

OFFICE OF INTELLIGENCE AND ANALYSIS  
**STRATEGIC PLAN**

FY 2020-2024



Homeland  
Security





# Homeland Security



I am pleased to publish the Office of Intelligence & Analysis Strategic Plan for Fiscal Years 2020-2024. This document provides a holistic approach that will guide the continued evolution of the Office over the next five years and serves as a foundational document for how DHS Intelligence executes its broad mission and vision. Following the September 11th, 2001 terrorist attacks, the Homeland Security Act of 2002 created the Department of Homeland Security and the Implementing Recommendations of the 9/11 Commission Act of 2007 established the Office of Intelligence & Analysis as the first federal agency statutorily mandated to share intelligence with state, local, tribal, and territorial law enforcement, as well as the private sector—creating the necessity for a comprehensive approach and strategy to Homeland security.

I&A provides timely, actionable intelligence to a far-reaching base of customers and partners—from the DHS Secretary and Components, policymakers, and the Intelligence Community to an expansive network of state, local, tribal, territorial, and private-sector partners with both national and global influence. Therefore, this strategy outlines a forward-leaning approach to provide dominant capabilities and anticipatory intelligence to meet the diverse needs of DHS partners, customers, and stakeholders.

The threat environment is never static, thus I&A will remain dynamic in its actions to combat the challenges of today, as well as the future, through partnerships, information sharing, and a concrete understanding of the evolving landscape at home and beyond our Nation's borders. Terrorist networks continue operations to inspire and mobilize those in our country, transnational criminal organizations seek to exploit our borders, and state and non-state cyber actors target our critical infrastructure, information networks, and the American people; all of these threats will be met with our most forceful and innovative efforts to repel all threats to the Homeland. This strategy further develops I&A's contributions to national security as a member of the Intelligence Community while simultaneously outlining this Office's activities to integrate and strengthen Department of Homeland Security Intelligence capabilities.

To reiterate my commitment to empowering DHS Intelligence professionals, I&A developed this strategy using vital input of I&A employees as well as contributions from internal and external stakeholders. I am committed to investing in the DHS workforce to develop premier Homeland Intelligence professionals, truly the most important factor in delivering superior intelligence capabilities in our fight against hostile actions that threaten American security, prosperity, and values that are the fabric of our Nation.

Thank you for your continued support as we work to foster a collaborative environment and continue to bridge the gaps between the federal government, the Intelligence Community, and our state, local, tribal, territorial, and private-sector partners. It is imperative that we evolve together, as a unified community, to provide the most comprehensive and robust protection possible for the American people.

A handwritten signature in black ink, appearing to read "David J. Glawe".

**David J. Glawe**  
Chief Intelligence Officer  
Under Secretary for  
Intelligence and Analysis

# OPERATING PRINCIPLES



**Foster** a fully synchronized, cohesive enterprise that integrates intelligence into operational functions and drives action through Mission Centers to mitigate all threats to the Homeland including Counterintelligence, Counterterrorism, Cyber, Economic Security, and Transnational Organized Crime.

**Deliver** Intelligence Community (IC) capabilities, access to data and systems, infrastructure, analytic expertise and mission readiness services to DHS Operational Components.

**Invest** in our people, who are critical for achieving the above operating principles, by continuously enhancing our talent and leadership development to foster a cadre of high-performing Homeland Security Intelligence Professionals.

**Drive** multi-directional information exchanges with State, local, tribal, territorial, private sector (SLTTP), and foreign partners to fill critical information and intelligence gaps.

**Ensure** unique DHS datasets are available to Mission Centers, the IC and law enforcement partners to bolster whole-of-government efforts to counter threats.

**Produce** strategic intelligence products that leverage law enforcement, unique DHS data and IC holdings to facilitate intelligence-driven decision making by all levels of DHS leadership, other U.S. Government (USG) policymakers, and SLTTP partners.

**Provide** unique immigration, travel, and intelligence data, analytic tools, analysis, and technical infrastructure to assist the USG stand-up of the National Vetting Center.



# Homeland Security

# I&A Mission, Vision, and Value Statements

## I&A Mission

Equip the Homeland Security Enterprise (HSE) with timely intelligence and information needed to keep the Homeland safe, secure, and resilient.

## I&A Vision

A dominant and superior intelligence enterprise, driving intelligence integration and information sharing, and delivering unique intelligence and analysis to operators and decision-makers at all levels to identify and mitigate threats.

## I&A Values

- **Vigilance:** We relentlessly identify threats that pose a danger to our Homeland or threaten American values and our way of life.
- **Respect:** We highly value the relationships we build with our customers, partners, and stakeholders. We honor concepts, such as liberty and democracy, for which America stands.
- **Integrity:** Each of us serves something far greater than ourselves. We demonstrate integrity in our conduct, faithful to the duties and responsibilities entrusted to us; we maintain the highest ethical and professional standards, while being mindful that all of our actions, whether public or not, should reflect positively on the Intelligence Community (IC) and Department at large.
- **Mission:** We serve the American people, and understand that our mission requires selfless dedication to the security of our Nation and fellow citizens.
- **Truth:** Through an analysis of all available information, we seek to provide intelligence objectively, and exhibit the moral courage to speak truth to power.
- **Lawfulness:** We support and defend the Constitution, and comply with the laws of the U.S., ensuring that we carry out our mission in a manner that respects privacy, civil liberties, and civil rights.
- **Stewardship:** We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, and protect intelligence sources and methods diligently.
- **Accountability:** We are accountable to ourselves, our oversight institutions, and to the American people. At all levels, we report wrongdoing through appropriate channels, and will not retaliate against whistleblowers.
- **Excellence:** We continuously seek to improve our performance and our tradecraft, share information responsibly, collaborate productively with colleagues, and demonstrate innovation and agility when faced with new challenges.
- **Diversity:** We embrace the wealth of experiences, perspectives, and talents that derive from the diverse background of our Nation, and promote understanding, inclusion, and respect throughout our workforce.



# Homeland **Strategic Environment**

---

## **I&A Strategic Environment**

The strategic environment for Homeland security includes critical threats from transnational criminal organizations, terrorism, hostile nation-states, cyber threats, and emerging disruptive technologies. I&A must continuously adapt, enabling the HSE to comprehensively respond to an evolving threat landscape and focus on proactive resiliency. Nefarious actors are increasingly capable of penetrating digital and physical borders, threatening the balance of power of the international system, and instantly exploiting power vacuums around the globe.

**Transnational criminal organizations** will continue to conduct larger and more sophisticated activities across international borders and into the U.S. interior that encompass smuggling illicit goods, illegal movement of people, and financial and logistical support networks that exist in both physical and virtual environments. Transnational organized crime remains a concern as it threatens U.S. public health and safety, undermines the integrity of government institutions in partner nations, interferes with legitimate commerce, and exploits vulnerable populations.

**Terrorists**, both foreign and domestic, will continue to attempt to carry out attacks against U.S. citizens and infrastructure. Advances in technology will continue to allow terrorists to use social media, anonymous and encrypted messaging applications, and online forums to recruit, radicalize, and inspire individuals inside the U.S. to plot attacks, and to provide material support. U.S.-based homegrown violent extremist attacks are likely to continue to occur with little or no warning, because perpetrators are able to remain undetected by law enforcement, and often strike soft targets using simple tactics that do not require advanced skills or outside training.

**Hostile nation-states** pose significant challenges as they continue asserting themselves through all elements of national power such as economic trade, espionage, and cyber-attacks that seek to undermine the interests of the U.S. and its democratic institutions, processes, and values. In addition to cyber-attacks that involve intrusions of networks and infrastructure, hostile nation-states will continue to expand their capabilities, including the use of disinformation campaigns.

**Cyber adversaries and criminals** are increasingly using cyberspace to threaten national and economic security interests. They will continue using cyber capabilities—including espionage, influence, and attack—to seek political, economic, and military advantages over the U.S. and our allies. Nation-state adversaries and competitors, including those developing cyber-attack

capabilities against critical infrastructure, will increasingly build and integrate cyber operations into their efforts to influence U.S. policies, and advance their own national interests. Non-state cyber criminals will continue to conduct for-profit, cyber-enabled theft and extortion against U.S. public and private-sector networks, sometimes with disruptive effects to core operations. More broadly, U.S. adversaries will conduct enduring online influence operations in an attempt to weaken democratic institutions, undermine U.S. alliances and partnerships, and shape policy outcomes in the U.S. and elsewhere.

**Global threat actors and adversarial nations** continue to undermine our national and economic security through sustained efforts that threaten America’s innovation, economy, and competitiveness, the livelihoods of U.S. workers, and, in some cases, the health and safety of consumers. Antagonistic trade practices, such as intentionally misidentifying or misclassifying goods to evade detection, or falsely repackaging or re-labeling products as originating in a third country, will continue to undercut the competitiveness and profitability of U.S. companies. This situation ultimately leads to losses in the U.S. manufacturing industry and unemployment. Additionally, retaliatory trade practices and asymmetrical enforcement efforts by adversarial nations will continue to undermine the U.S. government’s efforts to promote equitable customs and trade enforcement globally, expand U.S. and global economic prosperity, and protect U.S. national security and economic interests.

**Emerging disruptive technologies** continue to outpace legislation and countermeasures across the Homeland. Unmanned aerial systems (UAS) will continuously enable transnational criminal organizations and criminals to carry out cross-border drug smuggling operations. Actors will continue to use UAS to conduct surveillance of law enforcement, and potentially facilitate kinetic attacks on stationary, mobile, and high-consequence targets. Additionally, nefarious actors are increasingly acquiring new capabilities, and enhancing their use of technology previously only accessible to nation-state actors.

The I&A Strategic Plan 2020-2024 ensures I&A is properly positioned to keep our customers and partners informed of an ever-changing threat environment. During this era of dynamic threats that cross borders in both the physical and digital arenas, I&A will continue to ensure it is positioned to provide intelligence and information on transnational organized crime, terrorism, cyber-threat actors, counterintelligence vulnerabilities, economic security, and other developing threats that pose a critical danger to the Nation’s security and our democratic way of life.



# Foundational **Mission Goals**

---

The foundational mission goals address the three types of intelligence that I&A produces—anticipatory, strategic, and operational. These three types of intelligence transcend the various threats and topics that I&A analyzes and collects against for partners and customers. Together, these three goals represent I&A’s central and comprehensive intelligence missions.


**Anticipatory Intelligence** addresses new and emerging trends, changing conditions, and underappreciated developments.

**Strategic Intelligence** addresses issues of enduring national security.

**Operational Intelligence** supports planned and ongoing operations.

## **Executive Order 12333**

**National Intelligence and Intelligence Related to National Security means all intelligence, regardless of the source from which derived and including information gathered within or outside the U.S., that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director to pertain to more than one U.S. Government agency; and that involves threats to the U.S., its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on U.S. national or Homeland security.**







## Anticipatory Intelligence

With the global environment rapidly changing, and threats to the Homeland ever evolving, I&A seeks to continuously develop new insights, and notify policymakers and operators about new trends and changing conditions. Through promoting subject-matter expertise, enhancing collection efforts, expanding DHS datasets, and by pro-actively alerting customers, I&A will enhance the ability of DHS and further enable the capabilities of the DHS Intelligence Enterprise, IC, SLTTP, and foreign partners to anticipate and respond to new threats that negatively impact the Homeland.

### **Goal 1.1:** Identify new trends and changing conditions to alert customers and prepare for emerging threats to the U.S. Homeland.

- **Objective 1.1.1:** *Expand analysis and collection to identify and assess emerging trends, changing conditions, and issues that affect the security of the Homeland.*
- **Objective 1.1.2:** *Increase subject-matter expertise and tradecraft to generate new insights, and address intelligence analytic and collection gaps.*
- **Objective 1.1.3:** *Strengthen integrated capabilities to proactively and efficiently provide timely and relevant warning of developing trends and changing conditions, enabling DHS leadership, operational component, SLTTP, and foreign government partners' responses.*

Anticipatory intelligence involves collecting and analyzing information to identify emerging trends, changing conditions, potential trends, and underappreciated developments that challenge long-standing assumptions, encourage new perspectives, and provide warning of new opportunities and threats to the U.S. Homeland and interests. Anticipatory intelligence usually leverages a cross-disciplinary approach and often utilizes specialized tradecraft to identify emerging issues surrounding intelligence gaps and conflicting information, cope with high degrees of uncertainty, and consider alternative futures. Anticipatory intelligence may uncover previously unconnected groups or regions, and include indicators or benchmarks to identify key developments as trends change over time. It assesses risk, intelligence gaps, and uncertainties by evaluating the probability of occurrence and potential effects of a given development on the security of the Homeland.



## Strategic Intelligence

I&A will continue enhancing its knowledge of the global environment—including cultural, political, and economic factors—and the intentions and capabilities of nation-state and non-state actors to inform Homeland and national security policy and operations. Additionally, I&A will work with the IC, DHS Components, and SLTTP partners, invest in DHS datasets, and enhance tradecraft to produce comprehensive assessments, including joint-seal production, to hinder the threat posed by foreign intelligence entities, terrorist organizations, malevolent cyber actors, transnational criminal organizations, and malicious foreign actors that violate trade laws and evade sanctions.

**Goal 1.2:** Prioritize the development and maintenance of an understanding of threats to the U.S. Homeland, enhance collaborative efforts with partners, and expand the production of assessments to further a comprehensive understanding of the strategic environment of the Homeland.

- **Objective 1.2.1:** Provide tailored, strategic assessments about the Homeland environment to inform decision making in the HSE and throughout the federal government.
- **Objective 1.2.2:** Increase and promote production of joint-seal products between I&A, the Intelligence Enterprise, and external DHS partners to provide the HSE customers with greater awareness and certainty in their decision making.
- **Objective 1.2.3:** Expand and retain subject-matter expertise to obtain an in-depth understanding of transnational and domestic threats to the U.S. Homeland.

Strategic intelligence is the process and product of developing the context, knowledge, and understanding of the strategic environment required to support U.S. Homeland security policy and planning decisions. This work includes identifying and assessing the capabilities, activities, and intentions of states and non-state entities to identify risks to and opportunities for U.S. Homeland security. Strategic intelligence involves assimilating a variety of information—including knowledge of political, diplomatic, economic, and security developments—to create a deep understanding of issues of enduring importance to the U.S. Homeland. Strategic intelligence also provides in-depth assessments of trends and developments to recognize and warn of changes related to issues that will affect the future strategic environment.



## Operational Intelligence

I&A will respond to the needs of DHS, IC, and SLTTP operators so they can plan and conduct operations to protect the Homeland. I&A will partner with our operational customers to increase collaboration, develop a deeper understanding of their needs and the threat, and produce analysis and information that gives our customers an operational advantage.

**Goal 1.3:** Provide tailored intelligence, using unique DHS intelligence, information, and other data, and increase collaboration to enable federal and SLTTP operations to prevent threats to the U.S. Homeland and interests.

- **Objective 1.3.1:** *Deliver relevant and timely analysis and collection to enable DHS, SLTTP, and other federal operations.*
- **Objective 1.3.2:** *Strengthen I&A's coordination and communication with the HSE to attain and preserve operational decision advantage.*
- **Objective 1.3.3:** *Expand collaboration opportunities to support and maintain mutual awareness of DHS, SLTTP, and other federal operations.*

Operational intelligence is the collection, analysis, and planning support provided to federal and SLTTP partners to enable successful planned and ongoing operations. Operational intelligence includes the intelligence necessary to support the time-sensitive needs of HSE customers in times of crisis, but also provides opportunities to shape future operations and desired operational outcomes.



## Topical Mission Goals

---

The topical mission goals, supported by the foundational mission goals, focus on the enduring threats to the Homeland. These five goals represent I&A's partners' and customers' most significant needs, and are inclusive of specific regional and functional threats.

**Counterintelligence** addresses threats from foreign intelligence entities and implements appropriate countermeasures.

**Counterterrorism** addresses state and non-state actors engaged in terrorism and related activities to impact the Homeland or U.S. interests.

**Cyber** addresses state and non-state actors participating in malevolent cyber activities.

**Economic Security** addresses threats from foreign actors to undermine U.S. economic competitiveness.

**Transnational Organized Crime** addresses transnational criminal activities that threaten the U.S. Homeland and our interests.

### **Homeland Security Act of 2002**

***Directs I&A to integrate relevant information, analyses, and vulnerability assessments (whether...provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.***



## Counterintelligence

The current and emerging counterintelligence challenges facing DHS and the HSE require an integrated, whole-of-Department response. Rapid technological advances allow a broad range of Foreign Intelligence Entities (FIE) to field increasingly sophisticated capabilities, and aggressively target the government, private-sector partners, and academia. FIEs are proactive and use creative approaches—including the use of cyber tools, malicious insiders, espionage, and supply chain exploitation—to advance their interests and gain advantage over the U.S. These activities intensify traditional FIE threats, place U.S. critical infrastructure at risk, erode U.S. competitive advantage, and weaken our global influence. In order to effectively identify and assess current and future FIE efforts targeting DHS and the HSE, I&A will drive innovative counterintelligence solutions, further integrate counterintelligence responses into Department business practices, advance Component integration, effectively resource programmatic efficiencies, and continuously assess and refine counterintelligence programs to ensure the HSE remains relevant, responsive, and effective.

### **Goal 2.1:** Expand counterintelligence coordination across DHS, SLTTP, and federal partners to rapidly recognize the contemporary threat environment, identify vulnerabilities, and implement appropriate countermeasures.

- **Objective 2.1.1:** Advance integrated IE intelligence activities and collection, including operationalizing DHS-wide datasets, to develop insights and improve understanding of evolving FIE threats against the U.S. Homeland and interests.
- **Objective 2.1.2:** Increase the production of all-source counterintelligence analytic products on FIE threats, at the lowest classification possible, and joint analytic efforts on FIEs to support counterintelligence activities.
- **Objective 2.1.3:** Operationalize DHS datasets using data as a service, developing and implementing new intelligence capabilities, to strategically target foreign intelligence operations against the HSE.
- **Objective 2.1.4:** Increase DHS counterintelligence education and awareness training to identify and report FIE threats against the HSE and the IC.
- **Objective 2.1.5:** Practice and promote comprehensive, integrated, and unified DHS counterintelligence activities to create a robust DHS-wide counterintelligence program.
- **Objective 2.1.6:** Increase interaction with SLTTP on FIE threats to critical infrastructure, enabling SLTTP partners to implement appropriate countermeasures.

A FIE is any known or suspected foreign state or non-state organization or persons that conduct intelligence activities to acquire information about the U.S., block or impair intelligence collection by the U.S. Government, influence U.S. policy, or disrupt systems and programs owned or operated by or within the U.S. The term includes foreign intelligence and security services, international terrorists, transnational criminal organizations, and drug trafficking organizations conducting intelligence-related activities.



## Counterterrorism

The evolving nature of domestic and international terrorist threats facing the U.S. requires an equally adaptable response, particularly regarding our travel and border security. I&A plays an integral role in providing strategic and operational analysis using unique DHS data and support from the DHS Intelligence Enterprise, to inform policy makers, as well as our SLTTP partners of the threats we face in the Homeland from all forms of extremism.

### **Goal 2.2:** Detect terrorists and collaborate with partners on operations to prevent terrorist attacks against the U.S. Homeland, U.S. persons, and U.S. interests.

- **Objective 2.2.1:** *Expand collection, and improve efficiency of analysis, providing timely intelligence to mitigate terrorist threats and reduce vulnerabilities in the Homeland.*
- **Objective 2.2.2:** *Enhance the dissemination of terrorism-related intelligence, at the lowest classification possible, enabling policymakers' and operational decision makers' efforts to disrupt terrorist attacks and planning.*
- **Objective 2.2.3:** *Enhance coordination, synchronization, and timeliness of counterterrorism analysis focused on DHS equities and shared with federal and SLTTP partners to institutionalize relationships and detect nefarious activities and terrorist threats to the Homeland.*

Counterterrorism intelligence is the collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign terrorist organizations and violent extremists, intentions, capabilities, research and development, tactics, targets, operational activities and indicators, and their impact or potential effects on U.S. national security interests. Counterterrorism intelligence also includes information and assessments on threats to potential vulnerabilities to U.S. critical infrastructure, policies, and programs, including travel and immigration practices and border security.



## Cyber

Advanced and persistent actors will continue their efforts to conduct cyber-enabled operations against U.S. Government, critical infrastructure, and SLTTP networks. Additionally, foreign actors will likely continue engaging in malicious influence operations. These operations are often intended to undermine confidence in democratic institutions, degrade democratization efforts, and influence public sentiment by disseminating false information via state-controlled media and overt online personas. I&A will continue providing intelligence to identify cyber threats, protect federal, SLTTP information systems and critical infrastructure, and deter cyber incidents effectively.

### **Goal 2.3:** Detect and understand cyber threats to identify and mitigate risks across DHS, the federal government, and the HSE.

- **Objective 2.3.1:** *Develop new insights into emerging foreign influence operations and cyber threats to remedy risks within federal and SLTTP cyber realms and critical infrastructure.*
- **Objective 2.3.2:** *Integrate intelligence, information, and other data from DHS, the IC, and SLTTP partners with existing protective capabilities to improve investigations, and deter and counter malicious cyber actors and activities.*
- **Objective 2.3.3:** *Expand joint production and dissemination of finished and raw intelligence, at the lowest classification level possible, to mitigate threats, enhance DHS and federal cyber-incident response, and prevent additional harm.*

Cyber threat intelligence is the collection, processing, analysis, and dissemination of information from all intelligence sources on foreign actors' influence operations, cyber capabilities, and the effects on U.S. and SLTTP security interests. Cyber threat intelligence also includes information on cyber threat actor information systems, infrastructure, and data; and network characterization, or insight into the components, structure, use, and vulnerabilities of foreign cyber program information systems.



## Economic Security

DHS's role in ensuring the uninterrupted flow of goods, services, people, capital, information, and technology across our borders is critical. The systems and structure that make this flow possible are targeted for exploitation by our adversaries, and DHS remains responsible for identifying vulnerabilities. Specifically, DHS has a role in identifying fraudulent trade activities, retaliatory trade practices, the evasion of customs enforcement, and the circumvention of financial sanctions, which all undermine the U.S.'s efforts to promote fair and equitable customs and trade enforcement globally.

### **Goal 2.4:** Identify and understand foreign economic threats and engage DHS, other federal, and SLTTP partners to inform Homeland policy deliberations that preserve and enhance the competitiveness of the U.S. economy.

- **Objective 2.4.1:** *Develop new insights and improve understanding of malicious foreign actors who violate and evade U.S. law to deter and counter illicit economic activity.*
- **Objective 2.4.2:** *Expand tailored analysis and collection on evolving threats to critical infrastructure and the economic security of the U.S., at the lowest classification level possible, and operationalize DHS-wide data sets to achieve and maintain the U.S.'s economic decision advantage.*
- **Objective 2.4.3:** *Promote collection and analysis of economic security information of DHS, other federal, and SLTTP partners to enable diplomatic and law enforcement operations for upholding and enforcing U.S. and international trade laws.*

Economic security represents the ability of a nation to protect its sovereignty by affording military protection, extending diplomatic relations, engaging in international trade, exercising its internal system of governance, and protecting the innovations and intellectual property of its citizens.





## Transnational Organized Crime

Transnational organized crime (TOC) continues to pose enduring challenges to the U.S., including threats to public safety, public health, and economic stability. The scope of DHS's mission and authorities places DHS in a unique position to target the threat posed by TOC. DHS, with a combination of border, immigration, maritime, and cybersecurity protection and investigative authorities, is uniquely placed to prevent transnational criminal organizations (TCOs) from entering, remaining in, and/or operating within in the U.S. These efforts must continue to be integrated into and informed by the intelligence process, furthering the effectiveness of DHS's extensive authorities. Given this position, I&A will work to bring DHS data together and provide the intelligence data available to the HSE collaborating with the IC, the DHS IE, DHS Components, other government agencies, foreign partners, and SLTTP partners.

### **Goal 2.5:** Enhance understanding of tactics, trends, and actors to combat transnational criminal activities that threaten the U.S. Homeland and interests.

- **Objective 2.5.1:** *Broaden and deepen strategic knowledge of regime and geopolitical landscapes, and TCO network exploitation of those dynamics, to provide customers with a decision advantage and support regional stabilization.*
- **Objective 2.5.2:** *Expand tailored analysis and collection, at the lowest classification level possible, enabling DHS, other federal, and SLTTP operations to counter illicit movement of contraband and illegal migrants entering the U.S.*
- **Objective 2.5.3:** *Enhance the identification of national and regional TOC actors to disrupt or dismantle TOC networks.*

TOC refers to crime committed by self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary or commercial gains, wholly or in part by illegal means—while protecting their activities through a pattern of corruption/violence or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. TOC networks vary widely in their structure, from loose affiliations of criminals, to centralized, hierarchical organizations.



# Enterprise Goals

---

The eight enterprise goals focus on the mission and business practices of I&A. These goals integrate partners' and customers' needs enabling the successful completion of the topical and foundational mission goals.

**Homeland Security Enterprise Analytic and Collection Activities** seeks to integrate analytic and collection requirements to enhance response to partner and customer needs.

**Homeland Security Enterprise Integration of Personnel** seeks to build well-rounded Homeland Intelligence professionals.

**Partnerships** seeks to enhance I&A's support to partners through greater collaboration.

**Information Sharing and Safeguarding** addresses collaboration and integration in accordance with applicable laws and policies.

**People** seeks to develop a collaborative and unified organization where ideas and people are respected.


**Privacy, Civil Liberties, and Transparency** seeks to protect U.S. values and enhance accountability, trust, and confidence.

**Technological Innovation** seeks to increase information access and data resiliency through new technologies and innovative application.

**Business Functions** addresses I&A business processes crucial to mission success.

**Under Secretary Glawe, June 2017**

***I&A has one of the broadest customer bases among intelligence agencies, ranging from the DHS Secretary and Components; policymakers; the US Intelligence Community; thousands of state, local, and private sector officials; and foreign partners—each of whom have different mission, information, and classification requirements. I&A will continue to meet their diverse needs by producing a broad range of usable intelligence products for strategic and tactical use.***





## Homeland Security Enterprise Analytic and Collection Activities

I&A seeks to strike a balance between an integrated effort and specialization, using the best of each organization to meet mission objectives. Integrated analytic and collection efforts drive collaboration, create efficiencies, and optimize resource decisions, enabling our customers and partners to operationalize intelligence and more effectively execute their missions.

### **Goal 3.1:** Integrate analytic and collection requirements across the IE to support departmental and SLTTP partners.

- **Objective 3.1.1:** Institutionalize Intelligence Community Directives as DHS standards, as appropriate, to standardize DHS Intelligence activities.
- **Objective 3.1.2:** Enhance the DHS Program of Analysis (POA) to synchronize analytic lines of effort across the Department.
- **Objective 3.1.3:** Leverage the collections governance framework to build and institutionalize a comprehensive, integrated, and unified DHS-wide collection program.
- **Objective 3.1.4:** Identify, document, and integrate DHS customer intelligence priorities, including from SLTTP partners, to influence federal and SLTTP analytic and collection priority frameworks, products, activities, and operations.
- **Objective 3.1.5:** Develop Homeland Unifying Intelligence Strategies to improve use of unique DHS data, enhance efficiency of analysis, and prioritize collection across the Department.

Effective mission execution requires unified, comprehensive, and responsive efforts to share information and intelligence across organizational boundaries. I&A will synchronize and integrate analytic and collections efforts to meet customer needs.



## Homeland Security Enterprise Integration of Personnel

I&A will lead the effort to implement effective tools and resources that harmonize, synchronize, and integrate workforce planning, continuous learning, and the sharing of subject-matter expertise. Additionally, I&A needs to guide the IE in making long-term strategic investments in the workforce to promote agility and mobility throughout employees' careers, including rotations, and ensure other development opportunities and customer needs are fully considered and/or implemented wherever feasible.

### **Goal 3.2:** Create and implement synchronized approaches to improve the skills and integration of Homeland Intelligence professionals.

- **Objective 3.2.1:** Increase exchange of personnel between I&A, the IC, the IE, and SLTP to strengthen coordination, communication, processes, and awareness of customer needs and capabilities.
- **Objective 3.2.2:** Develop DHS Intelligence career roadmaps, which reflect the full spectrum of development opportunities, to mature Homeland Intelligence professionals.
- **Objective 3.2.3:** Establish additional opportunities for IE personnel at IC agencies to provide career development opportunities for Homeland Intelligence professionals.
- **Objective 3.2.4:** Optimize DHS Intelligence training to minimize redundancy, and ensure employees obtain common foundational intelligence training at every level in their career, creating an agile intelligence workforce that meets the future needs of our employees and the IE's customers.

Successful mission execution requires a flexible, resilient, and interchangeable intelligence workforce with common core knowledge, skills, and abilities that promote agility and mobility throughout employees' careers.



# Partnerships

I&A's partnerships are critical to successfully protect the U.S. Homeland. Through leveraging their unique capabilities, the wealth of data they provide, and exceptional insights, our partners are indispensable to our mission. I&A will continue to strengthen our existing partnerships and cultivate new ones to produce world class intelligence and inform our decision makers.

### **Goal 3.3:** Expand and strengthen partnerships to enrich intelligence, inform decisions, and enable actions throughout the Homeland Security Enterprise.

- **Objective 3.3.1:** Reinforce existing and create new opportunities for engagement with public-private coordination bodies to develop more opportunities for cooperation with the private sector.
- **Objective 3.3.2:** Enhance follow-up opportunities for tailored intelligence assessments with SLTTP to increase frequency and broaden partnerships post engagement.
- **Objective 3.3.3:** Promote the linkage between fusion centers and field-based partners, including, but not limited to, federal and SLTTP, to develop relationships and enhance collaboration.
- **Objective 3.3.4:** Institutionalize relationships with SLTTP partners to reduce the impact of future organizational changes.

I&A's partners are governments, agencies, organizations, and entities working with us to advance Homeland security priorities, including state, local, tribal, and territorial officials, DHS Component entities, private-sector stakeholders, other federal departments and agencies, and IC counterparts.



## Information Sharing and Safeguarding

Mission success depends on the right people getting the right information at the right time to inform decision making. To do this, I&A will take a cutting-edge approach to appropriately access information, regardless of where the information resides. Information that is better organized into appropriate data formats, and tagged with metadata to increase its quality and usability, will aid the transition to information-centered intelligence processes.

### **Goal 3.4:** Increase collaboration, expand standardization of data, and improve tools to better serve the Department's information sharing and safeguarding, in accordance with applicable laws and policies.

- **Objective 3.4.1:** Increase access and shareability of data with the Department, IC, and SLTTP partners to promote integration and inform a comprehensive situational awareness and understanding of the threat landscape, as appropriate, with organizational authorities.
- **Objective 3.4.2:** Create additional common enterprise technological tools to accelerate the standardization of data, provide the ability to efficiently and effectively integrate HSE data and other sources in accordance with applicable laws and policy, and rapidly deliver data and analytic results with the appropriate protections.
- **Objective 3.4.3:** Leverage the exchange of personnel between I&A, Department, IC, and SLTTP partners to increase the quantity and application of information shared.
- **Objective 3.4.4:** Expand partner access to analysis and collection, at the lowest classification level possible, to broaden the dissemination of unique DHS intelligence, information, and data.

The Under Secretary for Intelligence and Analysis (USIA) serves as the Department's Senior Information Sharing and Safeguarding Executive.



## People

Protecting and preserving the Homeland can only be achieved with a professional, trusted, agile, and well-led workforce. I&A personnel will adhere to the Principles of Professional Ethics for the IC. Effective and innovative approaches are crucial to recruiting, retaining, developing, and motivating employees who possess skills that are fundamental to the intelligence mission, including critical thinking, effective communication, and data literacy. I&A will have effective tools and resources that integrate workforce planning, transformational leadership, continuous learning, information sharing, performance management, and accountability.

### **Goal 3.5:** Empower and develop all levels of the DHS Intelligence workforce to build a collaborative and respectful organization dedicated to protecting the U.S. Homeland.

- **Objective 3.5.1:** Advance efforts to prevent discrimination, harassment, and fear of reprisal to create an inclusive environment, ensuring all managers and employees take ownership for organizational diversity.
- **Objective 3.5.2:** Promote greater exchange opportunities for I&A personnel within I&A, as well as across the DHS IE and SLTTP, to create well-rounded Homeland Intelligence professionals.
- **Objective 3.5.3:** Establish and promote information exchanges within and between all parts of the organization to enable greater collaboration and hold all employees and leadership accountable.
- **Objective 3.5.4:** Increase awareness of and access to professional development opportunities across the IE in order to continue developing Homeland Intelligence professionals.
- **Objective 3.5.5:** Create opportunities for rotating and nurturing high performers throughout the organization to develop a cadre of I&A employees prepared for formal leadership roles.
- **Objective 3.5.6:** Promote and institute employee decision making by respecting employee expertise, keeping employees informed and involved with leadership decisions to create a leadership culture that empowers employees at the lowest possible level.
- **Objective 3.5.7:** Institutionalize the organization's diversity so that it mirrors the customers it serves and encourage diversity of thought, experiences, and backgrounds to strengthen mission execution.
- **Objective 3.5.8:** Mature workforce planning efforts and human capital processes across I&A to more effectively attract, retain, and develop Homeland Intelligence professionals with the requisite skills to meet current and emerging threats.

The people of I&A all bring a wealth of varied experiences that are essential attributes directly supporting organizational success. The backgrounds and capabilities of our workforce are vital to the intellectual diversity needed to inform our customers.



## **Privacy, Civil Liberties, and Transparency**

I&A will uphold American civil liberties, and practice transparency, both internally and externally. Committing to the core principles of transparency results in mission success for I&A in upholding the country's values and protecting the American people and our way of life. Fulfilling our bond with the American people allows I&A to gain the public's trust, which directly impacts our authorities, capabilities, and resources.

### **Goal 3.6: Protect privacy and civil liberties and strengthen transparency to foster accountability, trust, and confidence with our partners and the public.**

- **Objective 3.6.1:** *Enhance integration of privacy, civil rights, and civil liberties requirements across I&A to ensure that our national values inform the DHS Intelligence mission.*
- **Objective 3.6.2:** *Proactively engage with oversight institutions and partners to enhance understanding and confidence in I&A.*
- **Objective 3.6.3:** *Practice and encourage transparency, throughout the DHS IE, to make information publicly available without compromising Homeland or national security.*
- **Objective 3.6.4:** *Institutionalize communication methods to promote transparency of intelligence activities across the HSE.*

The Intelligence Community's Principles of Intelligence Transparency provides I&A with a framework to follow when making information publicly available and available to our partners across the SLTP sectors. I&A's goal is to create finished intelligence products at the lowest classification level for the widest dissemination possible. This practice allows the public to understand intelligence activities affecting the Homeland while I&A continues to protect information, that if improperly disclosed, would harm national security.





## Technological Innovation

In order to continue to be a leader in the development of secure and efficient architectures that support the Department and our operational partners, I&A will continue to innovate through an iterative process that advances original proposals and concepts to solve our most significant problems. I&A will keep abreast of current and emerging technologies and be a leader in the development of secure and efficient architectures that support the Department and our operational partners.

### **Goal 3.7:** Promote technological advancements, securing and modernizing systems, to increase information access and data resiliency throughout the Homeland Security Enterprise allowing peak performance.

- **Objective 3.7.1:** Develop and implement innovative technology solutions and leverage emerging technologies that integrate HSE, IC, and SLTTP data, empowering the workforce to develop new insights into continually evolving and sophisticated threats against the Homeland and U.S. interests.
- **Objective 3.7.2:** Establish and continually upgrade technical and data management frameworks, life-cycle programs, and policies to support the integration of Department, IC, and SLTTP partners' activities and improve collection, exploitation, reporting, and dissemination of intelligence, information, and data across the HSE.
- **Objective 3.7.3:** Modernize and secure technical system infrastructure and architectures with a cloud-first approach, optimizing performance of IT systems and ensuring technical functionality, to enable maximum performance of DHS Intelligence personnel.
- **Objective 3.7.4:** Enhance cybersecurity and information assurance compliance to ensure the security and protection for the Department's intelligence systems and data.
- **Objective 3.7.5:** Integrate machine learning and artificial intelligence platforms into the IT infrastructure to solve DHS Intelligence enterprise challenges.

Innovation is the relentless pursuit of technological advancements, novel solutions, and securing and modernizing systems. Innovation is critical to DHS's mission of ensuring increased information access and secure data integration within the HSE, the IC, and SLTTP.



## Business Functions



I&A will enhance business integration and organizational resiliency through the efficient use of capital and facilities. Improving performance evaluation, acquiring additional shared services, and implementing industry standards will improve accountability and productivity. Additionally, it will enhance cooperation throughout the office to foster modernization and ensure I&A effectively applies resources.

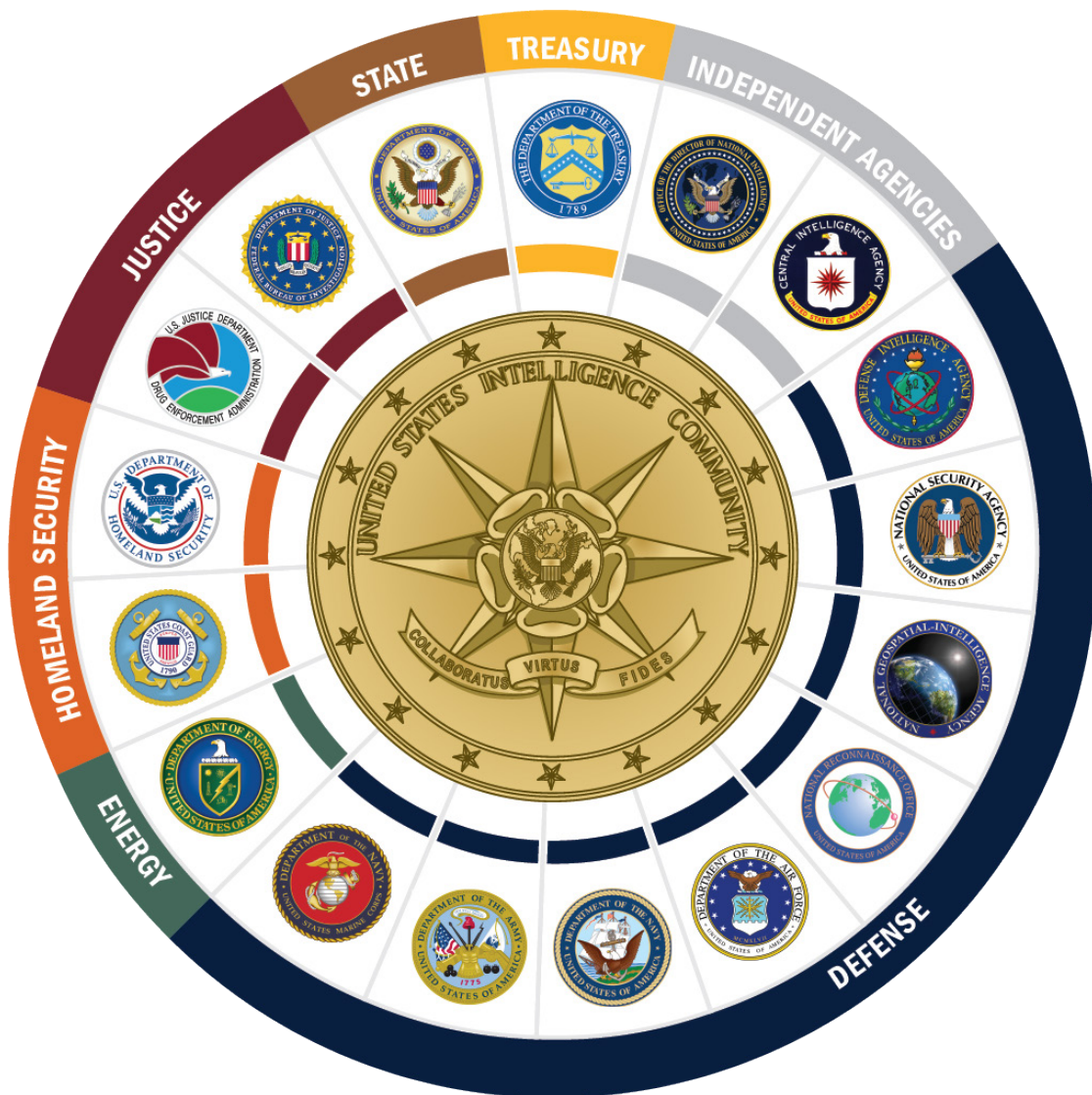
### **Goal 3.8:** Enhance I&A business functions to enable mission success.

- **Objective 3.8.1:** Enhance data-driven performance evaluation across I&A to enable informed business decisions, and ensure strategic and efficient application of resources.
- **Objective 3.8.2:** Advance financial standards, processes, tools, and services to achieve fiscal efficiency, transparency, accountability, and security.
- **Objective 3.8.3:** Improve integration and transparency of acquisition and procurement across I&A to improve organizational efficiency and agility of acquiring and procuring products and services.
- **Objective 3.8.4:** Practice disciplined risk management and continuity activities to enable organizational resilience and sustain critical mission capabilities under all conditions.
- **Objective 3.8.5:** Enhance facilities and logistics through innovative processes to increase efficiency, joint-use functionality, and shared services.

Business functions and practices enable I&A to perform across multiple missions, responsibilities, and operations. This includes the coordinated development, alignment, de-confliction, execution, and monitoring of plans and procedures needed to manage and secure I&A and its people, information technology, and physical infrastructure.

# I&A *within the U.S.* Intelligence Community

The Office of Intelligence and Analysis, as one of 17 Intelligence Community agencies and organizations, is the only IC agency statutorily charged with delivering intelligence to our state, local, tribal, territorial, and private-sector partners, and developing intelligence from those partners for the Department and the IC. I&A develops this intelligence through our partnerships with the Homeland Security Enterprise and other IC agencies. In addition to utilizing traditional IC and federal relationships to share this information, I&A has a vast network of state, local, tribal, territorial, and private-sector partners, with whom we work in the field every day, ensuring vital Homeland and national security information is collected and shared at every level of government.

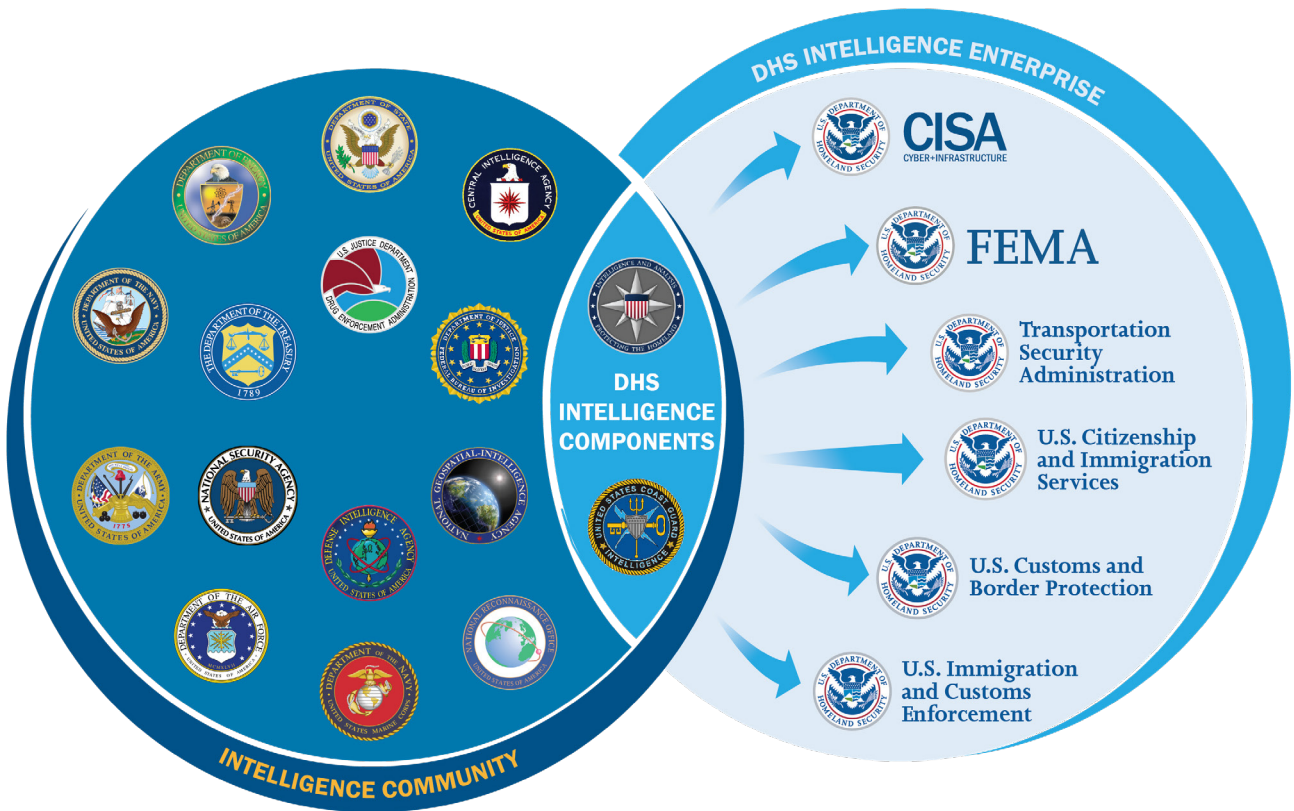


# I&A within the DHS Intelligence Enterprise

The Office of Intelligence and Analysis (I&A) partners with the DHS Intelligence Enterprise (IE) to develop a comprehensive approach for addressing intelligence needs to protect the Homeland. To accomplish this goal, I&A works with the IE through the Homeland Security Intelligence Council (HSIC), the DHS advisory body that assists the DHS Chief Intelligence Officer (CINT), in evaluating and determining the best course of action for the Department’s national and Homeland Intelligence functions. The CINT also coordinates several boards on analysis and production, collection, and training, enabling the Department to better address Homeland Intelligence needs as one team.

The IE is made up of the Office of Intelligence & Analysis (I&A), U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Transportation Security Administration (TSA), U.S. Coast Guard (USCG), Federal Emergency Management Agency (FEMA), Countering Weapons of Mass Destruction (CWMD), and Cybersecurity and Infrastructure Security Agency (CISA). While not a chartered member of the DHS IE, the U.S. Secret Service (USSS) is an integral part of the Departmental intelligence process, offering unique resources for the Secretary of Homeland Security. USSS serves on the HSIC at the CINT’s request.

I&A also benefits from information shared by other DHS Components who are not formally part of the IE, but whose insight and perspectives help shape our collection, analysis, and overall mission of protecting the Homeland.



# Aligning **I&A's Strategic Plan**



NSS

## National Security Strategy

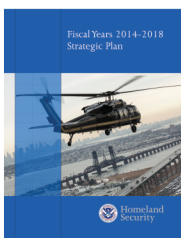
The National Security Strategy (NSS) outlines the major national security priorities of the United States. The NSS provides the President's high-level strategic vision for protecting the American people and preserving our way of life. The document is purposely general in content and its implementation relies on elaborating guidance provided in supporting documents such as the National Intelligence Strategy (NIS).

## Departmental Strategic Guidance

The DHS Quadrennial Homeland Security Review (QHSR) and the DHS Strategic Plan are capstone strategy documents that offer guidance on long-term strategy and priorities across the Homeland Security Enterprise.



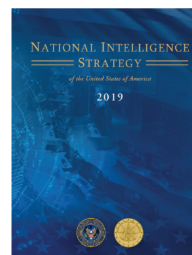
QHSR



DHS

## National Intelligence Strategy

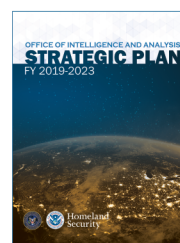
The NIS provides the IC with the mission direction of the Director of National Intelligence for the next four to five years. The NIS also provides strategic guidance for the development of individual IC element plans.



NIS

## I&A Strategic Plan

The I&A Strategic Plan focuses on organizational goals, objectives, and initiatives. It is aligned with higher-level guidance provided by both the IC and Departmental strategic plans. Additionally, the I&A Strategic Plan is equivalent to other IC element strategic documents (e.g., Defense Intelligence Agency, Department of the Treasury's Office of Intelligence and Analysis).



I&A

## Departmental Intelligence Strategic Guidance and Annual Budget Request

The I&A Strategic Plan provides guidance to documents such as the DHS Counterintelligence Strategy, as well as the development and long-term adoption of the Homeland Unifying Intelligence Strategies. Strategic programmatic guidance drives funding, to include I&A's budget submission to Congress.

# Implementing the I&A Strategic Plan

## FY 2020-2024



The I&A Strategic Plan will succeed through the dedicated work of I&A and its partners throughout the HSE. I&A developed this plan through gathering feedback from our employees and a wide-range of our partners and customers, drawing from national and departmental strategies, and utilizing the subject-matter expertise of dozens of I&A employees representing a totality of the organization. Going forward, I&A will continue as a partner-focused, flexible, and dynamic organization empowered to provide vital information and intelligence to partners at all levels of the government and private sector.

**Strategic Alignment** - I&A will integrate the goals and objectives into the other strategies and plans written using the Under Secretary's authorities. I&A will also incorporate this Strategic Plan's goals and objectives into other Departmental, IC, and federal strategies, as necessary, while I&A employees at all levels will incorporate and align their activities to this Strategic Plan.

**Implementation Plans** - I&A will develop an implementation plan, revising annually, to ensure the Office completes the necessary steps in each year of the Strategic Plan and accomplishes the goals by 2024.

**Performance Evaluation** - I&A will monitor implementation through gathering and analyzing performance metrics on a regular basis. I&A leadership will use these metrics to make periodic adjustments, as necessary, to ensure I&A makes substantial progress annually towards accomplishing the goals and objectives, therefore meeting the needs of our employees, partners, and customers.

**Drive I&A Budget and Resource Allocation** - I&A will use this Strategic Plan to allocate resources throughout the Office, enabling leadership to ensure I&A's investments best support Homeland security goals and objectives. Additionally, I&A will utilize this plan when developing justifications in future budget requests.



