conducted by Acting Under Secretary John Cohen and his team in 2021. Our review was a three-stage process by which we reset I&A's priorities through a fundamental restructuring of (1) I&A's organizational scheme and elements (the organizational prioritization), (2) the subjects I&A addresses with its intelligence work (the topical prioritization), and (3) the specific functions it performs in furtherance of its above-stated mission (the functional prioritization).

I&A 360 – 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 demonstrated our prioritization of certain critical operations with the establishment of new organizational structures to lead and support those operations. This included (1) creating a Deputy Under Secretary for Partnerships, (2) establishing separate offices and leadership for our collection and analysis operations, (3) creating the Transparency and Oversight Program Office, and (4) establishing the Intelligence Enterprise Program Office.

Establishing the Office of Partnerships

Secretary Mayorkas often says that DHS is a "department of partnerships," and nowhere is that more true than at I&A. Throughout its existence, I&A has prioritized the building of meaningful relationships across the country to execute on its mission to create an effective intelligence-sharing network within the United States.

To further that effort, we elevated the partnership function within the organization, creating a Deputy Under Secretary for Partnerships and bringing in Boston Police Department intelligence veteran Dave Carabin. Dave and his team manage I&A's strategic relationship with SLTTP entities and oversee I&A's field intelligence personnel, whose work with partners around the country is so core to our information-sharing mission.

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—particularly with respect to the protection of privacy and civil liberties. I&A veteran Jim Dunlap has taken the helm at Analysis, and to lead Collection, we brought in Stephanie Dorsey—a highly respected 20-year veteran from the CIA who has brought an increased level of rigor to those sensitive operations. With this new

Deputy Under Secretary for Partnerships Dave Carabin speaks at a Field Intelligence Directorate offsite event in Springfield, VA.

Reviews of I&A's Collection Programs

Immediately upon establishing the new Office of Collection, I&A embarked on reviews of the Overt Human Intelligence Collection and Open Source Intelligence Collection programs, focusing on the efficacy of these programs' policies and procedures, the sufficiency of their privacy and civil liberties safeguards, the effectiveness of management and training, and the alignment of collection activities with I&A's strategic priorities. As a result of those reviews, I&A developed revised policy guidance concerning both categories of collection and strengthened coordination of these activities with the DHS Offices for Privacy and Civil Rights and Civil Liberties. I&A also developed a formal career service track for its collection personnel and an Intelligence Community-accredited training course for I&A personnel engaged in collection activities.

leadership 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 those collection activities that so directly implicate privacy and civil liberties concerns in the homeland.

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 the Under Secretary. This new office unites all the transparency and oversight functions that were previously dispersed throughout the organization—including privacy and intelligence oversight, the organizational ombuds, policy development and governance, congressional oversight support, Freedom of Information Act processing, internal controls, and the Government Accountability Office and Inspector General audit liaison.

Establishing a Briefing Process for the National Security Council

In addition to generating intelligence products for the President and the National Security Council (NSC), we initiated an NSC briefing process in 2022. Under this process, an I&A intelligence officer is available to brief NSC officials on a daily basis to provide them with the up-to-date homeland security intelligence, which has been a longstanding practice of other Intelligence Community agencies that provide briefings to the White House. In the past two years, our homeland intelligence briefer has held numerous briefings at the NSC, presenting policy makers with a diverse array of products across the homeland security mission space.

The Transparency and Oversight Program Office elevates these collective functions within I&A, and it ensures that compliance has a strong voice in all our front office decision making through the high-level participation of Andy Fausett and his team. Since it was established, that team has made tremendous progress in a number of critical areas, including in the issuance of operational guidance and clear policy documents.

Guidance Improvements Under the Transparency and Oversight Program Office

The Transparency and Oversight Program Office has been heavily engaged in drafting rules and guidance for our collectors and analysts. This guidance is crucial, especially for the handling of threats such as domestic violent extremism, where the terrorist violence typically arises in the context of political views and speech that are strongly protected by the First Amendment.

Policy Improvements Under the Transparency and Oversight Program Office

I&A's operating policy documents had not been maintained over the years in an orderly fashion. This lack of organization made the documents difficult to access for I&A personnel and for outside parties—such as Congress—seeking to understand the guardrails around I&A's operations. To remedy that situation, we directed the Transparency and Oversight Program Office to conduct a comprehensive review of all current policies to ensure they are up to date, user friendly for the workforce, easily accessible for external oversight entities and the public, and sufficiently focused on the ramifications of our work for Americans' privacy and civil liberties. The Transparency and Oversight Program Office is completing that review and will both update and codify I&A's guidance into a policy manual, which will be made available to the public. The initial version of the manual will be publicly released contemporaneously with this report.

Establishing the Intelligence Enterprise Program Office

As we re-examined the organizational structure of I&A, the Secretary directed I&A and the DHS Counterterrorism Coordinator 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 threat intelligence activities as well as the policy and response functions that are informed by those activities.

I&A's first National Security Council briefer, Jesús Montes, at the Eisenhower Executive Office Building.

As an initial step, we set out 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 DHS components. In statute, the Under Secretary—in his or her role as the DHS Chief Intelligence Officer—has the authority to set policy for the components' intelligence offices and coordinate intelligence capabilities across DHS to enhance threat identification, mitigation, and response. In practice, I&A has not always had the resources, leadership mandate, or organizational structure to fully fulfill this coordination and strategic oversight function.

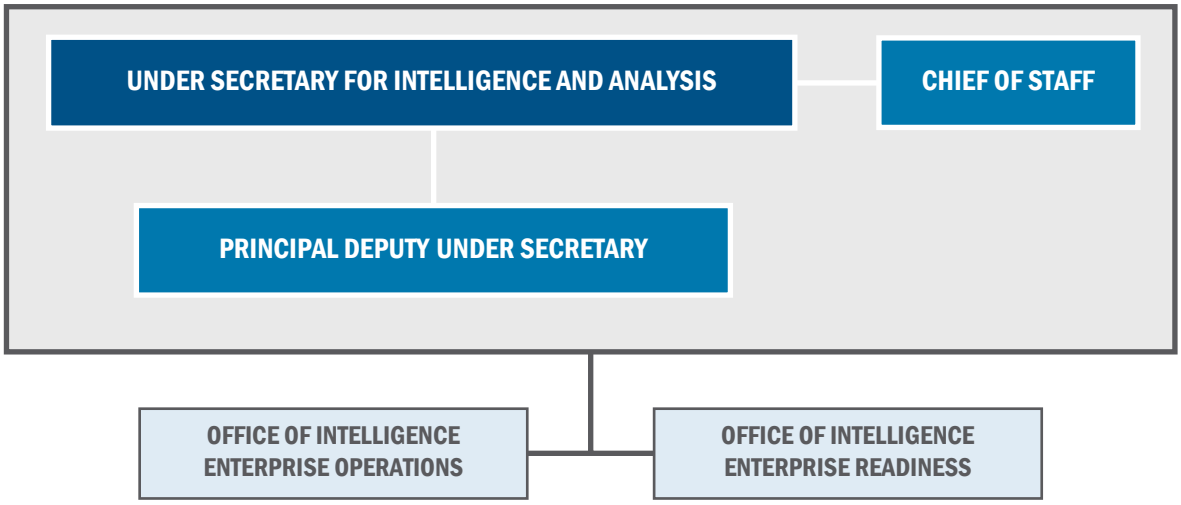
We created the Intelligence Enterprise Program Office as a vehicle to provide the strategic, administrative, and functional support necessary for the Chief Intelligence Officer to fully execute on this critical role. The office is led by intelligence veteran Steve Cash and reports directly to the Under Secretary.

The new office is already having a significant impact. For example, in 2024, the Intelligence Enterprise Program Office developed a consolidated budget for the Intelligence Enterprise for the first time—building on the foundation of the strong budgetary measures put in place by former I&A Under Secretary Francis Taylor. That budget was then presented to the Secretary on behalf of the entire Intelligence Enterprise, thereby advancing the Department-wide intelligence resource management that Congress envisioned in the Homeland Security Act. This past year, the office also established and led a rigorous, repeatable process for Enterprise-wide intelligence topic prioritization, resulting in the issuance in October 2024 of our annual prioritized ranking of intelligence topics—known as the Intelligence Enterprise Intelligence Priorities Framework—modeled on the Intelligence Community's National Intelligence Priorities Framework.

***

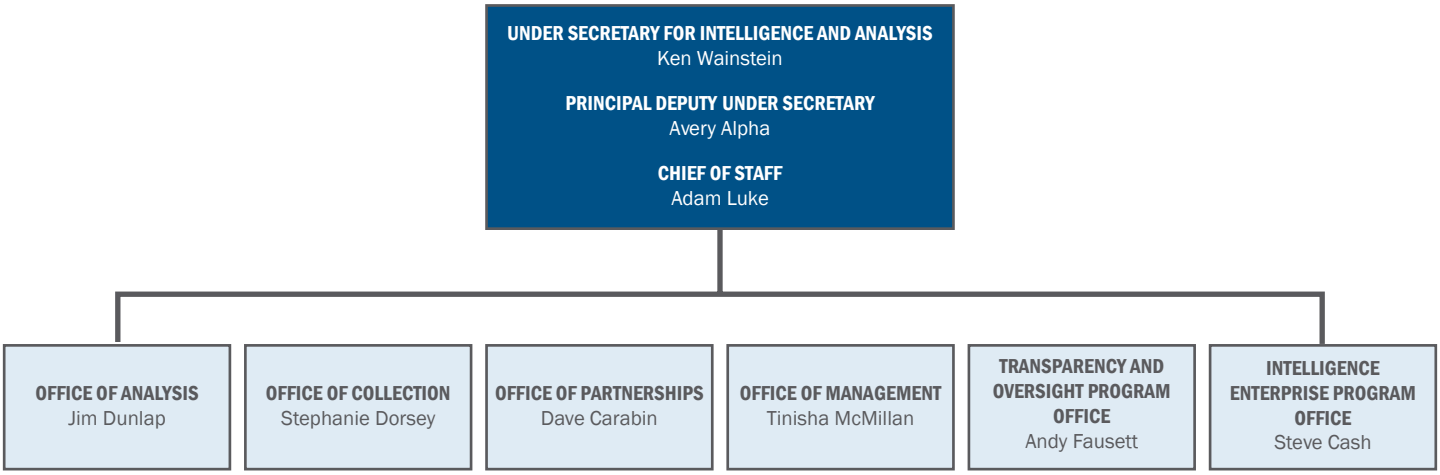
The organizational prioritization effort fundamentally changed the structure of I&A and its component offices. It took I&A from an organization with two large components for operations and management, each with a single supervisor—the Offices of the Deputy Under Secretary for Intelligence Enterprise Operations and the Deputy Under Secretary for Intelligence Enterprise Readiness—to one that now accords sufficient organizational emphasis and management focus to the functions of partnership building, collection and analysis supervision, Intelligence Enterprise management, and operational oversight.

One can glimpse the far-reaching nature of these structured changes by a review of the organizational chart before and after these changes. In the summer of 2022, this was I&A's structure:



2022 Office of Intelligence and Analysis Organizational Chart

With these changes in place, this is I&A's current structure:



Office of Intelligence and Analysis Organizational Chart

THE LEADERSHIP OF I&A

We have a strong group of leaders to oversee all of these new organizations within I&A.

Principal Deputy Under Secretary Avery Alpha spent most of her career before joining I&A at the Central Intelligence Agency (CIA), where she served as a senior manager in the Counterterrorism Mission Center. Avery also worked at the National Security Council as a Senior Policy Advisor and Chief of Staff to the President's Homeland Security Advisor.

Chief of Staff Adam Luke worked for 12 years in various intelligence roles and led international deployments as a U.S. Customs and Border Protection agent. Since joining I&A, Adam has worked extensively with the congressional Intelligence and Homeland Security Committees, and he recently served a stint as the Acting Deputy Under Secretary for Management for I&A.

Deputy Under Secretary for Collection Stephanie Dorsey is a Senior Intelligence Service officer at the CIA who is currently detailed to I&A. Stephanie has extensive experience leading foreign intelligence collection and operations related to counterproliferation, counterintelligence, and other critical national security threats.

Deputy Under Secretary for Analysis Jim Dunlap has served in various roles at I&A and elsewhere within DHS, and has almost 30 years of intelligence experience. Prior to his current role, he served as the Executive Director of I&A's Counterterrorism Center. Before joining DHS, Jim was a U.S. Air Force officer, where he served in a variety of roles as a signals intelligence officer, all-source intelligence officer, intelligence briefer, and strategic planner.

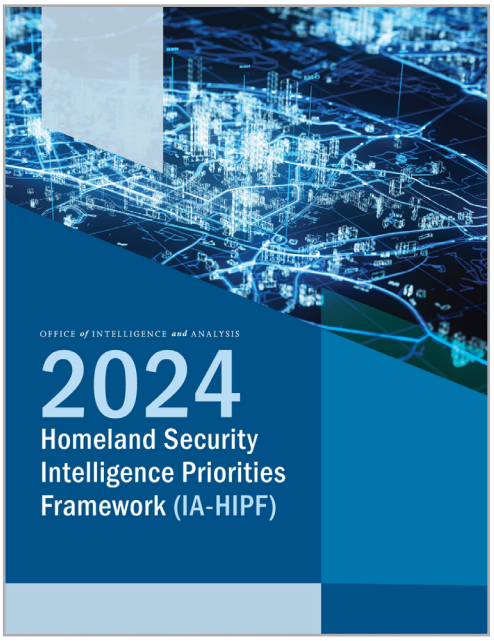
Deputy Under Secretary for Partnerships Dave Carabin has 21 years of experience in law enforcement. He arrived at I&A after serving as the Assistant Chief of the Boston Police Department's Bureau of Intelligence and Analysis since 2017, and as the Director of the Boston Regional Intelligence Center since 2010.

Deputy Under Secretary for Management Tinisha McMillan has served in several critical leadership positions at the Department of Defense related to intelligence and network defense capabilities. At the Defense Information Systems Agency, where Tinisha served immediately prior to joining I&A, she oversaw several organizations and commands that directly support the President and managed a portfolio of more than $14 billion responsible for enterprise end-user IT services.

Executive Director of the Intelligence Enterprise Program Office Steve Cash has broad experience at the federal and state level in the executive, legislative, and judicial branches. He was Chief Counsel and Staff Director (minority) to the U.S. Senate's Judiciary Committee, Subcommittee on Terrorism, Technology, and Homeland Security. Steve also served as an intelligence officer with the CIA, first as an Assistant General Counsel and then with the Directorate of Operations as an operations officer. Steve also served for six years as a prosecutor with the New York County District Attorney's Office.

Director of the Transparency and Oversight Program Office Andy Fausett joined I&A from the DHS Office of the General Counsel, where he served most recently as Deputy Associate General Counsel for Intelligence. Between October 2022 and April 2023, Andy served as the Acting Deputy Assistant Secretary for Counterterrorism and Threat Prevention for the DHS Office of Strategy, Policy, and Plans. Andy also served details at the National Security Council and on Capitol Hill with the Senate Judiciary Committee.

I&A 360 – Stage 2: Topical Prioritization

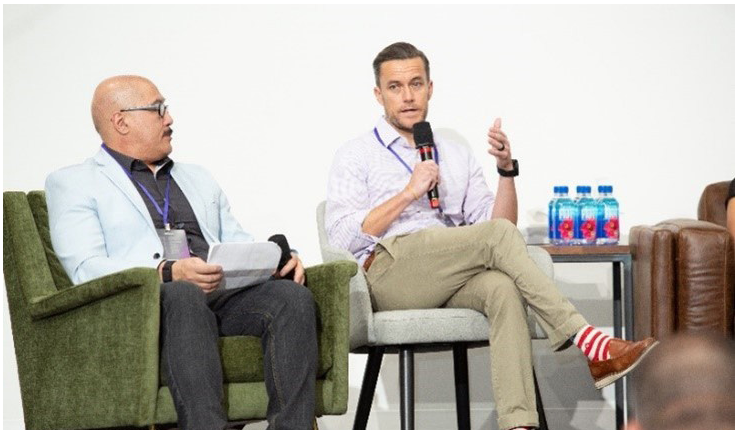


In the fall of 2023, for the first time in a decade, I&A produced a Homeland Intelligence Priorities Framework—a prioritized list of national and departmental intelligence topics to serve as an overarching strategic document for all our intelligence operations. Through that process, we categorized all of the homeland security threat topics into one of three priority levels based on both the severity of the threat and I&A's capacity relative to other Intelligence Community agencies to effectively address that threat. That ranking became I&A's Homeland Intelligence Priorities Framework, which, in turn, informed the formulation of both our Program of Analysis and Operating Directive—the strategic documents that guide our analytic and collection efforts, respectively. Together, these three documents help to keep our efforts focused on the most pressing threats and on those against which I&A can bring to bear capabilities not shared by other agencies.

Recognizing the value of that strategic framework, I&A coordinated with the DHS Intelligence Enterprise to develop a similar document—the Intelligence Enterprise Homeland Intelligence Priorities Framework—to guide the intelligence priorities of other components within DHS that conduct intelligence-related activities. This framework helps the DHS Intelligence Enterprise components prioritize among areas of intelligence work and conduct informed resource planning.

I&A 360 – Stage 3: Functional Prioritization

The final step in our 360 Review was the prioritization of the functions we perform in the course of our intelligence work. That effort included cataloging all the duties we perform and examining their importance to our mission in light of four operating principles that guided our decision making throughout this process. Those principles are:



I&A officer participates in a panel discussion at the Silicon Valley Security Group Public-Private Partnership Symposium.

1) **Focus on Serving the Intelligence Needs of Our SLTTP Partners:** Congress made clear that I&A is 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 consumers.

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 helps our SLTTP partners prepare for and meet the homeland security threats in their jurisdictions. 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 we focus on providing intelligence that illuminates broader threat patterns and doing so at the lowest classification level possible.

3) **Focus on Leveraging Unique Capabilities:** In prioritizing our functions, we should focus on areas where I&A can contribute unique capabilities and has distinct operational advantages. It is for this reason, for example, that we prioritized each topic in the I&A Homeland Intelligence Priorities Framework, the Program of Analysis, and the Operating Directive based largely on how well positioned we were to 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.

Providing All-Source Analysis to Our Stakeholders

I&A maintains a full suite of product lines to deliver all-source analysis to our stakeholders. This year, recognizing a gap in the ability to deliver rapid "breaking news" analysis and context on developing incidents, I&A created a "Critical Incident Note" line, co-authored by our watch and intelligence analysts, to provide initial analysis and reporting to SLTTP partners. We provide these preliminary summaries to our partners to enable them to respond as quickly as possible to emerging threats.

We applied these four principles in every stage of our functional reprioritization process, and the result was approximately 30 significant functional changes across I&A. Every one of those changes was designed to advance these four principles.

For example, to advance our service to our primary SLTTP consumers, we restructured the organization of our field presence, which provides the day-to-day touchpoint and intelligence support for those partners, and started a program to recruit and integrate SLTTP detailees into I&A who will help the rest of our staff produce intelligence products and services that better meet the particular intelligence needs of our SLTTP partners. To enhance the strategic focus of our analysis, we are embedding our open source collectors within our analytic centers to more directly tether their collection to each center's strategic analytic efforts. To leverage the unique

advantage of our intra-DHS relationships with CBP and Immigration and Customs Enforcement, we are embedding our personnel within those components to gain access to their data and investigative information. Finally, to improve I&A's management, we are conducting a comprehensive review of our supervisory ranks and implementing a number of initiatives to enhance the supervisory support provided to our line personnel.

Several of the more significant changes growing out of the functional prioritization are the following:

Realigning I&A's Field Presence

In July 2024, I&A announced a realignment of its field posture, which is designed to bolster management of field resources, improve connectivity with both headquarters and our SLTTP partners, and enhance integration with other components of DHS.

The realignment makes several key changes to I&A's Field Intelligence Directorate, which include:

1) Realigning I&A's 12 field regions into 10 regions to align with the regional structure used by the Federal Emergency Management Agency (FEMA), CISA, and other DHS offices and agencies. This allows I&A personnel to collocate with personnel from other DHS components to achieve cost savings and increase collaboration and information sharing.

2) Grouping the regions into four divisions, each led by a division director and staff who will strengthen management and support for field personnel and build closer connectivity between the field and headquarters.

3) Adding compliance staff to the field to more effectively ensure field activities are aligned with Intelligence Community and departmental policies and protect individuals' privacy and civil liberties.

Establishing a Field-HQ Rotational Program

The Under Secretary hands out an award at a Field Intelligence Directorate awards ceremony.

The Principal Deputy Under Secretary speaks with a participant in I&A's Field Intelligence Directorate networking event in December 2023.

To promote cohesion between the field and headquarters and better integrate field personnel into overall I&A operations, we have initiated a program for bringing field personnel into I&A headquarters for details of varying lengths. Simultaneously, we are developing a rotational program for headquarters analysts and collectors to complete rotations to the field to increase their exposure to and understanding of field operations.

Focusing Our Overt Human Intelligence Collection on Border Threats

During our 2023 assessment of our Overt Human Intelligence Collection program, we found that the program has been particularly 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.

I&A officer from the Field Intelligence Directorate gives a threat overview on transnational organized crime

To build on that success and leverage our relationships with DHS components with border enforcement responsibility, we are now largely focusing our field interviews on individuals with information about border security-related threats, and, in particular, on the interviews of detained migrants of homeland security interest that we conduct in coordination with CBP along the southwest border. Those interviews generate significant raw intelligence reporting about the illicit narcotics trade, human smuggling, cartel activity, and other cross-border threats—reporting that is not conducted by any other intelligence agency outside DHS. While field personnel may still submit operational proposals for other field interviews, the majority of the field intelligence program is now focused on border-related issues.

Refocusing Our Open Source Intelligence Program

In June 2024, we completed a review of our Open Source Intelligence Program and identified several reforms that we believe will increase the relevance of collection for both our analysts and SLTTP partners.

Embedding Collectors in Analytic Centers

First, we are moving our open source intelligence collection staff from their current office at the DHS St. Elizabeth's campus and integrating them within I&A's analytic mission centers at the

Nebraska Avenue Complex. This will enable the collection staff to better align their collection efforts with the analysts' priorities and improve the utility of that collection for finished intelligence production.

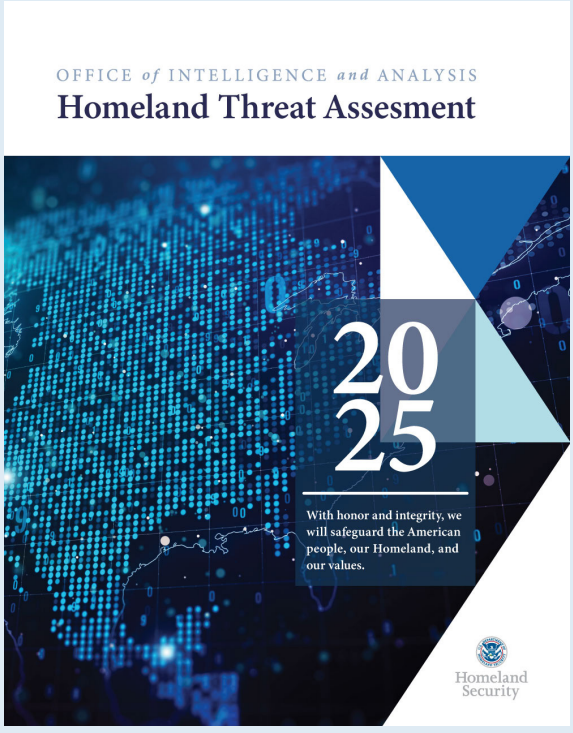
Focusing on Strategic Intelligence Collection

Second, we are refocusing our open source collectors' efforts from tactical to strategic collection. Open source collection can be used to obtain tactical information about unfolding threat events or to identify longer term patterns and trends that are the grist for strategic intelligence products. In recent years, I&A moved toward more tactical-level open source collection as the Office increasingly tasked its collectors to search, collect, and provide warnings about the possibility for violence developing around specific events of heightened tension, such as the mass gatherings in the aftermath of the October 7, 2023, Hamas attacks against Israel.

For several reasons, our open source collectors are not adequately postured to perform that tactical warning function. They operate with strictly constrained authorities; they are a small unit without the manpower to conduct the wide-ranging internet search that is often necessary to provide warning during unfolding threat situations; and the unit has now been further constrained in dealing with domestic terrorism threats by language in the 2024 National Defense Authorization Act that limited our open source collection on the domestic terrorist threat to a handful of collectors. As a result of these limitations, from now on we will largely defer to the FBI to perform tactical open source threat reporting, and will instead steer our open source collectors

The Homeland Threat Assessment

I&A issues the Homeland Threat Assessment, its marquee annual product, in September of each year at the direction of the Secretary. Designed as the homeland analog to the Office of the Director of National Intelligence's Annual Threat Assessment, the assessment is an unclassified overview of the primary homeland security threats facing the nation and how we expect those threats to manifest and evolve over the coming year. It is intended to identify and describe those threats in a way that informs our SLTTP partners' policy decisions and allocation of resources, and is regularly used by DHS senior leaders in their interactions with Congress and the public.



toward collection that supports the generation of strategic intelligence products by the analytical centers.

The Homeland Intelligence Advisory Board

The Under Secretary stood up a Homeland Intelligence Advisory Board to provide insight into national and homeland security intelligence matters. The Board provides information and advice to the Under Secretary and to the DHS Counterterrorism Coordinator on various relevant issues, including those related to operational adherence to the principles of privacy and civil liberties. The Board convenes on a quarterly basis, and its members represent diverse perspectives and a variety of communities—including intelligence and homeland security, privacy and civil liberties, law enforcement, state and local government, private industry, and academia.

Strengthening Analytic Production

Our Analytic Advancement Division is the component within the Office of Analysis that is responsible for reviewing the drafts of all finished intelligence products and ensuring we meet the highest standards of analytical practice and tradecraft. Division Director Rob Barocas and his team have made significant strides in improving both the quality of our products and their utility to our consumers, improvement that has been reflected recently 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 consumers. We will use this data to reassess the allocation of our analysts within mission centers and to ensure we are well positioned to cover near-term departmental priorities and needs.

Updating I&A's Style Guide

In June 2023, I&A updated its style guide for finished intelligence products for the first time in 10 years. It is standard practice for Intelligence Community analytic organizations to have up-to-date style guides to enable different analysts to present their assessments to consumers in a consistent and reliable manner. The I&A style guide reminds analysts to articulate assessments in terms of their relationship to the homeland, to maximize the use of DHS-specific information and resources, and to concentrate on writing concisely and with specificity. The style guide includes instruction on building products and appropriate sourcing and classification practices, among other topics.

As an example of its enhanced proficiency, I&A clearly displayed both the quality of its work and the agility of its operations in its response to the horrific attacks in Israel on October 7, 2023 and to the ensuing conflict. In the aftermath of

the attacks, analysts produced clear daily situational reports about the conflict and its homeland implications for DHS leadership and our partners and published several products jointly with the FBI and the National Counterterrorism Center. As part of that effort, our subject-matter experts also participated with the FBI and the National Counterterrorism Center in national threat calls with state and local partners to discuss the homeland threat environment, and we continue to report on potential threats stemming from the heightened tensions surrounding the conflict.

Reestablishing the SLTTP Fellows Program

To help ensure our analysis is tailored to the needs of SLTTP stakeholders, we are reestablishing our SLTTP fellows program to integrate individuals from our SLTTP partners across the Office. This will help to better orient our products and services to address our SLTTP partners' most pressing security priorities.

Leveraging Investigative Case Files

Consistent with our reorientation toward strategic-level intelligence, we are now focusing on the production of 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 homeland security intelligence, various obstacles have historically prevented that information from being fully leveraged for strategic intelligence purposes. To address that shortcoming, we are now participating in two pilot programs in which our analysts are reviewing and generating intelligence products from the case files of our law enforcement agency partners.

Nationwide Functional Teams

Starting in 2024, we established Nationwide Functional Teams (NFTs) as mechanisms to facilitate coordination between I&A's Offices of Analysis, Partnerships, and Collection and to focus our activities on priority intelligence topics. The NFTs are composed of a senior field officer, a senior analyst, a collection operations manager, and a tailored group of subject-matter experts. They synchronize efforts between the field and I&A headquarters through the use of joint plans that direct information sharing, collection, and analysis for each NFT with written taskings and set clear performance metrics. I&A has four NFTs, one for the mission of each analytic center: counterterrorism, cybersecurity, nation-state threats, and transborder security.

First, as part of the Department's counter-fentanyl campaign, our analysts and reports officers are working closely with Homeland Security Investigations personnel to review their fentanyl investigation files and generate intelligence information reports with actionable intelligence for our federal and SLTT partners. We are also entering into 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, all under the strict controls

necessary to protect such sensitive investigative information. This latter arrangement is particularly important. With Congress prohibiting the National Counterterrorism Center from producing analytic products related to domestic terrorism threats that lack a foreign nexus, it is all the more critical that we work with the FBI to review the information about such threats in its domestic terrorism case files and turn it into actionable strategic intelligence for our SLTT partners.

I&A WORKFORCE

Beyond these areas of institutional change (the organizational, topical, and functional changes detailed above), the I&A 360 Review has also focused on reforms and initiatives that enhance the effectiveness of the management and support we provide to the I&A workforce—the individuals, the teams, and the community of I&A homeland security professionals who dedicate themselves to our mission set day in and day out.

Those changes can be seen at every stage of the employment lifecycle at I&A—from employee recruitment and onboarding through training and supervisory development. The below section summarizes those changes and their significance to the health and morale of the organization.

Workforce Recruitment

I&A has long prioritized the recruitment of strong entry-level talent. While we attract many strong applicants through USA Jobs and by word of mouth, a primary means of recruiting talent to I&A is through our internship program, which was formally established in 2016 at the direction of then-Under Secretary Francis Taylor to develop a recruitment pipeline and accelerate efforts to diversify the

Special Events Program

I&A also provides support to special events, primarily through its Special Events Program. This program coordinates support across the federal government to assist state and local partners to address any capability shortfalls, thus helping to ensure a safe and secure event. To execute this mission, the Special Events Program annually collects data on special events occurring across the country; manages an interagency process to review the risks associated with each event, ultimately assigning a Special Event Assessment Rating to each event; and coordinates support across the federal government for the highest risk events. Examples of submitted events include the Super Bowl, Indianapolis 500, and the Kentucky Derby. I&A also works closely with its federal partners and state and local law enforcement to issue Joint Special Event Threat Assessments for select high-risk events.

I&A 2023 intern cohort

skill sets and backgrounds of the workforce. The internship program recruits undergraduate and graduate students for summer jobs, sponsors them for Top-Secret security clearances, and then provides them with meaningful, substantive work on different threat issues. The program has proven to be a resounding success, with the 2024 solicitation generating a record 2,300 applicants from a range of higher education institutions, and a large percentage of our eligible graduating interns accepting permanent positions within I&A. In support of the program, our Workforce Management and Engagement team has effectively integrated technical tools and systems that allow it to advertise the program to—and accept and evaluate applications from—more than 1,000 colleges and universities, including many of the nation's Historically Black Colleges and Universities and Minority Serving Institutions.

Workforce Onboarding

In October 2022, I&A rolled out its New Hire Onboarding Program by which it introduces new employees to I&A and its mission. The program is a two-week introduction designed to give new hires basic training in the fundamentals of homeland security intelligence, the authorities exercised by DHS and I&A, and the privacy and civil liberties limitations on those authorities. Following the program, each cohort is assigned additional intelligence training depending on their position, with analysts receiving a six- or eight-week course on intelligence analysis and tradecraft and non-analysts taking a three-week course covering I&A and the intelligence cycle.

The Intelligence Training Academy, I&A's Federal Law Enforcement Training Academy-accredited training operation, in Springfield, Virginia.

After completing their onboarding training, each cohort of new I&A employees travels to New York's National September 11 Memorial and Museum, accompanied by the Under Secretary. They visit Ground Zero, hear from 9/11 survivors, and discuss the significance of that day for the country and for our organization. At the end of the trip, the Under Secretary administers the oath of office to the new hires in the 9/11 Museum. Taking the oath is a significant milestone in every public servant's career, and doing so at Ground Zero poignantly reminds every employee why I&A exists—to share the intelligence that equips our partners to prevent threats and terrorist attacks like those we suffered on 9/11.

Workforce Training

Our personnel continue to receive training throughout their tenures at I&A's Intelligence Training Academy, which is our Federal Law Enforcement Training Academy-accredited training operation in Springfield, Virginia. Over the past few years, I&A has invested significant resources into the Academy to develop courses for employees and managers and for our state, local, tribal, and

territorial partners. Last year, the Academy trained more than 2,300 students, 700 of whom were SLTT personnel, and in 2025, the Academy will offer about 40 courses to I&A employees, approximately half of which are available to state and local partners.

Workforce Recognition

Recognizing the achievements of the workforce is an absolutely critical responsibility of leadership. We foster a culture of excellence by highlighting the best qualities we see in our personnel and rewarding the most deserving employees.

The Under Secretary grants an award to an I&A employee, now a member of the Intelligence Enterprise Program Office, for her service to I&A.

In service of that goal, we now hold regular all-hands awards ceremonies and have reorganized our awards program, launching new categories of I&A-wide awards, allocating funds for special act awards, and establishing a process for peer-nominated awards. Each quarter, we also give out the Employee of the Quarter award and the Under Secretary awards recognizing outstanding performance and employees who best represent the values of our organization.

Workforce Mentoring

As directed by the I&A 360 Review, we are integrating employee mentoring at all levels of I&A to enhance professional development at every grade. We expect all our senior leaders to prioritize and perform mentoring and are taking that corporate contribution into consideration in their annual performance reviews. As an example, the Principal Deputy Under Secretary is personally leading two monthly mentoring circles—one for a small group of entry-level personnel and a second for a small group of first-line managers across all offices—to discuss challenges, expand skill sets, and share best practices.

Workforce Supervision

We recognize that the key to a healthy organization is the development of a strong supervisory cadre. Given the size of our organization and the breadth and variety of the intelligence work we perform, it is crucial that our supervisory personnel are both fully equipped and fully accountable to provide the necessary support to the officers who are doing that work each day. To enhance our supervisory capabilities across all offices, the Deputy Under Secretary for Management is implementing the following initiatives:

1) Establishing a Foundations of Management training program for new managers and implementing a development plan for existing managers that focuses on improving

supervisory and leadership skills—including managers' ability to prevent and resolve conflict, deliver effective feedback, communicate with others, and hold themselves accountable.

2) Revising performance evaluations for supervisory personnel—to more thoroughly assess their management strengths and weaknesses—and implementing 360 reviews for managers at all levels.

3) Using surveys to evaluate supervisory interest and potential, including an I&A-wide survey of current supervisors to assess their interest in maintaining or expanding their supervisory responsibilities, and a survey and annual assessment of the current GS-13 cadre to identify interest in and readiness for promotion into the supervisory ranks.

4) Developing an Aspiring Managers Program for the GS-13 cadre to provide them greater insight into the responsibilities of managers, help inform their consideration of future management roles, and develop the skills necessary to succeed in them.

5) Reexamining the promotion process for GS 7-13 personnel to ensure equitable workforce evaluation and promotion.

Workforce Organizations

I&A has established a number of employee organizations that fortify and create connections within our workforce. Those include the Employee Advisory Council and the six employee associations that bring colleagues together to share and celebrate our backgrounds, interests, and heritage.

Employee Advisory Council

The I&A Employee Advisory Council is an advisory body composed of employees from across I&A that focuses on:

1) Improving the organization through open dialogue between senior leadership and the workforce;

2) Providing workforce perspectives to leadership and recommending ways to improve work conditions and employee morale; and

3) Increasing the workforce's participation in and ownership of I&A's strategic direction.

To achieve these objectives, Council members solicit input from their respective centers or offices, update the Council on this input during regular meetings, engage with teams across I&A to address any concerns, and meet regularly with the Under Secretary and senior leadership to communicate this feedback and make recommendations. Over the years, the Employee Advisory Council has grown to account for I&A's organizational expansion and the importance of the Council's mission. With only about eight representatives in its early years, the Council now has 26 members.

Employee Associations

I&A now has six employee associations that offer employees a chance to drive positive change in the organization and to be in community with individuals who share similar interests, demographic backgrounds, or life experiences. These groups include the following:

Pride, Resources, Inclusivity, Support, Mentorship (PRISM) Employee Association: PRISM, established and chartered in June 2019, addresses diversity issues specific to the LGBTQIA+ community and provides a forum for education and communication around sexual orientation and gender minority concerns. PRISM also serves as a chapter of the Intelligence Community Pride and DHS Pride organizations, which are the official LGBTQIA+ employee associations for Intelligence Community and DHS employees, respectively.

Members of PRISM participate in the first ever I&A Employee Association Summit.

Gender, Equity, and Mobility (GEM) Employee Association: GEM, established and chartered in August 2022, brings I&A employees together to engage around issues particular to gender equity and mobility. Its approximately 70 members engage in monthly meetings to discuss gender issues in the workplace, and during Women's History Month, it sponsors programs for I&A staff—including mentorship training, a panel discussion, and a networking hour to drive conversation around gender equity.

GEM helps to host I&A's inaugural Women's History Month flag raising ceremony in March 2022.

African American Employee Association (AAEA): The AAEA, established and charted in June 2024, serves as a collective voice on shared concerns specific to I&A's African American community. The AAEA focuses on establishing open and trusting communication between that community and I&A leadership, expanding cultural awareness within I&A, and advocating for the career advancement and development of its members throughout the ranks of I&A.

Juneteenth flag raising in June 2024 and AAEA charter signing with members of the Blacks In Government leadership board, the official DHS employee association for African American departmental employees.

Disability, Neurodivergence, and Accessibility Employee Association (DNA): The mission of I&A DNA is to create a forum where employees of all abilities and neurotypes can discuss workforce diversity issues particular to disability, neurodivergence, and accessibility.

Members of DNA pose for a photo following the employee association's signing of its charter.

Asian American, Pacific Islander, and Native Hawaiian Employee Association (AAPINH): AAPINH's mission is to empower and elevate individuals of Asian American, Pacific Islander, and Native Hawaiian descent in the I&A workforce; foster within I&A the inclusion of its community members along with those of other communities; and advocate for professional development that will help the AAPINH community with career advancement.

The AAPINH employee association gathers at the Nebraska Avenue Complex with I&A senior leadership for the association's official charter signing in November 2024.

Hispanic/Latin American Professionals in Intelligence (HAPI): HAPI is committed to supporting individuals within I&A of Hispanic and Latin American descent. It promotes opportunities for Hispanic and Latin Americans, as well as allies and serves as a bridge for communication among I&A leadership, the workforce, and external partners. The organization strives to increase the presence and influence of those in its community, while shaping a more inclusive future for I&A.

Members of the HAPI employee association and the DEIA Council convene for the association's official charter signing.

Diversity, Equity, Inclusion & Accessibility (DEIA) Council

The DEIA Council, chartered in March 2021, champions the Department's commitment to inclusive diversity practices in the areas of recruitment, employee engagement, and diversity training. The DEIA Council serves as the overarching support element for I&A's employee associations and is part of the I&A Workforce Health and Resilience team within the Workforce Management and Engagement team. The Council is overseen by the Chief Diversity, Equity, and Inclusion Officer, whose job is to drive diversity and equity initiatives.

Workforce Programming

Over the past few years, we have placed an organizational priority on enhancing workforce engagement and morale. In furtherance of that goal, we have developed or reinvigorated several workforce programs to build a stronger and more connected organization.

Family Day

To recognize the critical role of families in our employees' homeland security work, in the fall of 2022 I&A hosted its first Family Day event in the last decade. Over 300 of our employees' family and friends visited the Nebraska Avenue Complex (NAC) to learn about and celebrate the organization, its workforce, and its mission. Thanks to generous participation from our fellow DHS components and other partners, our visitors were treated to a variety of exciting educational activities, including

Acting Deputy Secretary of Homeland Security Kristie Canegallo leads children in an oath to have fun with their new friends at I&A Family Day in April 2024.

viewings of a CBP Air and Marine Operations helicopter landing, the Secret Service's presidential limousine nicknamed "The Beast," FEMA's Mobile Emergency Response Support vehicle, and Park Police horses. Visitors also toured the historic Nebraska Avenue Building No. 19 with employee escorts to see the cleared spaces where their loved ones work.

In the spring of 2024, our second Family Day was even larger, with over 500 attendees and even more activities. Highlights of the day included a swearing-in ceremony for children led by Acting Deputy Secretary of Homeland Security Kristie Canegallo, and over 20 informational tables from I&A centers and divisions in the NAC gymnasium. History presentations, working canine demonstrations, and Customs and Border Protection drone flights all added to an exciting day for I&A families.

Speaker Series

Beginning in the fall of 2022, I&A started hosting the I&A Speaker Series, where we invite intelligence professionals and other current or former government officials to participate in a fireside chat with the workforce. In this setting, the Under Secretary and the speaker sit down in the NAC Chapel to discuss the speaker's career, any lessons learned along the way, and advice for our employees as they progress through their own careers. We have been fortunate to host a large number of highly respected public servants, including former Director of the National Counterterrorism Center Christine Abizaid, former Under Secretary for Intelligence & Analysis Charlie Allen, former CIA Director John Brennan, the Acting Deputy Secretary of Homeland Security Kristie Canegallo, former Secretary of Homeland Security Michael Chertoff, former Director of National Intelligence James Clapper, Deputy Director of the CIA David Cohen, Principal Deputy Director of National Intelligence Stacey Dixon, Director of National Intelligence Avril Haines, former Director of the National Security Agency Michael Hayden, Secretary of Homeland Security Alejandro Mayorkas, Deputy Attorney General Lisa Monaco, former Under Secretary for Intelligence & Analysis Francis Taylor, and former Deputy Secretary of Homeland Security John Tien.

Former Secretary of Homeland Security Michael Chertoff (top) and former Director of the National Counterterrorism Center Christine Abizaid (bottom) engage in fireside chats in the NAC Chapel with the Under Secretary as part of I&A's Speaker Series.

Historical Preservation Education Initiative

I&A personnel deserve to understand the rich history of those who have protected the homeland in pathbreaking ways in the very space in which I&A employees are doing so today. We have therefore recently turned an eye toward elevating and celebrating the history of the NAC, and in particular the significant cryptanalytic role it played in the Allied victory in World War II. In April 2024, I&A launched an education campaign to elevate the legacy of Elizabeth Smith Friedman, regarded as "America's first female cryptanalyst," and her team of female Coast Guard cryptanalysts who were stationed at the Nebraska Avenue Complex, then called the Naval Communications Annex, during World War II. This cryptanalytic team worked simultaneously with, but independently of, the well-known British codebreaking group led by Alan Turing to break the code behind Germany's Enigma G machine and thereby give the Allies an immeasurable operational and strategic advantage over the Nazi forces.

This has been a multi-faceted education campaign. We designed a tour to show visitors the historically significant locations throughout the NAC facility. We installed a display (pictured) with cryptographic equipment, photographs, and a uniform from the team that served at the NAC, which were generously loaned by the National Cryptographic Museum. And in July 2024, we and several cryptologic organizations (Cryptologic Warfare Activity Sixty Seven Naval Command, the National Security Agency Center for Cryptologic Heritage Team, and the U.S. Naval Cryptologic Veterans Association) hosted a ceremony celebrating the World War II female Navy cryptanalysts who worked at the NAC.

Workforce Wellbeing

Our 360 Review and accompanying effort also included several initiatives and reforms designed to enhance workforce wellbeing, cohesion, and resiliency, including the following.

Wellness and Resilience Programming

The organization has taken several positive steps with respect to employee wellness and resilience. For instance, in 2023 I&A initiated a Graphic and Disturbing Content Resiliency program led by a veteran psychologist from the CIA. Leadership developed this program in response to concerns from employees exposed to traumatic events and online content. The program provides

individual coaching and hosts group exercises to ensure every employee has access to support and mental health resources. Also, in 2024 I&A appointed a Deputy Director for Workforce Well-Being, who oversees employee resource groups and runs wellness activities for the workforce. Finally, to further workforce wellness and align with departmental policy, I&A has now updated its internal policies to grant employees up to five hours of administrative leave per week to engage in fitness and mental health activities with their supervisor's approval.

Telework Policy

During the COVID pandemic, I&A instituted a telework policy that authorized telework for I&A staff according to their position and responsibilities, resulting in a significant reduction in employees physically present in the workplace and limiting the opportunity for in-person teamwork. While this policy was an appropriate means of affording locational flexibility during the pandemic, it exacted a cost in terms of workforce cohesion and the supervision, training, and mentoring that is often most effective in person.

To create a stronger sense of community and promote engagement among the workforce, we revised that telework policy in April 2024. The new policy reduces the number of telework days for many of our employees, requires all staff to be present for two in-person "collaboration days" per week, and generally limits those in supervisory positions to one telework day every two weeks. We are already seeing how the adjusted telework policy is increasing collaboration and camaraderie across our organization and improving the quality of supervisory support for our workforce.

We are also seeing a workforce that has admirably adjusted to the new policy, despite the challenges and dislocation it has caused for some. We are grateful to our colleagues for their understanding and for the professionalism with which they have adapted to the new telework conditions.

Workforce Input and Feedback

I&A has also recently established mechanisms for employees to provide leadership with feedback or express concerns about the circumstances of their work. Among these mechanisms are the routinely held office-wide town hall meetings, brown bag lunches, and the introduction of the Management Analysis and Assistance Program, where employees complete surveys and provide direct feedback on their specific unit's supervisors and managers. I&A then reviews the feedback, takes action based on that feedback, and communicates those changes to the workforce.

Additionally, I&A employs two ombudsmen—an organizational ombudsmen and an analytic ombuds. We hired an organizational ombudsman to serve as an independent, impartial dispute resolution practitioner and provide an informal and confidential forum to hear, informally investigate, and help address individual and organizational concerns. Our analytic ombudsman is available for I&A employees to raise the full scope of concerns related to I&A's operations, including about collection practices and analytic tradecraft. Beyond facilitating equitable outcomes for employees with these concerns, the ombuds seek to promote transparency and foster constructive dialogue within the workforce.

Finally, we have implemented an advanced analytic employee feedback survey, which can be used to examine the operation of an individual I&A center or division, diving deeply into the operation of leadership and work environments. This tool has already provided actionable insight into several areas for improvement—contributing to adjustments in work-unit dynamics, leadership training, and work flexibility opportunities.

CONCLUSION

As the foregoing demonstrates, I&A has gone through—and is still going through—a period of transformation that is deep and significant. In ordering the I&A 360 Review in 2022, Secretary Mayorkas directed that we undertake this transformation in a strategic and methodical manner. Specifically, he asked that we first define I&A's core mission; that we then identify the primary challenges to the execution of that mission; and finally, that we implement changes that address those challenges and redesign the organization to align with our operating principles and our mission.

That is exactly what we have done over the past 31 months. First, we clarified that our primary mission is to develop a domestic intelligence network for the sharing of homeland security information among our SLTTP partners, and to operate that network with full regard for the very significant privacy and civil liberties concerns that are implicated by the conduct of intelligence activities within the United States.

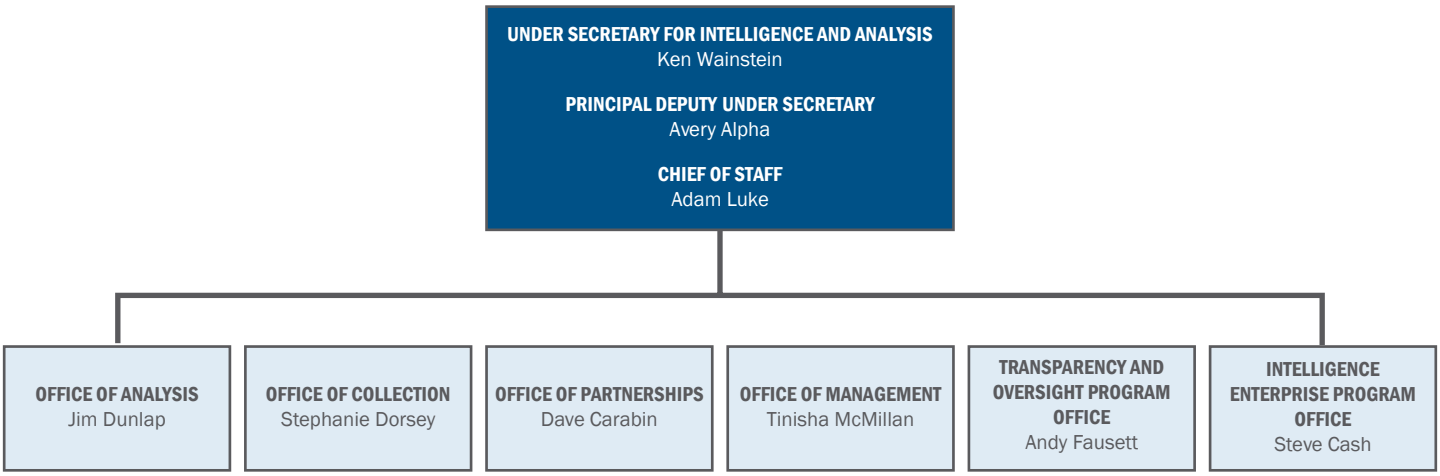
Then, we identified I&A's four primary challenges (p. 18) and addressed those challenges by (1) clarifying our vaguely defined organizational mandate; (2) accounting for our limited resources by reallocating funding and manpower from less productive to more productive intelligence pursuits; (3) differentiating our primary role of disseminating strategic intelligence from the FBI's primary role of disseminating tactical, investigative intelligence; and (4) establishing the infrastructure needed to conduct our operations with the transparency and compliance that is necessary to earn and maintain the trust of the American people.

And finally, with those changes, we are institutionalizing our four guiding principles (p. 27-28) and building an organization that recognizes that our primary consumers are our SLTTP partners; that our primary contribution is strategic-level (versus tactical-level) intelligence for those consumers; that our primary operational priority is to focus our attention and limited resources in those areas where we have distinct operational advantages; and that our primary obligation as I&A leaders is to develop the strong management culture that will empower I&A to effectively advance its homeland security mission for the American people today and in the years ahead.

While all of these changes have resulted in significant progress for the organization, we fully recognize that there is still much work to be done and many obstacles yet to overcome. With the structure provided by these changes, however, we are confident that our exceptional staff and management will continue that progress and further evolve I&A's role as the nation's homeland intelligence coordinator that Congress envisioned when it established I&A in the aftermath of the 9/11 attacks.

APPENDIX – DESCRIPTION OF I&A ORGANIZATION

With the foregoing changes in place, I&A now has the following structure:

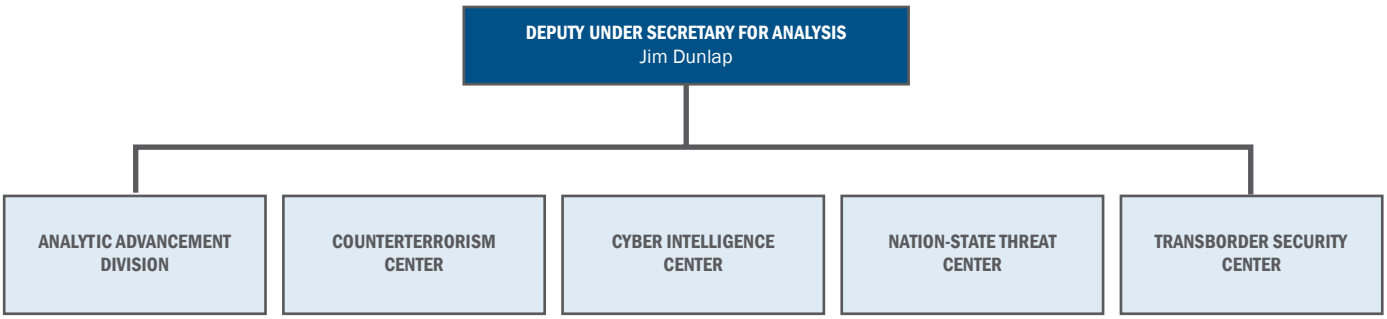


Office of Intelligence and Analysis Organizational Chart

This structure is composed of a front office and four operational offices. The front office consists of a staff that oversees executive correspondence and support and strategic communications, and two program offices—the Transparency and Oversight Program Office and the Intelligence Enterprise Program Office—that report directly to the Under Secretary. The four operational offices—the Office of Analysis, the Office of Collection, the Office of Partnerships, and the Office of Management—cover each of I&A's primary areas of operation and report to the Principal Deputy Under Secretary and to the Under Secretary.

OFFICE OF ANALYSIS

The Office of Analysis is composed of the approximately 200 analysts who author, edit, and publish I&A's finished intelligence products. It is organized around four substantive analytic centers: The Counterterrorism Center, the Cyber Intelligence Center, the Nation-State Threat



Office of Analysis Organizational Chart

Center, and the Transborder Security Center.

The analytic centers are supported by two components: (1) the Analytic Advancement Division, which reviews, edits, and publishes products to ensure they meet tradecraft standards and the needs of our partners; and (2) the Homeland Enterprise Intelligence Support team, which provides daily intelligence support and briefings to DHS leadership.

Counterterrorism Center

The Counterterrorism Center synthesizes and integrates terrorism-related intelligence, serving as the focal point for counterterrorism collaboration throughout the DHS Intelligence Enterprise. It also fields counterterrorism intelligence questions from our partners and advocates for counterterrorism intelligence equities across the interagency and the Intelligence Community.

Cyber Intelligence Center

The Cyber Intelligence Center develops cyber threat analysis to enhance the cybersecurity and resilience of the federal government, of our SLTT partners, and of our nation's critical infrastructure networks.

Nation-State Threat Center

The Nation-State Threat Center provides intelligence regarding the identification, assessment, and mitigation of threats from nation-state adversaries. Nation-State Threat Center intelligence informs foreign engagement, policy discussions, and economic security decisions for our partners. In its economic and financial analytic efforts, the Center also regularly interfaces with the Department of Treasury, the Department of Commerce, and the U.S. Trade Representative.

Transborder Security Center

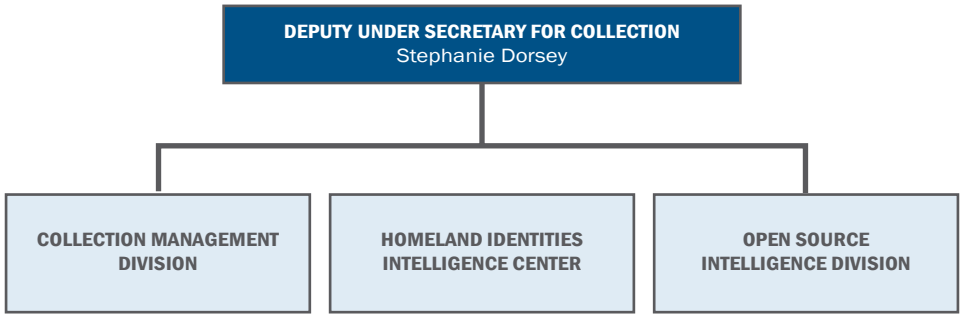
The Transborder Security Center integrates intelligence to counter transnational organized crime networks and facilitators. It focuses on transnational organized crime activities such as illicit drugs, human smuggling, weapons trafficking, and the movement of proceeds on behalf of transnational criminal enterprises.

Analytic Advancement Division

The Analytic Advancement Division conducts a variety of production and executive support functions to enable the successful delivery of I&A's intelligence to our consumers. This includes executive-level review of I&A's finished products to ensure analysis is objective, timely, relevant, and useful to a broad range of intelligence consumers. It also ensures products are well drafted and that they meet Intelligence Community tradecraft standards. Editors and graphic design artists within the Division also support the publication of I&A's products via the Department's authorized information-sharing platforms. The Homeland Enterprise Intelligence Support team

provides intelligence and briefing support to I&A and DHS Headquarters executive leadership, their staff, the DHS Intelligence Enterprise, and the broader Intelligence Community. The Analytic Advancement Division also ensures that DHS senior leaders and I&A analysts have access to relevant Intelligence Community Controlled Access Programs.

OFFICE OF COLLECTION



Office of Collection Organizational Chart

The Office of Collection collects and disseminates intelligence that provides frontline decision advantage to our key stakeholders. I&A's collection activities focus on liaison collection—collecting information directly from our SLTTP partners—open source collection, and identities intelligence to support the Department's screening and vetting efforts. The Office of Collection also provides management oversight of I&A's collection activities, including ensuring that I&A has adequate collection training and operating guidance and that compliance mechanisms are in place.

The Office of Collection is composed of three sub-offices: the Collection Management Division; the Homeland Identities Intelligence Center; and the Open Source Intelligence Division.

Collection Management Division

The Collection Management Division tracks and manages requirements—the validated intelligence needs and questions on which collectors report. It supports I&A's collection activities to ensure those requirements are addressed, and coordinates collection with the DHS Intelligence Enterprise and the Intelligence Community.

In addition, the Collection Management Division maintains I&A's Operating Directive, the annually issued guiding document outlining DHS's collection priorities, and assesses the performance of collection efforts in light of those priorities.

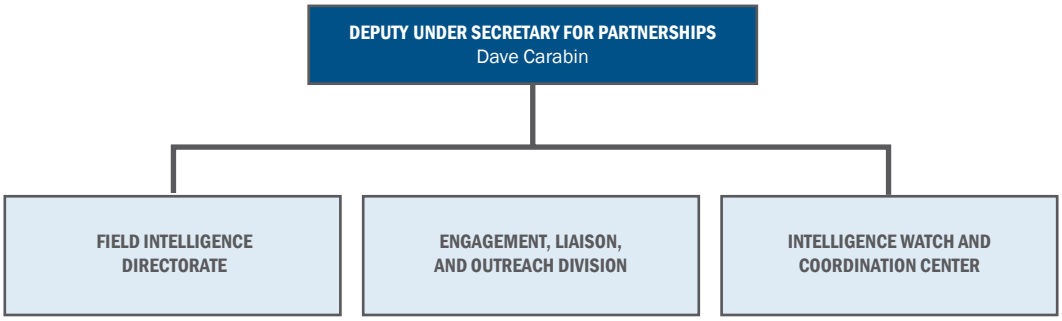
Homeland Identities Intelligence Center

The Homeland Identities Intelligence Center supports DHS's screening and vetting mission, applying advanced media exploitation methods, emerging technologies, and sound analytic tradecraft to DHS and Intelligence Community data to identify foreign and domestic actors who pose a threat to the homeland. The Center uses identities intelligence to distinguish individuals from each other; to discover new threats; and to identify connections among individuals, entities, groups, and networks of interest.

Open Source Intelligence Division

The Open Source Intelligence Division collects information from publicly available online sources based on validated collection requirements. It is organized into three branches: (1) the Cyber Branch; (2) the Terrorism Branch, and (3) the Transnational Organized Crime, Economic Security, and Counterintelligence Branch. Each branch identifies threat information relating to its area that informs our partners' security posture and finished intelligence production. Because the Open Source Intelligence Division's reporting is derived from publicly available sources, analysts can share these insights at the unclassified level, increasing their utility for I&A's SLTTP audience.

OFFICE OF PARTNERSHIPS



Office of Partnerships Organizational Chart

To better serve the needs of our SLTTP partners and maintain a strong homeland security intelligence network across the country, I&A established the Office of Partnerships in August 2022. Led by a new Deputy Under Secretary for Partnerships, the office oversees all of I&A's external relationships and supervises all deployed I&A intelligence officers.

This office is composed of three elements: the Engagement, Liaison, and Outreach Division; the Field Intelligence Directorate; and the Intelligence Watch and Coordination Center.

Engagement, Liaison, and Outreach Division

The I&A Engagement, Liaison, and Outreach Division manages strategic relationships with federal, state, local, tribal, territorial, private sector, and international stakeholders. This Division facilitates multidirectional intelligence and information sharing; assists partners with their intelligence requirements and needs; enables partner access to I&A products, resources, and expertise; and advocates on behalf of our partners to advance their homeland security equities within the Department.

It operates across five teams: the State, Local, Tribal, and Territorial Engagement Branch, the Private Sector Engagement Branch, the National Threat Evaluation & Reporting Branch, the Liaison Officer Branch, and the Foreign Liaison Branch.

State, Local, Tribal, and Territorial Engagement Branch

The State, Local, Tribal, and Territorial Engagement Branch collaborates with national-level law enforcement, emergency management, and homeland security associations, arranges briefings and seminars for our partners, and hosts the State and Local Intelligence Council—a group of practitioners from a variety of law enforcement and homeland security backgrounds that coordinates to improve the multidirectional information sharing that was lacking in the lead-up to 9/11. The Branch also regularly hosts calls with federal partners and manages HSIN-Intel,

the premier unclassified intelligence and information-sharing platform for federal and SLTT law enforcement and homeland security agencies.

Homeland Security Information Network - Intelligence

HSIN-Intel is the DHS-managed system for the sharing of Sensitive but Unclassified information, data, and intelligence products among vetted state, local, and federal partners. It provides secure online access to over 60,000 unclassified intelligence products for federal and SLTT partners on their desktops and now on their mobile phones with our new HSIN app. To support HSIN-Intel's continued membership growth and product demand, new tools and functionality have been added to the portal—including improved search, alert, and notification capabilities, a simplified and more user-friendly homepage, and a suite of data analysis tools.

Liaison Officer and Foreign Liaison Branch

The Liaison Officer program assigns experienced I&A intelligence professionals to organizations across the DHS Intelligence Enterprise, the Intelligence Community, the federal law enforcement community, and the Department of Defense. The program enhances coordination and information sharing between DHS and its interagency partners. I&A also maintains a Foreign Liaison Branch to serve as a central point of coordination for I&A-wide international engagements with foreign partners.

National Threat Evaluation and Reporting Program Office

I&A's National Threat Evaluation and Reporting Program Office provides law enforcement and homeland security partners with resources and training to assist in identifying and mitigating threats of terrorism and targeted violence. As the program and training lead for supporting the Nationwide Suspicious Activity Reporting Initiative, the office is reinvigorating and building more effective processes for identifying, evaluating, and sharing potential terrorism-related suspicious activities between SLTT and federal partners, including the FBI.

Private Sector Engagement Branch

The mission of the Private Sector Engagement Branch is to ensure that critical infrastructure owners and operators, private sector decision makers and analysts, national-level associations, and community-based organizations are equipped with the intelligence and information necessary to protect themselves against today's homeland

Chief of Staff Adam Luke gives the keynote address at the 2024 Silicon Valley Security Group Public-Private Partnership Symposium.

security threats. The Private Sector Engagement Branch hosts classified fora for partners with security clearances and unclassified Corporate Security Symposia, which connect individuals from the public and private sectors to discuss emerging security threats.

Field Intelligence Directorate

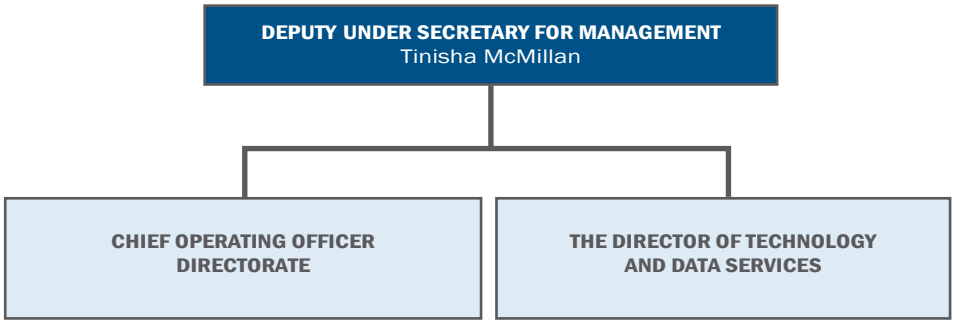
Principal Deputy Under Secretary Avery Alpha visits the U.S. Coast Guard Base Los Angeles/Long Beach in San Pedro, CA in partnership with the Field Intelligence Directorate.

I&A's Field Intelligence Directorate empowers homeland security leaders by driving multi-directional information sharing—providing intelligence briefs, responding to requests for information, supporting state and local security operations, among other things—between federal, state, local, tribal, territorial, and private sector partners and the Intelligence Community. The Directorate executes this mission through a network of approximately 150 officers assigned throughout the country—including regional directors, regional intelligence analysts, intelligence officers, and reports officers.

Intelligence Watch and Coordination Center

I&A's Intelligence Watch and Coordination Center provides 24/7 watch and warning services to DHS. It is integrated with the DHS National Operations Center to ensure DHS leaders and operations across the Department maintain situational awareness of homeland security events throughout the United States and around the world. During emerging events, the Watch produces situational reports that are shared broadly across the homeland security enterprise, including with the Secretary, the Intelligence Community, and DHS's SLTT partners. The Watch also supports I&A's analytic centers by reviewing ongoing intelligence traffic that meets I&A intelligence requirements.

OFFICE OF MANAGEMENT



Office of Management Organizational Chart

The Office of Management is composed of three directorates: the Chief Operating Officer Directorate, the Directorate of Technology and Data Services, and the Intelligence Training Academy.

Chief Operating Officer Directorate

The Chief Operating Officer Directorate is composed of the following four divisions:

Mission Assurance Division

The Mission Assurance Division manages I&A's facilities and security program. It also processes requests for security clearances from SLTTP partners.

Financial Resources Management Division

The Financial Resources Management Division oversees the annual budget process and the allocation of resources within I&A.

Program and Performance Evaluation Division

The Program and Performance Evaluation Division establishes and handles the performance management framework for I&A's operational and support functions. I&A uses the Division's analysis of financial and human resources information to inform strategic decision making, identify inefficiencies, measure I&A's performance against key milestones, keep Congress informed of its activities, and deliver performance reporting to DHS and Intelligence Community leadership.

Workforce Management and Engagement

Workforce Management and Engagement is responsible for the human resources planning, recruitment, development, and retention programs that support I&A's workforce of intelligence professionals. The team also manages I&A's employee engagement, organizational health, and diversity, equity, inclusion, and accessibility programs.

Directorate of Technology and Data Services

The Directorate of Technology and Data Services maintains systems to enable secure information sharing, collaboration, and analysis by facilitating access to data and analytics across I&A, the DHS Intelligence Enterprise, and certain Intelligence Community partners.

Business Management Division

The Business Management Division is responsible for the acquisition and budgeting to deliver information technology to support I&A.

Chief Technology Officer

The Chief Technology Officer oversees the development of technological solutions for I&A and aligns technology investment, strategy, and performance.

Cybersecurity Division

The Cybersecurity Division, led by the I&A Chief Information Security Officer, is responsible for establishing and maintaining the I&A cybersecurity program. The Cybersecurity Division establishes policy and provides guidance to I&A and other DHS components to achieve and maintain secure information systems and data. It also provides IT security services and oversight to support Sensitive Compartmented Information Facilities to ensure persistent access to classified information for our SLTTP partners.

Data Analytics and Information Sharing Division

The Data Analytics and Information Sharing Division supports our analytic efforts by providing secure and efficient access to relevant data assets and advanced analytic capabilities.

Information Technology Operations and Engineering Division

The IT Operations and Engineering Division is responsible for delivery of Top Secret/Sensitive Compartmented Information data and related capabilities to DHS stakeholders. The Division also maintains and supports the C-LAN network, DHS's Top Secret-level classified network, and the Homeland Secure Data Network, a Secret-level classified network frequently used by state and local partners.

TRANSPARENCY AND OVERSIGHT PROGRAM OFFICE

To ensure I&A conducts its mission with careful regard for privacy, civil rights, and civil liberties, the Transparency and Oversight Program Office unites all the transparency and oversight functions that were previously dispersed throughout I&A. The office is responsible for policy coordination, privacy and intelligence oversight, Freedom of Information Act requests, support to congressional oversight, Government Accountability Office and Inspector General inquiries, internal controls, and the organizational ombuds.

Policy Coordination and Oversight Branch

The Policy Coordination and Oversight Branch collaborates with offices across I&A to develop guidance that informs and shapes our operations. The Branch is also responsible for arranging I&A's policies. It ensures I&A policy memoranda are easily accessible to the workforce and maintains the I&A Policy Manual—the authoritative compendium of I&A's polices.

Privacy and Intelligence Oversight Branch

The Privacy and Intelligence Oversight Branch ensures I&A complies with its Attorney General-Approved Oversight Guidelines and minimizes the impact on individual privacy in the execution of its intelligence and homeland security missions. The Branch reviews all of I&A's finished intelligence production, facilitates oversight training for personnel, and conducts privacy impact assessments of I&A systems containing personally identifiable information. The Branch also conducts regular compliance audits and preliminary inquiries to ensure strict adherence to I&A's Oversight Guidelines.

FOIA Branch

To promote transparency with the public, the Transparency and Oversight Program Office's FOIA Branch facilitates responses to Freedom of Information Act requests that concern I&A.

Component Audit Liaison

I&A's Component Audit Liaison personnel serve as the primary points of contact for external audit organizations, including the Office of the Inspector General and the Government Accountability Office. The liaison personnel coordinate with I&A subject-matter experts to develop responses for auditors, track the progress of audit activities, and monitor the implementation of recommendations from audit reports.

Internal Controls and Enterprise Risk Management

The Internal Controls program evaluates I&A's systems, processes, and practices to help ensure we identify and appropriately mitigate risks that may compromise our ability to carry out our homeland security mission.

Ombudsmen

Ombudsmen provide a new confidential forum to discuss, informally investigate, and help resolve individual and organizational concerns. We have two full-time ombuds—one who is focused on organizational issues and another who deals with intelligence issues.

INTELLIGENCE ENTERPRISE PROGRAM OFFICE

The mission of the Intelligence Enterprise Program Office is to coordinate with the intelligence programs of other DHS components, which collectively make up the Intelligence Enterprise. The office provides strategic and administrative support to the Under Secretary in his role as the Department's Chief Intelligence Officer and thereby exercises leadership over intelligence policy making across DHS.

The Intelligence Enterprise Program Office also manages the DHS Counterintelligence Program, which focuses on protecting DHS and its personnel from adverse intelligence activities.

Enterprise Privacy and Civil Liberties Intelligence Product Reviews

For over a decade, the DHS Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties have reviewed all of I&A's finished analytic products that are disseminated outside DHS, helping to ensure compliance with applicable laws and addressing concerns related to the protection of privacy and civil liberties. 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. The Intelligence Enterprise Program Office supported the oversight offices, including the DHS Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, in helping them to establish processes for reviewing the products developed by DHS Intelligence Enterprise components for legal, privacy, civil rights, and civil liberties concerns.

Counter Threats Advisory Board

The Intelligence Enterprise Program Office has worked with the Counterterrorism Coordinator to revise our approach to the Counter Threats Advisory Board. First established in 2010 by the Secretary as the Counterterrorism Advisory Board, the Board was reconstituted and renamed following 2020 legislation that expanded the Board's remit beyond only counterterrorism to encompass all threats within the Department's mission space and designated the Under Secretary as its chair. In 2022, the Secretary directed the Counterterrorism Coordinator and the Under Secretary to retool the Board into a more effective threat coordination mechanism. We have done so, and the Board is now a more focused and directed forum for operational planning and decision making. For example, the Board was the primary forum for weekly coordination meetings for leadership and for all component principals throughout the period of heightened threat during the fall of 2024.

Homeland Security Intelligence Council

The Intelligence Enterprise Program Office has also helped to reenergize the Homeland Security Intelligence Council, which was originally established in 2005 as a coordinating mechanism for representatives of the intelligence elements of each DHS component. Within the Council are six functional boards that focus on departmental coordination of different areas of the intelligence

discipline: (1) the Analysis and Production Board; (2) the Counterintelligence and Security Board; (3) the Career Force Management Board; (4) the Collection and Reporting Board; (5) the Intelligence Systems Board; and (6) the Strategy, Planning, and Resources Board. Each of these boards is co-chaired by a representative from I&A and one from a Component Intelligence Program.

The leadership of the Intelligence Enterprise Program Office has dramatically improved the operation of the Homeland Security Intelligence Council, evolving it from a forum where components provided primarily rote updates to one that generates meaningful Enterprise coordination and actionable policy decision making. Since October 2023, the Council has completed budget guidance for the components, developed a plan to standardize intelligence training, and improved information sharing to combat counterintelligence threats to the Department, among other initiatives.

Homeland Security