United States Government Accountability Office

Report to the Ranking Member, Committee on Homeland Security, House of Representatives

August 2023

HOMELAND SECURITY

Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Its Effectiveness

GAO-23-105475

GAO Highlights

Highlights of GAO-23-105475, a report to the Ranking Member, Committee on Homeland Security, House of Representatives

August 2023

HOMELAND SECURITY

Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Its Effectiveness

Why GAO Did This Study

The DHS Office of Intelligence and Analysis provides information to DHS components and other partners to identify and mitigate threats to homeland security. Because such reporting can involve information about U.S. persons, the office issued Intelligence Oversight Guidelines that identify safeguards to protect privacy, civil rights, and civil liberties.

GAO was asked to review how the office sets priorities; protects privacy, civil rights, and civil liberties; and assesses its effectiveness. This report examines (1) how the office prioritizes threats, (2) the extent to which it monitors implementation of its Intelligence Oversight Guidelines, and (3) the extent to which it assesses its effectiveness.

GAO assessed the office's monitoring activities against its guidelines, reviewed performance information, and interviewed officials and a nongeneralizable selection of partners. This included eight DHS intelligence components, seven state and local agencies, and three private-sector partners, selected on the basis of geographic location and other factors.

What GAO Recommends

GAO is making nine recommendations, including that the Office of Intelligence and Analysis (1) identify who is responsible for conducting audits of information systems and bulk data and ensure these audits are conducted, (2) develop performance measures that clearly align with strategic goals, and (3) assess the extent to which customer feedback data improve its understanding of customers' interests. The Department of Homeland Security agreed with our recommendations.

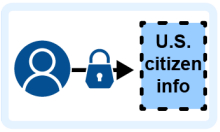
View GAO-23-105475. For more information, contact Triana McNeil at (202) 512-8777 or mcneilt@gao.gov.

What GAO Found

GAO found that the Department of Homeland Security (DHS) Office of Intelligence and Analysis collected input from its mission centers and partners to prioritize threats and guide intelligence production during fiscal years 2019 to 2022. Specifically, the office (1) integrated Intelligence Community priorities into a single framework; (2) coordinated with DHS intelligence components to prioritize threats identified in that framework; and (3) solicited input from state, local, and other partners to refine priorities and inform product development.

GAO also found that the Office of Intelligence and Analysis is not fully implementing activities intended to monitor whether personnel are following its policies to protect the privacy, civil rights, and civil liberties of U.S. persons, including U.S. citizens and lawful permanent residents. For example, the office has not conducted two required monitoring activities: audits of information systems and audits of bulk data.

Audits Required by the Intelligence Oversight Guidelines



Audits of information systems
The DHS Office of Intelligence and Analysis is to take reasonable steps to audit information systems containing information about U.S. persons—including U.S. citizens and lawful permanent residents—to assess whether personnel (1) had appropriate security clearances and met other requirements to access these systems, and (2) tailored their queries to minimize the amount of information returned about U.S. persons.

Audits of bulk data[a]
The DHS Office of Intelligence and Analysis is to audit bulk data transferred to or from the DHS Office of Intelligence and Analysis to assess whether personnel's access to, and searches conducted in, these data were appropriately limited to protect privacy, civil rights, and civil liberties.

Source: Department of Homeland Security, Office of Intelligence and Analysis, *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines*, Instruction IA-1000 (Jan. 19, 2017), GAO (icons). | GAO-23-105475

[a]Bulk data are large quantities of data acquired without the use of discriminants (e.g., specific identifiers or search terms), most of which does not have intelligence value.

The office has not identified who is responsible for conducting these audits. By doing so, and by ensuring that relevant staff conduct these audits, the office will be better positioned to address any failures to protect privacy, civil rights, and civil liberties within its information systems and bulk data transfers.

The Office of Intelligence and Analysis tracks 13 performance measures, but it lacks information about its effectiveness because the performance measures do not clearly align with its strategic goals. For example, the office does not have a performance measure relating to its strategic goal of protecting privacy and civil liberties or of promoting technological innovation. Developing performance measures that clearly align with its strategic goals would give leadership information about the office's overall effectiveness.

In addition, officials said the office intends to use data from questionnaires attached to its intelligence products to better understand its customer interests. However, the office has not assessed whether these data are fulfilling its intent. By conducting such an assessment, the office may be better positioned to produce intelligence that aligns with the interests and needs of its customers.

Contents

Letter		1
	Background	5
	I&A Used Input from Its Mission Centers and Partners to Prioritize Threats	12
	I&A Is Not Fully Monitoring Implementation of Its Intelligence Oversight Guidelines	17
	I&A Lacks Information to Fully Assess Its Effectiveness	27
	Conclusions	33
	Recommendations for Executive Action	33
	Agency Comments	34
Appendix I	Prior GAO and Office of Inspector General Recommendations to the Office of Intelligence and Analysis	36
Appendix II	Office of Intelligence and Analysis Policies and Procedures to Protect Privacy, Civil Rights, and Civil Liberties	41
Appendix III	Office of Intelligence and Analysis Performance Measures and Strategic Goals	50
Appendix IV	GAO Leading Practices for Strategic Planning and Performance Management	54
Appendix V	Agency Comments	56
Appendix VI	GAO Contact and Staff Acknowledgments	61
Tables		
	Table 1: Office of Intelligence and Analysis (I&A) National and Departmental Missions	6

Table 2: Privacy, Civil Rights, and Civil Liberties Safeguards in the Office of Intelligence and Analysis (I&A) Intelligence Oversight Guidelines 11
Table 3: GAO Recommendations to the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A), Fiscal Year 2023 36
Table 4: Department of Homeland Security (DHS) Office of Inspector General (OIG) Recommendations to the DHS Office of Intelligence and Analysis (I&A), Fiscal Year 2022 39
Table 5: Privacy, Civil Rights, and Civil Liberties Safeguards in the Office of Intelligence and Analysis (I&A) Intelligence Oversight Guidelines 41
Table 6: Office of Intelligence and Analysis (I&A) National and Departmental Missions 43
Table 7: Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Performance Measures, Targets, and Results Reported to DHS and the Office of the Director of National Intelligence (ODNI), Fiscal Years (FY) 2020 through 2022 50
Table 8: Alignment between Department of Homeland Security (DHS) Office of Intelligence and Analysis's (I&A) Strategic Goals and Performance Measures 52

Figures

Figure 1: Organizational Chart of Key Entities within the Office of Intelligence and Analysis (I&A) Involved in Intelligence Production and Oversight Activities 8
Figure 2: The Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Partners 9
Figure 3: The Department of Homeland Security Office of Intelligence and Analysis's Process to Assess Threats and Identify Priorities 15
Figure 4: The Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Process for Gathering Input to Prioritize Threats and Guide Product Development for Fiscal Years 2019 through 2022 17
Figure 5: Preliminary Inquiries Completed by the Department of Homeland Security Office of Intelligence and Analysis from January 2017 through September 2022 22

Figure 6: Audits of Information Systems and Audits of Bulk Data Required by the Office of Intelligence and Analysis (I&A) Intelligence Oversight Guidelines 25
Figure 7: Leading Practices for Aligning Strategic Goals and Performance Measures 28
Figure 8: Review Process for Office of Intelligence and Analysis (I&A) Finished Intelligence Products 44
Figure 9: Review Process for Office of Intelligence and Analysis (I&A) Open-Source Intelligence Reports 46

Abbreviations

DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
I&A	Office of Intelligence and Analysis
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

August 28, 2023

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Dear Mr. Thompson:

The civil unrest in Portland, Oregon, in the summer of 2020 and the attack on the U.S. Capitol on January 6, 2021, highlight the importance of disseminating threat information in a timely manner to mitigate violence and other threats to homeland security.[1] Within the Department of Homeland Security (DHS), the Office of Intelligence and Analysis (I&A) is responsible for supporting DHS's mission by providing its partners with timely, accurate, and insightful intelligence to identify and mitigate threats to homeland security.[2] I&A also serves as a member of the U.S. Intelligence Community and is responsible for supporting intelligence-related programs, projects, and activities.[3]

To fulfill its responsibilities, I&A collects and analyzes information to provide intelligence products and briefings to various partners, including federal, state, and local government entities. Because these products and briefings may include information about U.S. persons, I&A developed mandatory procedures for handling information concerning U.S. persons and required that staff be trained to implement them.[4] In 2017, I&A issued

[1]In the summer of 2020, some protestors in Portland, Oregon, threatened or committed violence against federal employees and property.

[2]See 6 U.S.C. § 121. See also Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 2.1.

[3]The U.S. Intelligence Community is composed of 18 elements: two independent agencies (the Office of the Director of National Intelligence and the Central Intelligence Agency); nine elements within the Department of Defense; and seven elements of other departments and agencies, including I&A.

[4]Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 2.3. This requirement applies to all Intelligence Community elements that collect, retain, or disseminate information about U.S. persons. A U.S. person is: (1) a U.S. citizen, (2) a foreign national known by the intelligence element to be a lawful permanent resident, (3) an unincorporated association substantially composed of U.S. citizens or permanent residents, or (4) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. See id.¶ 3.5(k).

these procedures—titled Intelligence Oversight Guidelines—with the stated purpose of protecting privacy, civil rights, and civil liberties.[5]

Despite these guidelines, in July 2020, I&A created and disseminated intelligence products about U.S. journalists' activities that the DHS Office of the General Counsel later found did not comport with its policies for protecting privacy, civil rights, and civil liberties.[6] In addition, we and the DHS Office of Inspector General (OIG) have reported on issues relating to I&A's protection of privacy, civil rights, and civil liberties, as well as the timeliness of I&A's intelligence production and information-sharing. For example, we and the OIG reported that I&A identified specific threat information prior to the January 6 attack but did not issue intelligence products about these threats until after the attack occurred.[7] Appendix I summarizes recent recommendations relating to the issues discussed in this report and actions I&A has taken to implement them.

You asked us to review issues related to I&A's protection of privacy, civil rights, and civil liberties and I&A's effectiveness. This report examines (1) how I&A prioritizes threats to guide the development of its products, (2) the extent to which I&A monitors the implementation of its guidelines to safeguard privacy, civil rights, and civil liberties, and (3) the extent to which I&A assesses its effectiveness. You also asked us to provide specific information about policies and procedures that I&A has

[5]Department of Homeland Security, Office of Intelligence and Analysis, *Intelligence Oversight Guidelines* (Washington, D.C.: Jan. 2017).

[6]Specifically, the DHS Office of the General Counsel found that the journalists' actions were First-Amendment-protected activities. See Department of Homeland Security, Office of the General Counsel, *Report on DHS Administrative Review into I&A Open Source Collection and Dissemination Activities During Civil Unrest: Portland, Oregon, June through July 2020* (Washington, D.C.: Jan 6, 2021). The First Amendment to the U.S. Constitution protects the freedoms of speech, press, association, and assembly, among others. U.S. Const. amend. I. The government generally may not prohibit speech because of its message, ideas, subject matter, or content—even speech that may be viewed by some as offensive or disagreeable. The term "civil liberties" refers to certain rights under the U.S. Constitution, which protect individuals' freedom from undue governmental interference or restraint.

[7]GAO, *Federal Agencies Identified Some Threats, but Did Not Fully Process and Share Information Prior to January 6, 2021,* GAO-23-106625 (Washington, D.C.: Feb. 28, 2023) and Department of Homeland Security, Office of Inspector General, *I&A Identified Threats Prior to January 6, 2021, but Did Not Issue Any Intelligence Products Before the U.S. Capitol Breach*, OIG-22-29 (Washington, D.C.: Mar. 4, 2022).

established to safeguard privacy, civil rights, and civil liberties, which is included in appendix II.

To address the first objective, we reviewed documents relating to I&A's threat prioritization and product development processes starting in fiscal year 2019—when I&A implemented a new prioritization process—through September 2022, the end of the most recent complete fiscal year. These were the most current documents available at the time of our review.

To address the second objective, we reviewed I&A's Intelligence Oversight Guidelines and its accompanying policy instruction, both of which focus on the protection of privacy, civil rights, and civil liberties.[8] We evaluated I&A's implementation of the monitoring activities identified in these documents against *Standards for Internal Control in the Federal Government* and *The Standard for Program Management*.[9] We determined that the control environment component of internal control was significant to this objective, along with the underlying principles that (1) management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives; and (2) management should design control activities to achieve objectives and respond to risks. We reviewed documentation relating to I&A's monitoring activities conducted between January 2017—when the Intelligence Oversight Guidelines took effect—through September 2022, the end of the most recent complete fiscal year at the time of our review. These documents included reports about compliance reviews and other inquiries, draft operating procedures relating to these activities, and assessments of privacy-protection mechanisms in I&A's information systems. In some cases, I&A provided us summaries of documents for our review; we note in the report when our findings reflect I&A summaries versus our review of actual documents.

To address the third objective, we reviewed I&A's performance measures, targets, and results for fiscal years 2020 through 2022 and customer feedback data from October 2017 through May 2022. These were the most recent data available at the time of our review. We assessed the reliability of these performance data by reviewing relevant documentation

[8]Department of Homeland Security, Office of Intelligence and Analysis, *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines,* Instruction IA-1000 (Washington, D.C.: Jan. 19, 2017).

[9]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014); The Project Management Institute, Inc. (PMI®), *The Standard for Program Management*, 4th ed., (Newtown Square, PA: 2017).

and interviewing knowledgeable officials about how they collect and use the data. We determined that the data were sufficiently reliable to report on I&A's performance data and customer feedback. We also reviewed I&A's fiscal year 2020–2024 strategic plan. We evaluated I&A's performance measures using I&A's policy instruction for strategic planning and leading practices for agencies to enhance the use of performance information in decision-making.[10]

To address all three objectives, we interviewed I&A officials responsible for threat prioritization; privacy, civil rights, and civil liberties protection; and performance measurement.[11] We also interviewed officials in the DHS Intelligence Enterprise, the Intelligence Law Division of the DHS Office of the General Counsel, the DHS Privacy Office, and the DHS Office for Civil Rights and Civil Liberties.[12]

To address our first and third objectives, we interviewed a nongeneralizable selection of 10 state, local, and private sector I&A partners, including six fusion centers, one local law enforcement agency, and three private sector representatives from critical infrastructure

[10]DHS Office of Intelligence and Analysis, *DHS Intelligence & Analysis Planning, Programming, Budgeting, and Evaluation*, Policy Instruction IA-301 (Nov. 20, 2013). DHS Office of Intelligence and Analysis, *Strategic Plan Fiscal Year (FY) 2020–2024* (Washington, D.C.: Feb. 6, 2020). GAO, *Managing for Results*: *Enhancing Agency Use of Performance Information for Management Decision Making,* GAO-05-927 (Washington, D.C.: Sept. 9, 2005). To identify the practices described in this report, we reviewed relevant literature (including our prior reports), spoke to experts in using performance information, and held group discussions with federal program managers.

[11]For example, we interviewed officials from I&A's Intelligence Enterprise Management Branch, Privacy and Intelligence Oversight Branch, and Program and Performance Evaluation Division.

[12]The DHS Intelligence Enterprise is headed by the Under Secretary for Intelligence and Analysis, who also holds the position of DHS Chief Intelligence Officer. It is composed of I&A and the intelligence components of the following DHS entities: the Countering Weapons of Mass Destruction Office, the Cybersecurity and Infrastructure Security Agency, the Federal Emergency Management Agency, Federal Protective Service (within the Management Directorate), the Transportation Security Administration, U.S. Citizenship and Immigration Services, U.S. Coast Guard, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement.

sectors.[13] We selected state and local entities that serve large populations and to reflect a range of geographic locations. We selected sectors that most frequently use I&A information from among the sectors that have DHS as their sole Sector Risk Management Agency.[14] For each sector, we interviewed representatives of the relevant Sector Coordinating Council, Information Sharing and Analysis Center, or both.[15] Although this selection is not generalizable, the interviews provided valuable insight into I&A's partners' perspectives on I&A's priorities and performance.

We conducted this performance audit from November 2021 to August 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

I&A's Mission, Authorities, and Organization

In addition to its role as a member of the Intelligence Community, I&A supports DHS's mission in a number of ways, such as by accessing, receiving, analyzing, and integrating the intelligence needed to identify and assess threats to homeland security.[16] To accomplish its mission, I&A personnel are authorized to conduct intelligence activities when they

[13]Fusion centers are state-owned and -operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information between state, local, tribal, territorial, federal, and private sector partners. There are 80 fusion centers across the country. The U.S. government has designated 16 critical infrastructure sectors whose assets, systems, and networks are vital to national security and health.

[14]We obtained information on the sectors that most frequently use I&A products from the Cybersecurity and Infrastructure Security Agency. The Cybersecurity and Infrastructure Security Agency is the national coordinator for critical infrastructure security and resilience. Sector Risk Management Agencies are responsible for providing specialized expertise to improve the security and resilience of each critical infrastructure sector.

[15]Sector Coordinating Councils enable critical infrastructure industry representatives to interact on sector-specific strategies, policies, and activities. Information Sharing and Analysis Centers deliver all-hazards threat and mitigation information to critical infrastructure owners and operators.

[16]See 6 U.S.C. § 121(d)(1). As discussed, I&A is a member of the U.S. Intelligence Community and has responsibilities for supporting Intelligence Community programs.

have a reasonable belief that doing so would support one or more national or departmental missions (see table 1).

Table 1: Office of Intelligence and Analysis (I&A) National and Departmental Missions

I&A personnel are authorized to engage in intelligence activities when they have a reasonable belief that doing so would support one or more national or departmental missions.[a]

National Missions	Departmental Missions
Assist executive branch officials in developing and conducting foreign, defense, and economic policies, or protecting national interests from foreign security threats. Foreign security threats include • international terrorism; • the development, proliferation, or use of weapons of mass destruction; • intelligence activities directed against the U.S.; • international criminal drug activities; and • other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents. National missions may also include assisting Congress, as appropriate.	Assist public or private sector entities in identifying protective and support measures regarding threats to homeland security. Such threats include • domestic terrorism; • threats to critical infrastructure and key resources; • significant threats to national economic security, public health, or public safety; • major disasters and other catastrophic acts; and • severe, large-scale threats for which the response is beyond the capabilities of affected state and local governments. Departmental missions also include support provided to DHS officials, offices, or elements in the execution of their lawful missions. For example, I&A supports U.S. Customs and Border Protection's inspection of travelers at U.S. ports of entry.

Source: Department of Homeland Security Office of Intelligence and Analysis, Intelligence Oversight Guidelines (Washington, D.C.: Jan. 2017). | GAO-23-105475

[a]I&A's Intelligence Oversight Guidelines define reasonable belief as a belief based on facts and circumstances such that a reasonable person would hold that belief. A reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge as applied to particular facts and circumstances. According to I&A officials, this definition is consistent across the U.S. Intelligence Community.

To support these national and departmental missions, I&A personnel are authorized to collect information either overtly—including from I&A's federal, state and local (including law enforcement), and private sector partners—or through publicly available sources.[17] Overt collection consists of activities that are openly acknowledged by, or readily attributable to, the U.S. government, or that would be acknowledged in response to a direct inquiry. For example, I&A personnel assigned to fusion centers work with state and local partners, including law enforcement agencies, to identify and report information to I&A and other Intelligence Community elements. Publicly available information, in general, is information that is published or broadcast for public consumption, available on request to the public, accessible online or

[17]Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 1.7(i); 6 U.S.C. § 121(d)(1).

otherwise to the public, or available to the public by subscription or purchase.[18]

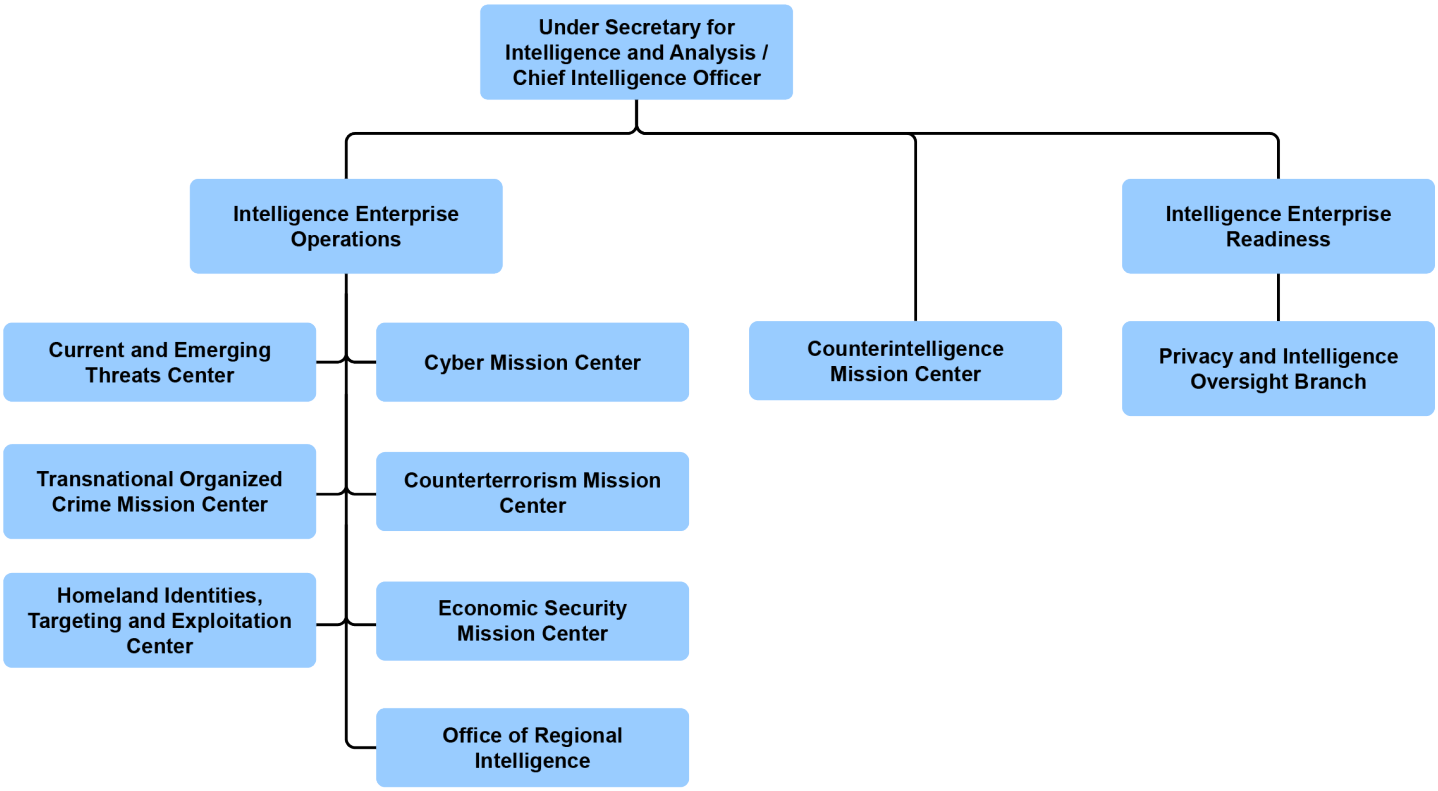
During the period of our review, I&A had eight organizational units that produced intelligence products: five mission centers, each of which focused on a topical area (e.g., cybersecurity), and three additional operational units.[19] In addition, I&A's intelligence oversight branch—led by the Intelligence Oversight Officer—had key responsibilities for ensuring that I&A protects individuals' privacy, civil rights, and civil liberties.[20] Key elements of I&A's structure, as relevant to this report, are shown in figure 1.

[18]In addition, publicly available information includes information that could be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event open to the public. Social media sites and other electronic fora that limit access by use of criteria that cannot generally be satisfied by members of the public are not publicly available sources.

[19]I&A underwent a realignment in May 2023, during which it changed the names and structure of some mission centers and other units.

[20]I&A officials told us that the May 2023 realignment did not impact the functions of the intelligence oversight branch or the responsibilities of the Intelligence Oversight Officer.

Figure 1: Organizational Chart of Key Entities within the Office of Intelligence and Analysis (I&A) Involved in Intelligence Production and Oversight Activities



Source: GAO analysis of DHS information. | GAO-23-105475

Note: This graphic represents I&A's organization as of March 2022. I&A underwent a realignment in May 2023, during which it changed the names and structure of some mission centers and other units.

I&A Products and Partners

I&A aims to provide timely, relevant, and actionable intelligence for operational and policy-level decision-making. To accomplish this, I&A generally produces and disseminates two types of products: (1) raw intelligence reports and (2) finished intelligence products. Raw intelligence reports contain unanalyzed content that is the same or substantially the same as when I&A acquired it. An example of a type of raw intelligence report is an Open-Source Intelligence Report, which may contain text or images copied from social media about specific plans for acts of violence.

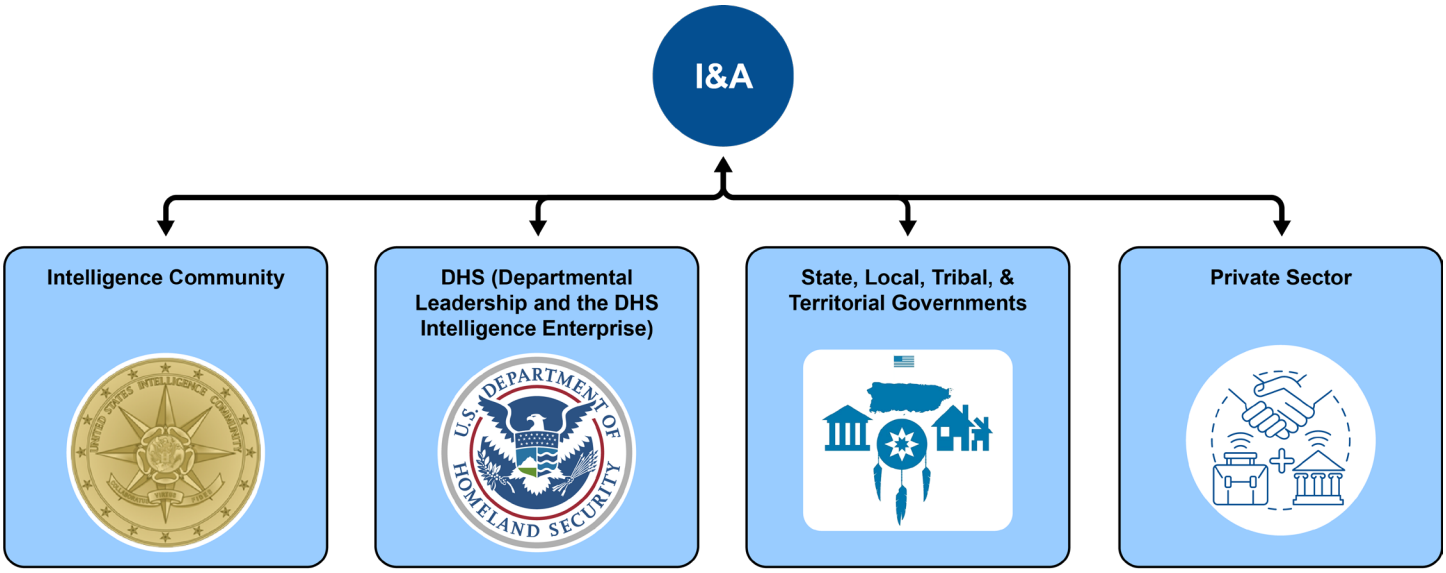
Finished intelligence products contain the assessment, judgment, or other analytic input of I&A personnel. To produce finished intelligence products,

analysts integrate, evaluate, and analyze information, and they generally coordinate with other agencies on these products. For example, I&A's Intelligence in Depth products analyze multiple angles of an issue, provide a forecast of what may unfold in the future, and identify key drivers and indicators relating to the issue.

Among other responsibilities, I&A is to disseminate, as appropriate, information analyzed by DHS within the department and to federal, state, local, and private sector entities with responsibilities relating to homeland security (see fig. 2).[21]

Figure 2: The Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Partners

I&A receives information from and provides information to members of the Intelligence Community and the DHS Intelligence Enterprise, as well as state, local, tribal, territorial, and private sector partners. I&A also provides information to DHS leaders.



Source: GAO analysis of DHS information, U.S. Intelligence Community, U.S. Department of Homeland Security, GAO (icons). | GAO-23-105475

Notes: The U.S. Intelligence Community is composed of 18 federal agencies, including I&A. The DHS Intelligence Enterprise is composed of I&A and the intelligence offices and entities of nine DHS components (e.g., the Cybersecurity and Infrastructure Security Agency). I&A's state, local, tribal, and territorial partners are government agencies, including law enforcement agencies. I&A's private sector partners include critical infrastructure industry organizations and associations. DHS officials told us that I&A also shares information and intelligence with foreign entities.

I&A disseminates information and products to its partners via in-person briefings and various information-sharing networks. For example, I&A uses DHS's Homeland Security Information Network, which DHS created

[21] 6 U.S.C. § 121(d)(6).

to share sensitive but unclassified information between federal, state, local, territorial, tribal, international, and private sector partners.

Protection of Privacy, Civil Rights, and Civil Liberties and the Intelligence Oversight Guidelines

All Intelligence Community elements that collect, retain, or disseminate information concerning U.S. persons are required to establish procedures governing these activities.[22] Therefore, as previously discussed, I&A issued its Intelligence Oversight Guidelines in 2017 to address this requirement.[23] These guidelines identify various safeguards to help ensure that I&A personnel protect the privacy, civil rights, and civil liberties of U.S. persons when conducting intelligence activities (see table 2).

[22]Executive Order 12333, as amended, authorizes Intelligence Community elements to collect, retain, or disseminate information concerning U.S. persons. Such actions may be undertaken only in accordance with procedures established by the head of the Intelligence Community element concerned and approved by the Attorney General, after consultation with the Director of National Intelligence. See Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 2.3. I&A is an Intelligence Community element.

[23]DHS Office of Intelligence and Analysis, *Intelligence Oversight Guidelines*.

Table 2: Privacy, Civil Rights, and Civil Liberties Safeguards in the Office of Intelligence and Analysis (I&A) Intelligence Oversight Guidelines

Privacy Safeguards	Civil Rights Safeguards	Civil Liberties Safeguards
When conducting intelligence activities, I&A personnel must • use overt collection methods or collect information from publicly available sources;[a] • use the least intrusive collection techniques feasible and sufficient when collecting U.S. persons information;[b] • collect U.S. persons information only when they have a reasonable belief that doing so would further a national or departmental mission; • access information systems with U.S. persons information only when they have appropriate security clearances and meet other access requirements; • retain U.S. persons information only for as long as is necessary to fulfill the specified purpose; • conduct searches in information systems that minimize the amount of U.S. persons information returned; and • delete U.S. persons information that does not meet certain requirements for permanent retention.	• I&A personnel may not engage in intelligence activities based solely on an individual's or group's race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, or nationality.	• I&A personnel may not engage in intelligence activities for the sole purpose of monitoring activities protected by the First Amendment.[c] • I&A personnel may not engage in intelligence activities for the purpose of affecting the U.S. political process.

Source: Department of Homeland Security Office of Intelligence and Analysis, Intelligence Oversight Guidelines (Washington, D.C.: Jan. 2017) | GAO-23-105475

Note: The Intelligence Oversight Guidelines do not apply to I&A personnel conducting activities for non-intelligence purposes, such as administrative or oversight activities, reporting a crime, or responding to a Freedom of Information Act request.

[a]Overt collection consists of activities that are openly acknowledged by or readily attributable to the U.S. government or that would be acknowledged in response to a direct inquiry. Information is publicly available if it was published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event open to the public.

[b]U.S. persons information is either a single item of information or information that, when combined with other available information, is reasonably likely to identify one or more specific U.S. persons. A U.S. person is: (1) A U.S. citizen, (2) a foreign national known by the intelligence element to be a lawful permanent resident, (3) an unincorporated association substantially composed of U.S. citizens or permanent residents, or (4) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 3.5(k).

[c]The First Amendment to the U.S. Constitution protects the freedoms of speech, press, association, and assembly, among others. U.S. Const. amend. I. The government generally may not prohibit speech because of its message, ideas, subject matter, or content—even speech that may be viewed by some as offensive or disagreeable. The Privacy Act of 1974 also restricts the ability of agencies that maintain a system of records to maintain records describing how any individual exercises First Amendment rights unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity. 5 U.S.C. § 552a(e)(7). The First Amendment does not protect certain categories of activity, such as "advocacy intended, and likely, to incite imminent lawless action," "so-called 'fighting words,'" and "true threats." United States v. Alvarez, 567 U.S. 709, 717 (2012) (citing Brandenburg v. Ohio, 395

U.S. 444, 447 (1969) (per curiam); Chaplinsky v. New Hampshire, 315 U.S. 568, 571-72 (1942); Watts v. United States, 394 U.S. 705, 708 (1969) (per curiam)).

The policy instruction accompanying the Intelligence Oversight Guidelines states that I&A's Intelligence Oversight Officer is to implement the guidelines and ensure that I&A personnel comply with them. To that end, the guidelines and its accompanying policy instruction identify various activities that I&A is to conduct to monitor whether personnel are appropriately implementing the guidelines. These activities include compliance reviews, preliminary inquiries, and specific kinds of audits, which we discuss later in the report.[24] While the Intelligence Oversight Officer is responsible for implementing the guidelines, the Under Secretary for Intelligence and Analysis—either directly or through designated personnel—is to ensure that I&A personnel conduct their activities in a manner that protects privacy, civil rights, and civil liberties.

I&A has issued other policies and procedures regarding how personnel are to protect privacy, civil rights, and civil liberties. We describe these policies and procedures in appendix II.

I&A Used Input from Its Mission Centers and Partners to Prioritize Threats

I&A collected input from its mission centers and partners to prioritize threats and guide the development of its products during fiscal years 2019 to 2022, according to I&A officials. Specifically, I&A officials told us that I&A (1) integrated Intelligence Community priorities into the DHS Information Needs Framework (an unprioritized list of threat topics); (2) coordinated with DHS intelligence components to prioritize the threats identified in that framework through a process called Intelligence Threat Banding; and (3) solicited the input of state, local, tribal, and territorial partners to refine its priorities in a Program of Analysis (a written document that guides I&A's production of intelligence products).

The DHS Information Needs Framework. The DHS Information Needs Framework is a one-page, un-prioritized list of threat topics that I&A and its DHS Intelligence Enterprise partners developed. I&A officials told us they started developing this framework in 2022 to serve as the foundation for I&A's priority-setting process and to replace two past frameworks that

[24]We refer to these activities collectively as monitoring activities because their stated purpose (e.g., to periodically verify compliance with agency policies) aligns with the description of monitoring activities in *Standards for Internal Control in the Federal Government*. See GAO-14-704G.

I&A used to prioritize threat topics.[25] I&A officials explained that the previous frameworks sometimes conflicted with each other and were too complex for the purpose of identifying and prioritizing threat topics. The DHS Information Needs Framework, in contrast, allows I&A to quickly view all identified threats that it should prioritize, according to I&A officials.

To fulfill the requirement that its intelligence collection be guided by presidential priorities, I&A officials stated that they included the President's intelligence priorities—as identified in the National Intelligence Priorities Framework—as threat topics within the DHS Information Needs Framework.[26] In addition, the framework includes the priorities of the Intelligence Community and DHS leadership. Officials said the framework is likely to remain relatively stable over time, with changes made on an as-needed basis, such as when there are changes in presidential administrations.

Intelligence Threat Banding. I&A led the DHS Intelligence Enterprise in conducting a process called Intelligence Threat Banding to prioritize the threat topics in the DHS Information Needs Framework. This process, which I&A initiated in 2019, was to help I&A determine which topics would be the focus of its intelligence activities over the following 12- to 18-month period, according to I&A officials. I&A officials said that while I&A's state, local, tribal, and territorial partners did not directly participate in this process, I&A and other DHS Intelligence Enterprise components incorporated these partners' viewpoints based on their understanding of the partners' interests.

To determine the priority levels of threat topics, I&A solicited subject-matter expertise from DHS Intelligence Enterprise members via multiple rounds of surveys and focus groups, according to I&A officials. According to officials, these methods enabled the experts to reach consensus about (1) the likely impact of the threats to U.S. national or homeland security

[25]I&A officials identified the following previous frameworks: (1) the DHS Standing Information Needs and (2) the Homeland Security Information Priorities Framework.

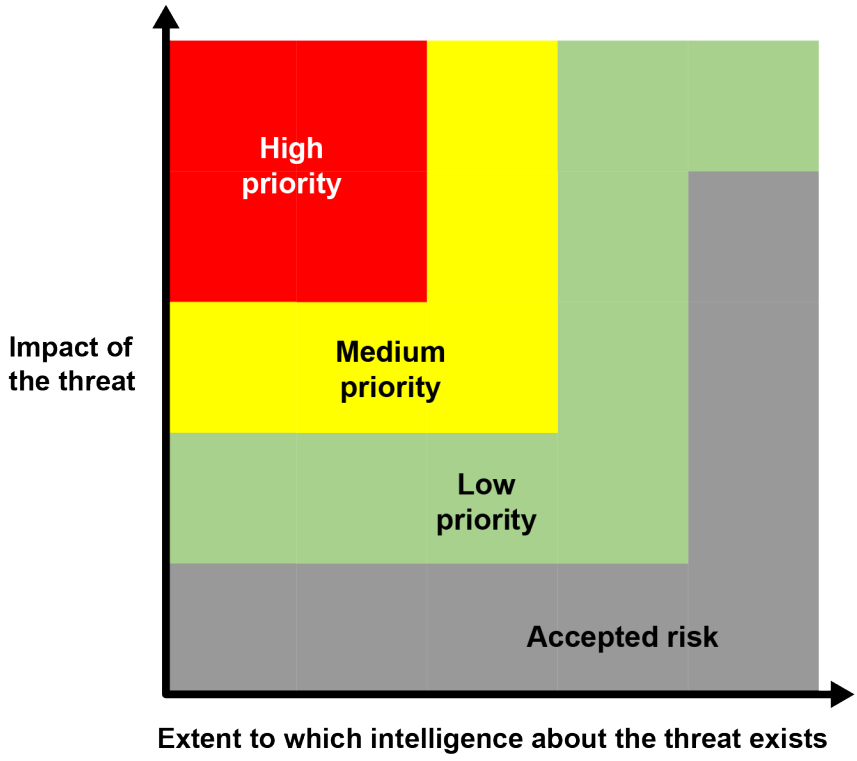
[26]The National Intelligence Priorities Framework is a classified national intelligence document that summarizes the U.S.'s intelligence-gathering priorities. Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 1.1.

over a 12- to 18-month period, and (2) the extent to which intelligence about the threats existed within the DHS Intelligence Enterprise.[27]

In assessing these factors, the DHS Intelligence Enterprise determined whether a threat was a high, medium, or low priority, or an accepted risk. For example, if the subject-matter experts determined that a specific threat, if realized, would have a high impact, and also found that there was a low level of understanding about that specific threat, then they labeled the threat a high priority. This meant that this threat was likely to cause severe damage to national interests or public safety in the upcoming 12- to 18-month period, and the DHS Intelligence Enterprise needed additional information to improve its understanding about the threat (see fig. 3). For example, as a result of the Intelligence Threat Banding process initiated in 2019, the DHS Intelligence Enterprise identified cyber threats to U.S. government networks as a high priority in 2020.

[27]Specifically, I&A officials said that the likely impact of a threat indicates the projected aggregate impact to U.S. national or homeland security over a 12- to 18-month period, as determined and validated by the surveys and focus groups conducted with the subject-matter experts.

Figure 3: The Department of Homeland Security Office of Intelligence and Analysis's Process to Assess Threats and Identify Priorities



High - These threat issues are likely to cause the most severe damage to national interests or public safety in the coming year, and require a surge in additional coverage from the Department of Homeland Security Intelligence Enterprise.

Medium - These threat issues are likely to cause moderate to severe damage to national interests or public safety in the coming year, and require some additional coverage from the Department of Homeland Security Intelligence Enterprise.

Low - These threats are likely to cause limited damage to national interests or public safety in the coming year, and are likely well covered by the Department of Homeland Security Intelligence Enterprise.

Accepted risk - Department of Homeland Security has a relatively complete understanding of the threat issue at the national level and/or is willing to accept the risk posed by this threat issue.

Source: DHS. | GAO-23-105475

I&A officials stated they were performing a new round of Intelligence Threat Banding in 2022. However, as of May 2023, I&A leadership had not finalized these results. In addition, in May 2023, I&A officials told us they were considering alternative methodologies for assessing and prioritizing threats that would align I&A resources with the priorities identified by Intelligence Threat Banding, but that no final decisions had been made.

Key intelligence questions guide product development

I&A's Program of Analysis builds on the most critical (high-level) threats identified through Intelligence Threat Banding by identifying specific key intelligence questions. I&A mission centers and partners are to address these questions in their products. For example:

Intelligence Threat Banding topic: Terrorism and targeted violence

Related key intelligence question: "What are the personal, group, and community factors contributing to targeted violence and mass casualty attacks?"

Source: Department of Homeland Security, Intelligence Enterprise Program of Analysis for Fiscal Year 2022 (no date). | GAO-23-105475

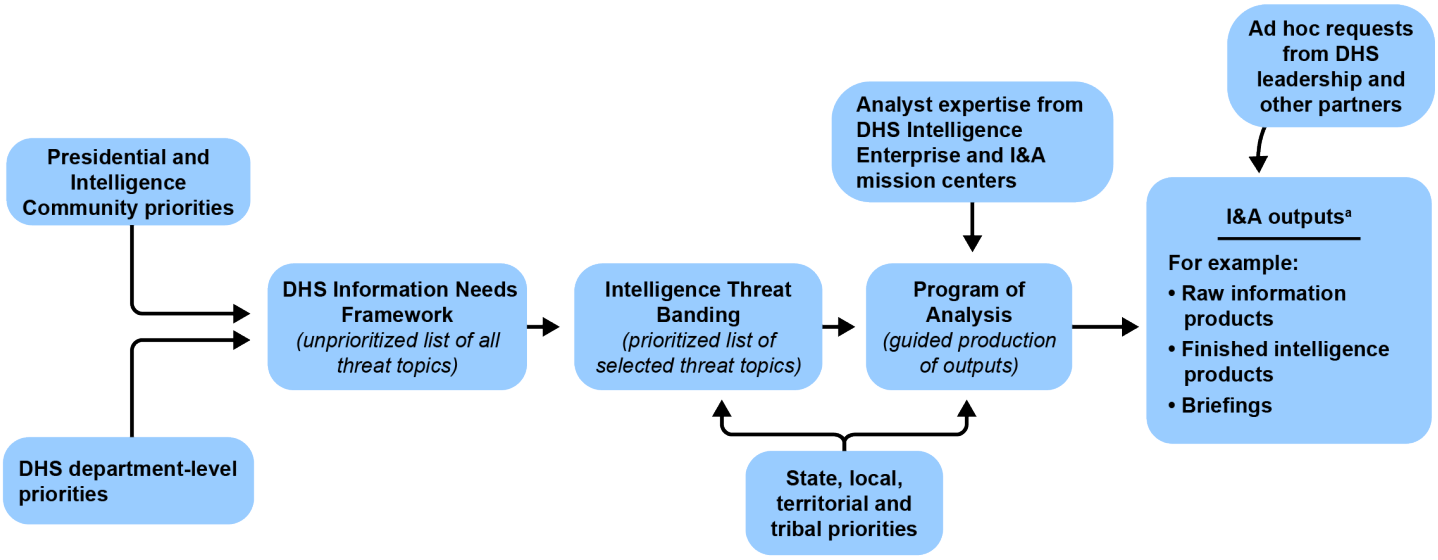
Program of Analysis. Based in part on the results of Intelligence Threat Banding, I&A created a Program of Analysis in fiscal years 2020 and 2022.[28] The Program of Analysis is a written document, generally produced annually, that (1) focuses on the most critical (high-level) threats identified through Intelligence Threat Banding, (2) prioritizes I&A's finished intelligence production to align with these threats, and (3) informs collection of information about these threats, according to I&A officials. The Program of Analysis identifies priorities in the form of key intelligence questions, which generally correspond with a threat topic identified during Intelligence Threat Banding (see sidebar). It also identifies which I&A mission centers and partners are responsible for addressing each key intelligence question through the development of their products.

While the 2020 and 2022 Programs of Analysis drew from Intelligence Threat Banding, I&A officials told us that other factors also influenced their development. For example, I&A's state, local, tribal, territorial, and private sector partners provided input on an annual basis by sharing their intelligence priorities with I&A. In addition, I&A's analysts in its mission centers and regional offices offered their expertise through structured brainstorming sessions and working groups. Lastly, I&A received ad hoc requests from Congress, DHS leadership, or other I&A partners. In general, these ad hoc requests related to threats that emerged after I&A issued the Program of Analysis.

Figure 4 summarizes how the development of the DHS Information Needs Framework, Intelligence Threat Banding, and the Program of Analysis incorporated I&A partners' input to prioritize threats and guide the development of I&A's products from fiscal years 2019 through 2022.

[28]I&A officials told us the Program of Analysis for 2022 was based on Intelligence Threat Banding results for 2020 because Intelligence Threat Banding results for 2022 were not finalized.

Figure 4: The Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Process for Gathering Input to Prioritize Threats and Guide Product Development for Fiscal Years 2019 through 2022



Source: GAO analysis of DHS information. | GAO-23-105475

[a]I&A officials stated that all I&A products, including those that stem from ad hoc requests, must address topics within the DHS Information Needs Framework.

I&A Is Not Fully Monitoring Implementation of Its Intelligence Oversight Guidelines

We were not able to confirm that I&A completed periodic compliance reviews (document reviews and other checks to verify personnel's compliance with the Intelligence Oversight Guidelines) between January 2017 and September 2022 because I&A officials did not document all the reviews they said they completed. To help ensure that it conducts compliance reviews periodically, I&A plans to establish a goal for the number of compliance reviews to be completed in a given period. However, I&A has not determined key details for the goal, such as the number and type of compliance reviews to be completed. In addition, while I&A completed 10 preliminary inquiries (brief investigations of potential violations of federal law or I&A policy) during our review period, none took place when the position of the Intelligence Oversight Officer was vacant from September 2018 through November 2019. Finally, I&A did not conduct the two other monitoring activities called for by the Intelligence Oversight Guidelines: (1) audits of information systems and (2) audits of bulk data.

I&A Did Not Document All Compliance Reviews and Has Not Established a Goal for These Reviews

Documenting Compliance Reviews

I&A did not document all compliance reviews to show these reviews were taking place periodically, in accordance with the Intelligence Oversight Guidelines. The guidelines require the Intelligence Oversight Officer, who leads I&A's intelligence oversight branch, to conduct periodic reviews to verify personnel's compliance with the Intelligence Oversight Guidelines.[29] These compliance reviews may involve employee or contractor interviews, reviews of audit logs, unannounced reviews (spot checks), or records reviews. I&A completed one compliance review involving record reviews between January 2017 and September 2022. The report for this review found staff were disseminating intelligence products in accordance with the Intelligence Oversight Guidelines.[30]

The Intelligence Oversight Officer said that the intelligence oversight branch conducted additional compliance reviews during the period, but did not document them. Specifically, the Intelligence Oversight Officer said the office initiated but did not complete three reviews, and it also completed several spot checks.[31] Regarding the completed spot checks, the officer said they did not document these compliance reviews because

[29]IA-1000—I&A's policy instruction accompanying the Intelligence Oversight Guidelines—provides the direction that compliance reviews should be conducted periodically.

[30]The intelligence oversight branch conducted this compliance review because two preliminary inquiries that were conducted a month before the review found that I&A personnel had not complied with the Intelligence Oversight Guidelines by disseminating intelligence products to entities that did not have a lawful mission relating to the products' subject matter. The compliance review allowed I&A to more broadly examine the issues discovered during these inquiries.

[31]The Intelligence Oversight Officer said that I&A's intelligence oversight branch did not complete two of these compliance reviews due to staffing shortages and the COVID-19 pandemic, among other factors. It did not complete the third compliance review—which included examining I&A's reporting about the civil unrest in Portland, Oregon, in 2020—due to differing viewpoints on the scope and presentation of this review, according to the Intelligence Oversight Officer. DHS's Office of the General Counsel later issued a report about I&A's activities relating to the civil unrest in Portland; see Department of Homeland Security, Office of the General Counsel, *Report on DHS Administrative Review into I&A Open Source Collection and Dissemination Activities During Civil Unrest: Portland, Oregon, June through July 2020* (Washington D.C.: Jan. 6, 2021).

they were informal, and as such, did not warrant a written report.[32] Nevertheless, documentation of reviews, including more informal spot checks, need not result in formal reports, but could consist of key facts about the review, such as the date conducted and method used.

Standards for Internal Control in the Federal Government states that management should design control activities to achieve objectives by requiring clear documentation of significant events so that this documentation is readily available for examination.[33] For I&A's intelligence oversight branch, such significant events would include the compliance reviews called for by I&A's Intelligence Oversight Guidelines. Documenting all compliance reviews will better position I&A to ensure its intelligence oversight branch is meeting the requirement to periodically assess personnel's compliance with the Intelligence Oversight Guidelines.

Establishing a Goal for Compliance Reviews

I&A has efforts underway to help ensure that it conducts compliance reviews periodically, including hiring more staff and working to establish a goal for annual compliance reviews. With respect to staff, I&A has hired more personnel to work in the intelligence oversight branch, according to the Intelligence Oversight Officer. This officer told us that staff shortages within this branch were the primary reason that it was unable to complete more compliance reviews from January 2017 to February 2021. As of February 2021, this branch has had sufficient staff to carry out its primary duties, such as conducting compliance reviews, according to the Intelligence Oversight Officer.

In addition, the intelligence oversight branch has taken steps to establish a goal for the number of compliance reviews to complete annually, but this effort is not complete.[34] Officials said in early 2022 that they documented a goal within a standard operating procedure to complete four compliance reviews annually. This procedure remained in draft form

[32]In May 2023, I&A officials provided us a memo that they said indicates that this branch completed a second compliance review in April 2022. Although this memo states that I&A personnel may have mishandled information about U.S. persons, which could be a violation of the Intelligence Oversight Guidelines, the memo does not include an assessment of whether I&A personnel actually did mishandle this information or failed to comply with any other aspects of the guidelines. Therefore, we did not consider this memo to be evidence of a second compliance review.

[33]GAO-14-704G.

[34]The Intelligence Oversight Officer told us this goal is based on the intelligence oversight branch's staffing capacity as of March 2023.

as of April 2023. I&A officials said that the approval process for this procedure has been lengthy because the procedure includes instructions for handling U.S. persons information and therefore must be reviewed by several entities throughout DHS.

Given these delays, the Intelligence Oversight Officer told us that the branch is considering establishing a goal for compliance reviews outside of the draft standard operating procedure, and there are no impediments to doing so. Further, the officer said I&A is considering a different goal than the one included in the draft standard operating procedure, and the branch has yet to determine key details for the goal, including the number and type of compliance review activities (records reviews, spot checks, etc.) that will be required or time frames for its establishment.

In September 2005, we identified practices to enhance the use of performance information in federal decision-making. For example, we found that when program offices establish their own program goals—as officials from the intelligence oversight branch said they plan to do—this increases the usefulness and relevance of performance information to the program's day-to-day activities.[35] Once program goals have been established, our work indicates that agency managers should assess a program's performance against its goals, and should use the resulting information to detect problems, identify the causes of those problems, and implement corrective actions.

Establishing a goal for the number of compliance reviews to complete in a given period—either in its standard operating procedure for compliance reviews or elsewhere—would help ensure I&A conducts the periodic compliance reviews called for by the Intelligence Oversight Guidelines. Further, once the goal is established, assessing the intelligence oversight branch's performance against this goal would allow I&A to use the resulting performance information to identify and address any factors preventing it from completing the reviews periodically.

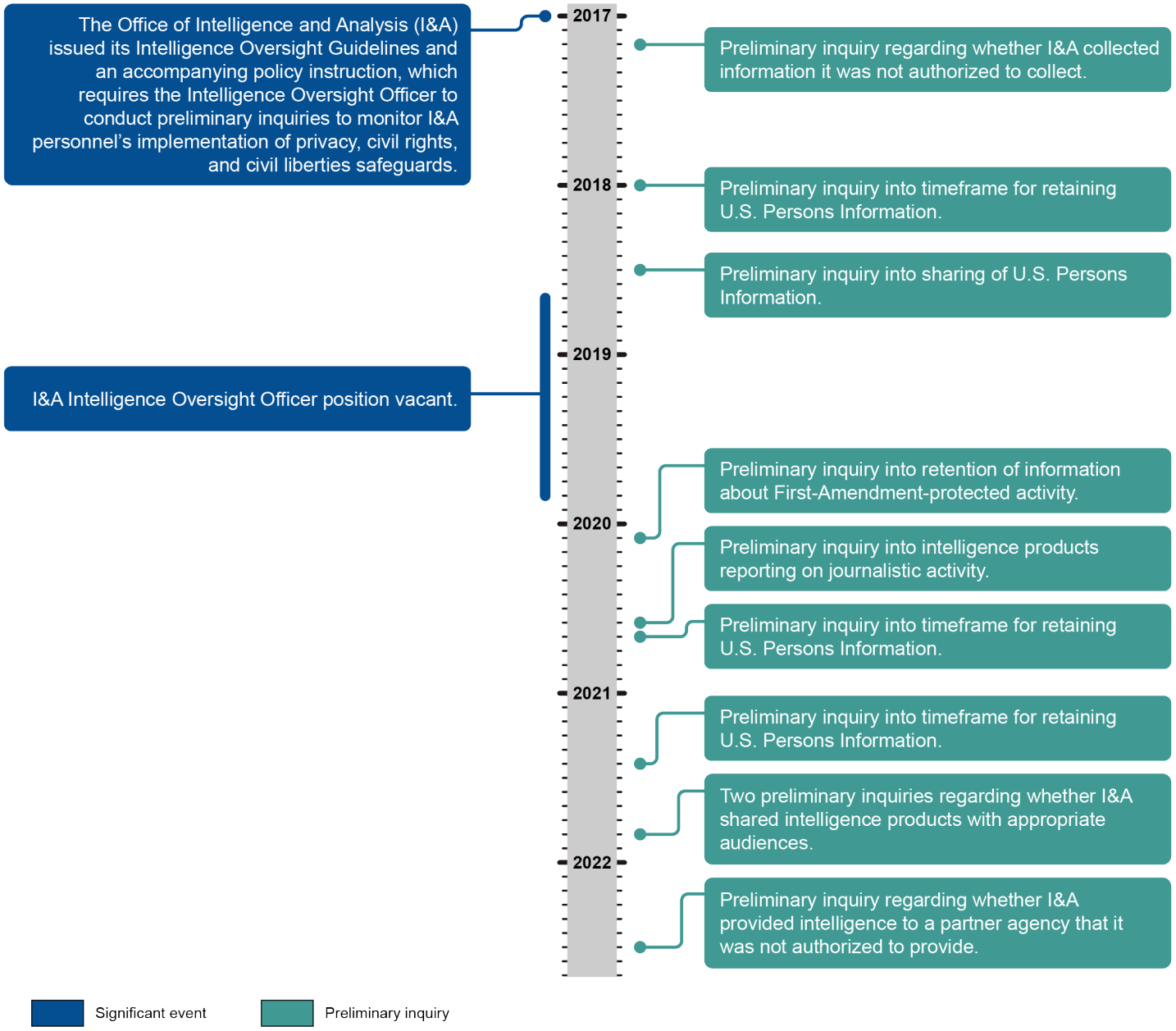
[35]GAO-05-927.

I&A Did Not Conduct Preliminary Inquiries during a 14-Month Period When the Intelligence Oversight Officer Position was Vacant

In addition to conducting compliance reviews, the Intelligence Oversight Officer is to conduct a preliminary inquiry when informed of a potential violation of federal criminal law, I&A's Intelligence Oversight Guidelines, or certain other policies.[36] According to I&A officials, these are to be quick, informal reviews. I&A conducted 10 preliminary inquiries from January 2017 through September 2022. Generally, it conducted more than one preliminary inquiry annually during this period, but it did not conduct any inquiries for 14 months when the Intelligence Oversight Officer position was vacant (see fig. 5).

[36]Specifically, I&A's policy instruction accompanying the Intelligence Oversight Guidelines states that the Intelligence Oversight Officer, in consultation with the Associate General Counsel for Intelligence, is to commence a preliminary inquiry upon notification of any potential violation of federal criminal law or questionable activity. A questionable activity is any conduct related to an intelligence activity that is reasonably believed to constitute a violation of any applicable law, executive order, presidential or other directive, regulation, international or domestic agreement or arrangement, or applicable national or departmental policy, including, but not limited to, the requirements of I&A's Intelligence Oversight Guidelines, with respect to I&A personnel.

Figure 5: Preliminary Inquiries Completed by the Department of Homeland Security Office of Intelligence and Analysis from January 2017 through September 2022



Source: GAO analysis of DHS information. | GAO-23-105475

Note: The dates in this graphic indicate the month and year that I&A issued a report with the results of the inquiry. We reviewed reports for five of these inquiries. For the remaining five inquiries, we reviewed I&A's summaries of the inquiries' findings.

We found that I&A addressed the issues identified by the preliminary inquiries it completed from January 2017 through September 2022. Specifically, in eight of the 10 inquiries, the Intelligence Oversight Officer found that I&A personnel did not appropriately implement some aspects of the guidelines. For example, three inquiries found that I&A personnel retained information about U.S. persons for longer than the permitted temporary retention period.[37] Two other inquiries found that I&A personnel erroneously labeled certain intelligence products as being about domestic terrorism and distributed them to I&A partners who did not have a lawful mission related to the products' subject matter.[38] In all eight of these cases, I&A took steps to address the issues identified by these inquiries. For example, in some cases, I&A provided written guidance and individual counseling to personnel regarding the nature of the guideline violations.[39] In other cases, I&A expunged or recalled documents and products that personnel distributed in violation of the guidelines. Finally, for two of the ten preliminary inquiries, the Intelligence Oversight Officer found that no violations of the Intelligence Oversight Guidelines had taken place and therefore no corrective actions were needed.

An I&A official said it is not possible to confirm whether any preliminary inquiries should have taken place while the position of the Intelligence Oversight Officer was vacant in 2018 and 2019, but it is likely that this vacancy inhibited preliminary inquiries from being completed. According to this official, personnel within I&A's intelligence oversight branch were not clear who should be performing the duties of the Intelligence Oversight Officer while the position was vacant.

In February 2021, I&A began drafting a standard operating procedure that identifies roles and responsibilities for performing preliminary inquiries. As of April 2023, I&A had not finalized this procedure, and I&A officials said they have not documented time frames for finalizing it. I&A officials said the review process to finalize this procedure has been lengthy because

[37]I&A personnel may temporarily retain U.S. persons information for the purpose of evaluating whether the U.S. persons information qualifies for permanent retention. The evaluation period generally cannot exceed 180 days from the date on which the U.S. persons information was collected.

[38]This information is based on report summaries that I&A provided to us.

[39]This information is based on one preliminary inquiry report that we viewed and a summary of another report that I&A provided to us.

the procedure relates to I&A personnel's use of U.S. persons information and, therefore, several entities within and outside of I&A must review it.

Standards for Internal Control in the Federal Government states that management should develop and maintain documentation of its internal control system.[40] Preliminary inquiries are a part of I&A's internal control system. Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having knowledge limited to a few personnel. Additionally, *The Standard for Program Management* states that programs should include the concept of time and incorporate schedules through which specific milestone achievements are measured.[41] By establishing time frames for finalizing its standard operating procedure for conducting preliminary inquiries, and by finalizing this procedure according to those time frames, I&A could better ensure that preliminary inquiries continue as needed throughout any future vacancies in the Intelligence Oversight Officer position.

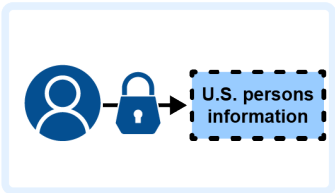
I&A Has Not Conducted Required Audits

I&A has not conducted two of the four monitoring activities called for in its Intelligence Oversight Guidelines—audits of information systems and audits of bulk data (see fig. 6). Neither the I&A Intelligence Oversight Guidelines nor the accompanying policy instruction identifies who is to conduct these audits.

[40]GAO-14-704G.

[41]The Project Management Institute, Inc. *The Standard for Program Management,* 4th ed.

Figure 6: Audits of Information Systems and Audits of Bulk Data Required by the Office of Intelligence and Analysis (I&A) Intelligence Oversight Guidelines



Audits of information systems

I&A is to audit information systems containing U.S. persons information to assess 1) whether I&A personnel had appropriate security clearances, a mission requirement, and met other requirements to access these systems; and 2) whether I&A personnel tailored their searches in these systems to minimize the amount of irrelevant U.S. persons information returned.[a]

Audits of bulk data

I&A is to audit bulk data that were transferred to or from I&A and that contain U.S. persons information.[b] These audits are to assess whether access to such data, and searches conducted in the data, were appropriately limited to protect individuals' privacy, civil rights, and civil liberties.

Source: Department of Homeland Security, Office of Intelligence and Analysis, *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines*, Instruction IA-1000 (Jan. 19, 2017), GAO (icons). | GAO-23-105475

[a]U.S. persons information is either a single item of information or information that, when combined with other available information, is reasonably likely to identify one or more specific U.S. persons. A U.S. person is: (1) A U.S. citizen, (2) a foreign national known by the intelligence element to be a lawful permanent resident, (3) an unincorporated association substantially composed of U.S. citizens or permanent residents, or (4) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 3.5(k).

[b]Bulk data are large quantities of data acquired without the use of discriminants (e.g., specific identifiers or selection terms), a significant portion of which are not reasonably likely to have intelligence or operational value. Any bulk data containing U.S. persons information that are transferred into or out of I&A are subject to terms and conditions that the Under Secretary for Intelligence and Analysis establishes for each transfer. I&A is required to audit access to or searches conducted in the bulk data collection only if the terms and conditions governing that collection require such audits.

The Intelligence Oversight Officer did not know who is responsible for conducting these audits, but identified various entities that might be responsible for conducting them. For example:

Audits of information systems. The Intelligence Oversight Officer directed us to I&A's Office of Technology and Data Services for information about the audits of information systems required by the Intelligence Oversight Guidelines. Officials from this office said they do not conduct these audits, and they are not responsible for conducting them. However, these officials described some practices that I&A implements to protect U.S.

persons information in its information systems.[42] For example, I&A is to conduct privacy threshold analyses and privacy impact assessments to determine how U.S. persons information is collected, stored, shared, and managed in information systems.[43] A privacy impact assessment for one of I&A's information systems describes how the system will automatically block a user's access to an intelligence product containing U.S. persons information unless the system authenticates certain information about the user, such as their clearance level. Officials said these are standard privacy practices that I&A conducts in general, not specifically for complying with the Intelligence Oversight Guidelines.

Audits of bulk data. The Intelligence Oversight Officer directed us to DHS's Data Access Review Council to discuss the audits of bulk data required by the Intelligence Oversight Guidelines.[44] Officials representing the Data Access Review Council said they do not conduct these audits because they are not responsible for doing so.

The Intelligence Oversight Officer said I&A may not have identified who is responsible for conducting and reporting on these audit activities when it issued the guidelines in 2017 because I&A is a relatively young agency

[42]We did not assess the extent to which I&A is implementing these practices because they are not required by the Intelligence Oversight Guidelines.

[43]Privacy threshold analyses identify whether an information system involves personal identifying information, describe the nature of that information, detail how the information will be used, and determine whether a privacy impact assessment is needed. Privacy impact assessments identify privacy risks and methods to mitigate those risks. DHS policy calls for all DHS entities to complete these analyses and assessments; see Department of Homeland Security, *Privacy Policy and Compliance,* Instruction 047-01-001 (Washington, D.C.; July 25, 2011).

[44]Bulk data are large quantities of data acquired without the use of discriminants (e.g., specific identifiers or selection terms), a significant portion of which are not reasonably likely to have intelligence or operational value. Any bulk data containing U.S. persons information that are transferred into or out of I&A are subject to terms and conditions that the Under Secretary for Intelligence and Analysis issues. I&A is to audit access to or searches conducted in the bulk data collection only if the terms and conditions governing that collection require such audits. According its charter, the Data Access Review Council is the coordinated oversight and compliance mechanism for the review of departmental initiatives and activities involving the internal or external transfer of personally identifiable information through bulk data.

and needs flexibility to reassign responsibilities as it matures.[45] However, although the guidelines do not specify who is to perform these audits, an official from a DHS office that helped draft the guidelines stated that they intentionally included the requirement for these audits due to I&A's mission.[46] In addition, I&A's Intelligence Oversight Guidelines state that I&A should take reasonable steps when developing and deploying information technology systems containing U.S. persons information to ensure effective auditing and reporting as required by the guidelines. Finally, I&A officials told us that the Under Secretary for Intelligence and Analysis's responsibilities include identifying who is to conduct the monitoring activities described in the Intelligence Oversight Guidelines.

Standards for Internal Control in the Federal Government states that management should assign responsibilities for reporting quality information that supports the internal control system and should establish reporting lines within the organization so units can communicate quality information about internal control activities.[47] In this case, quality information would include the results of the audits of information systems and bulk data required by the Intelligence Oversight Guidelines. Without identifying who is responsible for conducting these audits and to whom the results should be reported, and then ensuring they are conducted, I&A risks being unaware of potential failures of staff to appropriately protect privacy, civil rights, and civil liberties.

I&A Lacks Information to Fully Assess Its Effectiveness

I&A's performance measures generally do not align with its strategic goals. As a result, I&A cannot assess its effectiveness in meeting those goals. In addition, to fulfill a statutory requirement, I&A collects feedback from state, local, tribal, territorial, and private sector partners on its intelligence products; however, it has not produced required annual reports on these data for congressional committees since 2017. Further, the customer feedback that I&A collects may not fulfill its need to better understand the interests of its customers.

[45]This official did not work for I&A when the guidelines were being drafted and issued. Further, according to the Intelligence Oversight Officer, after the Attorney General approved I&A's guidelines in January 2017, I&A did not develop any additional implementation guidance that might have identified the responsible individuals.

[46]This official was from the DHS Office for Civil Rights and Civil Liberties, which participated in drafting the Intelligence Oversight Guidelines.

[47]GAO-14-704G.

I&A Does Not Assess Progress toward Strategic Goals

I&A's performance measures generally do not align with its strategic goals; therefore, I&A is unable to assess progress toward its strategic goals. I&A guidance states that performance measures should be developed as part of its strategic planning process.[48] Additionally, leading practices state that performance measures should align with an agency's strategic goals.[49] This alignment increases the usefulness of the performance information to decision makers at each level and reinforces the connection between strategic goals and the day-to-day activities of managers and staff (see fig. 7).

Figure 7: Leading Practices for Aligning Strategic Goals and Performance Measures

Strategic goals

Leading organizations we have studied set long-term strategic goals that were an outgrowth of a clearly stated mission. Setting long-term strategic goals is essential for results-oriented management because such goals explain in greater specificity the results that organizations are intending to achieve.

Performance measures

Performance measures allow an agency to track the progress it is making toward its mission and goals, provide managers information on which to base their organizational and management decisions, and create powerful incentives to influence organizational and individual behavior.

Source: GAO, Managing for Results: Critical Issues for Improving Federal Agencies' Strategic Plans, GAO/GGD-97-180 (Washington, D.C.: Sept. 16, 1997) and Executive Guide: Effectively Implementing the Government Performance Results Act, GAO/GGD-96-118 (Washington, D.C.: June 1996). | GAO-23-105475

I&A has identified 16 strategic goals to guide its performance, and I&A tracks its performance using 13 performance measures.[50] However, we found—and I&A officials confirmed—that these goals and measures generally do not align. This prevents I&A from assessing its effectiveness in meeting its strategic goals. Specifically we found:

- I&A's performance measures do not align with 11 of I&A's strategic goals. For example, I&A has a strategic goal relating to privacy, civil

[48]DHS Office of Intelligence and Analysis, *DHS Intelligence & Analysis Planning, Programming, Budgeting, and Evaluation*, Policy Instruction IA-301 (Nov. 20, 2013).

[49]GAO-05-927.

[50]I&A presented its strategic goals in its strategic plan that covers fiscal years 2020 to 2024. See DHS Office of Intelligence and Analysis, *Strategic Plan Fiscal Year (FY) 2020–2024* (Washington, D.C.: Feb. 6, 2020).

liberties, and transparency, but it does not have any performance measures relating to this topic.

- I&A's performance measures partially align with two strategic goals. For example, I&A's performance measure "percent of finished intelligence products shared with state, local, tribal, territorial, and private sector partners" is partially aligned with its strategic goal related to partnerships because the measure relates to sharing intelligence with partners. However, neither this measure nor any of the other measures address the extent to which I&A has expanded or strengthened those partnerships, as described by the goal.[51] Therefore, it does not fully assess progress toward the goal.
- I&A's performance measures clearly align with three strategic goals. For example, the four performance measures related to cyber threats align with I&A's strategic goal to detect and understand cyber threats. See appendix III for more information on I&A's performance measures and their alignment with I&A's strategic goals.

I&A officials told us that I&A's performance measures do not fully align with its strategic goals because I&A developed its performance measures to focus on finished intelligence production. I&A officials said that they plan to develop performance measures that align with strategic goals in the next strategic plan, which will cover fiscal years 2025 to 2029 and was under development as of March 2023. By aligning its performance measures with and assessing progress toward strategic goals, I&A leadership would know the extent to which I&A is making progress toward its goals and I&A's overall effectiveness. See appendix IV for a summary of leading practices that we have previously identified for aligning performance measures and strategic goals.

I&A Has Not Submitted Required Reports on Customer Feedback to Congress since 2017

Since 2017, I&A has not produced and submitted to Congress required reports on the feedback it collects from customers. Specifically, the Homeland Security Act of 2002, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, requires the Secretary of Homeland Security to create a mechanism for state, local, and tribal customers of DHS intelligence products to submit feedback on

[51]I&A's strategic goal for partnerships is to expand and strengthen partnerships to enrich intelligence, inform decisions, and enable actions throughout the Homeland Security Enterprise. See appendix III for more information on I&A's strategic goals and performance measures.

these products.[52] It also requires the Secretary to report annually to two congressional committees on the feedback received and any related adjustments made to intelligence production. In 2012, the Secretary delegated responsibility for these reports to the Under Secretary for Intelligence and Analysis.

To fulfill the first part of this statutory requirement, I&A attaches a voluntary questionnaire to the end of its finished intelligence products allowing customers to rate the product on its usefulness, timeliness, and other factors on five-point scales.[53] To fulfill the second part of this statutory requirement—that is, the congressional reporting requirement—I&A officials said that they produced and submitted these reports to the two congressional committees annually from 2010 to 2017.[54]

However, I&A has not produced these reports since 2017. Officials from I&A's Program and Performance Evaluation Division told us that they did not complete the reports for fiscal years 2017 through 2021 because they were not tasked to do so.[55] Furthermore, I&A officials we spoke with did not identify a process to ensure that I&A completes the report and submits it to Congress on an annual basis. Developing and implementing a process to ensure that I&A submits the annual report on customer feedback to relevant congressional committees, as required by statute,

[52]The Implementing Recommendations of the 9/11 Commission Act of 2007 amended the Homeland Security Act of 2002 by adding section 210A, which requires that the Secretary of Homeland Security create a voluntary mechanism for any state, local, or tribal law enforcement officer or other emergency response provider who is a consumer of DHS intelligence products to provide feedback to the DHS on the quality and utility of such intelligence products. The Secretary is also to submit a report annually describing such consumer feedback and, if applicable, how DHS has adjusted its production of intelligence products in response to the consumer feedback. Pub. L. No. 107-296, title II, subtitle A, § 210A, 116 Stat. 2135, as amended by Pub. L. No. 110-53, title V, subtitle B, § 511(a), 121 Stat. 266, 321 (classified, as amended, at 6 U.S.C. § 124h(g)). I&A partners and customers are the same entities. I&A uses the term "customers" for the purposes of soliciting feedback and assessing customer satisfaction.

[53]I&A also attaches questionnaires to its Open Source Intelligence Reports and Field Intelligence Reports. These questionnaires generally ask the same questions as the questionnaire appended to finished intelligence products.

[54]The report that I&A submitted in 2017 covers feedback it received in fiscal year 2016, according to I&A officials.

[55]In February 2023, after we asked I&A officials about this reporting requirement, officials stated that they started preparing the annual report that will cover feedback it received during fiscal year 2022.

would ensure that Congress has information needed to help evaluate the effectiveness of I&A's information-sharing mission.

I&A Has Not Assessed Whether Customer Feedback Data Meet Its Needs

I&A may be missing opportunities to collect different or additional data that could better meet its internal need to better understand its customers' interests. As discussed, I&A attaches questionnaires to its intelligence products to fulfill the statutory requirement to create a customer feedback mechanism.[56] I&A officials told us that I&A intends for the customer feedback data it collects to improve I&A's understanding of its customers' interests. To that end, I&A distributes feedback data from these questionnaires to its components (i.e., mission centers and other units that produce intelligence products). However, I&A officials said they have not assessed whether these data are improving these components' understanding of their customers' interests. Officials from I&A's unit that is responsible for the customer feedback questionnaire said they are not responsible for assessing whether the data collected are appropriate to address I&A's need to better understand its customers.

We found that the data I&A receives from its questionnaires may not fully reflect I&A's customers' interests and concerns and therefore may not be meeting I&A's needs. Specifically, 89 percent of questionnaire respondents in fiscal year 2022 said that they were "very satisfied" or "somewhat satisfied" with the usefulness of the finished intelligence product on which they provided feedback.[57] However, this high rate of satisfaction contrasts with some of the comments and concerns we heard in our interviews with I&A customers. For example, although I&A intends to provide its partners with actionable products, three of the eight DHS components and none of the seven state or local customers we interviewed indicated that the finished intelligence products they received were actionable. This may be because I&A did not write the products expressly for law enforcement and other front-line personnel, according to one law enforcement customer, or because I&A's products were not specific to the geographic area served, according to another law enforcement customer. In addition, private-sector officials we interviewed articulated ways in which I&A products and briefings did not meet their needs. For example, officials from one sector told us that I&A information

[56]I&A officials told us that they also collect feedback during meetings with customers and from personnel who brief senior DHS leaders using a less structured approach.

[57]These data come from an I&A performance measure that is based on questionnaire responses. This performance measure is defined as the percent of finished intelligence products rated satisfactory and useful by customers. Appendix III lists I&A's performance measures, targets, and results for fiscal years 2020 through 2022.

is sometimes redundant with information they receive from other intelligence entities. Officials from another sector told us that information from I&A is not tailored to their particular needs, and officials from a third sector told us the classification of products hinders their ability to share the information.

Further, we found that I&A's questionnaires are not designed to gather information related to customer interests. For example, the questionnaire for finished intelligence products contains questions solely about the product to which the questionnaire is attached. It prompts customers to rate the usefulness, relevance, timeliness, and responsiveness of the product on a five-point scale; to select options for how the product may be used; and to identify additional information in free-text fields. Although officials from two of I&A's five mission centers told us that they receive useful feedback on customers' interests in the free-text fields, the two free-text questions do not ask about customer interests and are focused on the product to which they are attached.[58]

In September 2005, we identified practices to help enhance the use of performance information—such as customer feedback data—in federal decision-making.[59] For example, we found that agencies should consider users' information needs to ensure that performance information is both useful and used in decision-making. We reported that one agency implemented this practice by assessing whether its performance information was appropriate for meeting the agency's intended uses of this information. We found that this practice helped ensure that the agency's performance information met management's needs. Without assessing the extent to which the customer feedback data it currently collects meets its needs and taking steps to address the results of this assessment, I&A may be missing opportunities to collect more useful information on customer interests. These opportunities could involve amending its questionnaire to ask more broadly about customer interests or using another mechanism to solicit this information.[60] Further, I&A

[58]The first free-text question asks for specific details about situations in which the customer might use the intelligence product. The second free-text question asks what the product did not address that the customer anticipated it would address.

[59]GAO-05-927.

[60]For example, I&A officials told us in August 2023 that I&A has used an annual survey of state, local, tribal, and territorial customers to gather feedback on its communications and services.

would be better positioned to produce intelligence products that align with the interests and needs of its customers.

Conclusions

I&A has an important role to play in collecting and disseminating threat information to mitigate violence and other threats to homeland security. In conducting these activities, the agency must implement safeguards to protect the privacy, civil rights, and civil liberties of U.S. persons. While I&A has taken some steps to monitor personnel's implementation of these safeguards, we identified some areas for improvement. Specifically, by requiring that compliance reviews be documented and establishing a goal for these reviews; establishing time frames for completing its standard operating procedure for preliminary inquiries; and identifying roles and responsibilities for required audits to ensure that these audits are completed, I&A will be able to more effectively monitor the extent to which its personnel are implementing required safeguards to protect privacy, civil rights, and civil liberties.

I&A could also take additional steps to improve how it assesses its overall effectiveness. Specifically, ensuring full alignment between performance measures and strategic goals will enable I&A's leadership to better understand and assess the agency's progress toward these goals and its effectiveness over time. In addition, by developing and implementing a process to ensure that I&A reports annually on customer feedback to relevant congressional committees and by assessing the extent to which collected feedback data meet I&A's needs for information on customer interests, I&A could better ensure that it is meeting its customers' needs and that Congress has the information needed to evaluate how effectively I&A is carrying out its mission.

Recommendations for Executive Action

The Under Secretary for Intelligence and Analysis should ensure that I&A's intelligence oversight branch documents the reviews it conducts to verify I&A personnel's compliance with I&A's guidelines for protecting privacy, civil rights, and civil liberties. (Recommendation 1)

The Under Secretary for Intelligence and Analysis should establish a goal for the number of compliance reviews that I&A's intelligence oversight branch is to conduct during a given period to verify personnel's compliance with I&A's guidelines for protecting privacy, civil rights, and civil liberties. (Recommendation 2)

The Under Secretary for Intelligence and Analysis should assess the intelligence oversight branch's performance against its goal for compliance reviews, including identifying any factors preventing it from

meeting this goal and any needed corrective actions. (Recommendation 3)

The Under Secretary for Intelligence and Analysis should establish time frames for completing I&A's standard operating procedure for conducting preliminary inquiries and should finalize this procedure according to these time frames. (Recommendation 4)

The Under Secretary for Intelligence and Analysis should identify who is responsible for conducting the audits of information systems and bulk data described in I&A's Intelligence Oversight Guidelines, and to whom the results of these audits should be reported. (Recommendation 5)

The Under Secretary for Intelligence and Analysis should ensure that the responsible entities conduct audits of information systems and bulk data, as described in I&A's Intelligence Oversight Guidelines. (Recommendation 6)

The Under Secretary for Intelligence and Analysis should develop performance measures for I&A that clearly align with and assess progress toward its strategic goals. (Recommendation 7)

The Under Secretary for Intelligence and Analysis should develop and implement a process to submit the statutorily required annual report related to customer feedback on intelligence products to relevant congressional committees. (Recommendation 8)

The Under Secretary for Intelligence and Analysis should assess the extent to which customer feedback data meet its need to understand its customers' interests and, if necessary, take steps to collect more appropriate data. (Recommendation 9)

Agency Comments

We provided a draft of this report to DHS for review and comment. In its comments, reproduced in appendix V, DHS concurred with all of our recommendations. DHS I&A and the DHS Office for Civil Rights and Civil Liberties also provided technical comments, which we incorporated as appropriate.

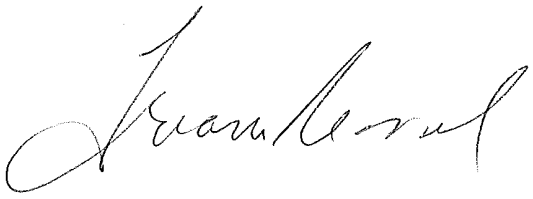
As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 15 days from the report date. At that time, we will send copies to appropriate congressional committees, the Secretary of Homeland Security, and the Under

Secretary for Intelligence and Analysis. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Triana McNeil at (202) 512-8777 or McNeilT@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

Sincerely yours,

Triana McNeil



Director
Homeland Security and Justice

Appendix I: Prior GAO and Office of Inspector General Recommendations to the Office of Intelligence and Analysis

In fiscal years 2022 and 2023, GAO and the Department of Homeland Security (DHS) Office of Inspector General (OIG) issued reports with recommendations to the DHS Office of Intelligence and Analysis (I&A). These recommendations—and the extent to which I&A has implemented them as of March 2023—are summarized in tables 3 and 4.

Table 3: GAO Recommendations to the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A), Fiscal Year 2023

Report	Key Findings	Recommendations	Recommendation status
Domestic Terrorism: Further Actions Needed to Strengthen FBI and DHS Collaboration to Counter Threats February 22, 2023 GAO-23-104720	The National Defense Authorization Act for Fiscal Year 2020 required the Federal Bureau of Investigation (FBI) and I&A, in consultation with the Office of the Director of National Intelligence, to submit several reports on domestic terrorism to specified congressional committees. FBI and I&A did not report comprehensive domestic terrorism incident data in their 2021 and 2022 strategic intelligence reports.	The Under Secretary for Intelligence and Analysis should, in coordination with the Director of the FBI, report domestic terrorism incident data from both agencies in response to the annual update requirement in the National Defense Authorization Act for Fiscal Year 2020.	**I&A has not yet fully implemented this recommendation as of April 2023**. DHS reported that I&A and FBI are working collaboratively to develop the 2023 Strategic Intelligence Assessment report, which, according to DHS, will reflect both organizations' input regarding significant domestic terrorism incidents during fiscal year 2022.
	FBI and I&A collaborate via headquarters staff, fusion centers, and through serving on task forces to identify and counter domestic terrorism threats but they have not consistently evaluated the effectiveness of their collaborative efforts.	The Under Secretary for Intelligence and Analysis should, in collaboration with the Director of the FBI, implement a process to periodically evaluate the effectiveness of collaborative practices to identify and counter domestic terrorism threats.	**I&A has not yet fully implemented this recommendation as of April 2023**. DHS noted that DHS and FBI domestic terrorism issue managers and counterterrorism senior leaders have regular meetings, in which ongoing collaboration practices are evaluated, and adjustments to processes are subsequently made, as appropriate.

Report	Key Findings	Recommendations	Recommendation status
	While FBI and DHS have agreements in place, they have not assessed the extent to which these agreements fully reflect FBI's and I&A's charge to jointly prevent domestic terrorism attacks respective to their role.	The Under Secretary for Intelligence and Analysis should, in collaboration with the Director of the FBI, assess existing formal agreements to determine if they fully articulate a joint process for working together to counter domestic terrorism threats and sharing relevant domestic-terrorism-related information and update and revise accordingly.	**I&A has not yet fully implemented this recommendation. As of April 2023**, DHS stated that it has reviewed its formal agreements with FBI and is taking steps to strengthen collaboration and coordination on domestic terrorism threats. For example, DHS is establishing a Deputy Under Secretary for Intelligence Partnerships to elevate partner engagement efforts with federal and other partners. Also, according to DHS, FBI is working to identify an FBI Counterterrorism Division employee to be co-located within I&A's Counterterrorism Mission Center to provide on-site access and support. Additionally, DHS stated that it continues to work with FBI on certain DHS employees obtaining direct access to FBI investigative data.
Capitol Attack: Federal Agencies Identified Some Threats, but Did Not Fully Process and Share Information Prior to January 6, 2021 February 28, 2023 GAO-23-106625	I&A internal controls did not ensure that personnel followed its policies for processing open-source threat information from manual searches or from other agencies related to the attack on the Capitol on January 6, resulting in threat products not being developed and shared.	The Under Secretary for Intelligence and Analysis should assess the extent to which its internal controls ensure personnel follow existing and updated policies for processing open-source threat information.	**I&A has not yet taken actions to implement this recommendation as of February 2023**. DHS stated that it recognizes the need for a robust internal controls program and noted that it is gathering data to establish processes for assessing internal controls. DHS agreed with these recommendations and described steps it plans to take and time frames for completion of these various steps. Once this process is established, DHS expects to complete the recommended assessments by September 29, 2023.

Report	Key Findings	Recommendations	Recommendation status
	While I&A is implementing internal control changes, I&A has not yet determined whether these changes are effective measures to address internal control deficiencies. As I&A continues with these efforts, it can benefit from assessing the extent to which internal controls are in place to ensure personnel follow existing and updated policies for processing open-source threat information.	The Under Secretary for Intelligence and Analysis should, following its assessment, implement a plan to address any internal control deficiencies identified to ensure personnel consistently follow the policies for processing open-source threat information.	**I&A has not yet taken actions to implement this recommendation as of February 2023**. DHS stated that it will work with stakeholders to develop corrective action plans for all identified deficiencies. Specifically, DHS noted that the corrective action plans will include root cause analysis, remediation milestones with due dates, and follow-up actions to be reported to DHS senior leadership on a quarterly basis. DHS expects to complete the corrective action plans by December 29, 2023.
	While I&A developed reports regarding domestic violent extremist activity and potential violence at January 6 events, it did not share all of these reports with Capitol Police.	The Under Secretary for Intelligence and Analysis should assess the extent to which its internal controls ensure personnel consistently follow the policies for sharing threat-related information with relevant agencies such as Capitol Police.	**I&A has not yet taken actions to implement this recommendation as of February 2023**. DHS stated that it recognizes the need for a robust internal controls program and noted that it is gathering data to establish processes for assessing internal controls. DHS agreed with the recommendation and described steps it plans to take and time frames for completion of these various steps. Once this process is established, DHS expects to complete the recommended assessments by September 29, 2023.
	I&A internal controls did not provide for timely sharing of critical information with the Capitol Police. I&A can benefit from assessing its internal controls related to information sharing to ensure that they allow for effective sharing of threat information.	The Under Secretary for Intelligence and Analysis should, following its assessment, implement a plan to address any internal control deficiencies identified to ensure personnel consistently follow the policies for sharing threat-related information with relevant agencies such as Capitol Police.	**I&A has not yet taken actions to implement this recommendation as of February 2023**. DHS stated that it will work with stakeholders to develop corrective action plans for all identified deficiencies. Specifically, DHS noted that the corrective action plans will include root cause analysis, remediation milestones with due dates, and follow-up actions to be reported to DHS senior leadership on a quarterly basis. DHS expects to complete the corrective action plans by December 29, 2023.

Source: GAO. | GAO-23-105475

Table 4: Department of Homeland Security (DHS) Office of Inspector General (OIG) Recommendations to the DHS Office of Intelligence and Analysis (I&A), Fiscal Year 2022

Report	Summary of Findings	Recommendation	Status (as of March 2023)
I&A Identified Threats prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach March 4, 2022 OIG-22-29	I&A identified threats prior to the attack on the Capitol on January 6, 2021, but it did not disseminate products about these threats until after the attack occurred. As a result, I&A did not provide its state, local, and federal partners with timely, actionable, and predictive intelligence.	The Under Secretary for Intelligence and Analysis should provide enhanced annual training and guidance to Open-Source Collection Operations staff reviewing the Intelligence Oversight Program and Guidelines, including all criteria for reporting open-source intelligence information.	**I&A has not yet taken actions to implement this recommendation**. According to OIG officials, OIG is waiting for I&A to provide evidence of training guidance that aligns with criteria for reporting information from social media and other publicly available sources.
		The Under Secretary for Intelligence and Analysis should develop and implement a process to provide new Open-Source Collection Operations members with adequate training and guidance with input from experienced collectors or the Intelligence Training Academy.	**I&A took actions to fully implement the recommendation**. According to OIG officials, new Open-Source Collection Operations staff received training from the experienced collectors as well as from the Intelligence Training Academy.
		The Under Secretary for Intelligence and Analysis should establish and implement a process to request and receive timely reviews for open source intelligence products when they relate to upcoming events or urgent threats.	**I&A took actions to fully implement the recommendation**. According to OIG officials, I&A addressed this recommendation by issuing a Standard Operating Procedure for Producing and Disseminating Open-Source Collection Operations Branch Products in June 2022.
		The Under Secretary for Intelligence and Analysis should develop and implement policies, procedures, or guidance on the timely issuance of warning analysis, both strategic and tactical, about threats or upcoming events across I&A's mission areas.	**I&A has not yet taken actions to implement this recommendation**. According to OIG officials, I&A has not yet developed guidance that addresses the timely issuance of I&A analytic products (i.e., finished intelligence).
		The Under Secretary for Intelligence and Analysis should create and implement redundant capabilities for I&A to disseminate intelligence products addressing departmental threats, including Field Intelligence Reports and Open-Source Intelligence Reports.[a]	**I&A took actions to fully implement the recommendation**. According to OIG officials, I&A developed a new Field Intelligence Report tool that implements redundant dissemination mechanisms, allowing I&A to disseminate the reports through an alternate system, if necessary.

Report	Summary of Findings	Recommendation	Status (as of March 2023)
DHS Actions Related to an I&A Intelligence Product Deviated from Standard Procedures April 26, 2022 OIG-22-41	DHS did not comply with applicable Intelligence Community standards and requirements when editing and disseminating an I&A intelligence product regarding Russian interference in the 2020 U.S. Presidential election.	The Under Secretary for Intelligence and Analysis should work with the DHS Secretary and four oversight entities to identify and implement changes to the review and dissemination process for I&A's election-related intelligence products to ensure they are in accordance with applicable policies and guidelines.	**I&A has not yet taken actions to implement this recommendation**. According to OIG officials, I&A has plans to implement this recommendation but has not yet done so.
The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting July 6, 2022 OIG-22-50	I&A's challenges with the collection, management, and protection of open-source intelligence may be attributed to insufficient policies and procedures, inadequate internal controls and training, and a reliance on an outdated and unreliable information technology system to create and disseminate reports.	The Deputy Under Secretary for Intelligence Enterprise Operations should finalize and implement an overarching policy and standard operating procedures to guide the timely, complete, and accurate review and release of open source intelligence reports.	**I&A took actions to fully implement the recommendation**. According to OIG officials, I&A addressed this recommendation by issuing a Standard Operating Procedure for Producing and Disseminating Open Source Collection Operations Branch Products in June 2022.
		The Deputy Under Secretary for Intelligence Enterprise Operations should establish a standard process to determine whether additional oversight or review is needed for open source intelligence reports before their dissemination.	**I&A took actions to fully implement the recommendation**. According to OIG officials, I&A addressed this recommendation by issuing its Standard Operating Procedure for Producing and Disseminating Open-Source Collection Operations Branch Products in June 2022
		The Deputy Under Secretary for Intelligence Enterprise Readiness should develop and implement initial and ongoing, standardized training for open source intelligence collectors, certified release authorities, and content managers to ensure that these employees adhere to privacy protections, civil rights and civil liberties, and legal requirements.	**I&A took actions to fully implement the recommendation**. In its July 2022 report, OIG reported that I&A addressed this recommendation by providing updated training to all Open-Source Collection Operations personnel and scheduling refresher trainings in the future.
		The Deputy Under Secretary for Intelligence Enterprise Readiness should implement the information-technology system improvements needed to promote efficiency and enhance the Open-Source Collection Operations' ability to produce and disseminate open-source intelligence reports.	**I&A took actions to fully implement the recommendation**. In its July 2022 report, OIG reported that in August 2021, I&A deployed a new system to process Open-Source Intelligence Reports that increases automation and usability for open-source collections personnel.

Source: OIG. | GAO-23-105475

[a]Field Intelligence Reports document unevaluated information that responds to departmental requirements and are disseminated within DHS as well as to state, local, tribal, and territorial partners.

Appendix II: Office of Intelligence and Analysis Policies and Procedures to Protect Privacy, Civil Rights, and Civil Liberties

This appendix describes the Department of Homeland Security (DHS) Office of Intelligence and Analysis's (I&A) policies and procedures as of April 2023 to govern how I&A personnel are to protect the privacy, civil rights, and civil liberties of U.S. persons when conducting intelligence activities.[1]

Intelligence Oversight Guidelines

I&A's Intelligence Oversight Guidelines, which were approved by the Attorney General, are I&A's primary guidance regarding privacy, civil rights, and civil liberties, according to I&A officials. These guidelines identify various safeguards to help ensure that I&A personnel protect the privacy, civil rights, and civil liberties of U.S. persons when conducting intelligence activities (see table 5).

Table 5: Privacy, Civil Rights, and Civil Liberties Safeguards in the Office of Intelligence and Analysis (I&A) Intelligence Oversight Guidelines

Privacy Safeguards	Civil Rights Safeguards	Civil Liberties Safeguards
I&A personnel must • use overt collection methods or collect information from publicly available sources;[a] • use the least intrusive collection techniques feasible and sufficient when collecting U.S. persons information;[b] • collect U.S. persons information only when they have a reasonable belief that doing so would further a national or departmental mission; • access information systems with U.S. persons information only when they have appropriate security clearances and meet other access requirements; • retain U.S. persons information only for as long as is necessary to fulfill the specified purpose; • conduct searches in information systems that minimize the amount of U.S. persons information returned; and • delete U.S. persons information that does not meet certain requirements for permanent retention.	I&A personnel may not engage in intelligence activities based solely on an individual's or group's race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, or nationality.	I&A personnel may not engage in intelligence activities for the sole purpose of monitoring activities protected by the First Amendment.[c] I&A personnel may not engage in intelligence activities for the purpose of affecting the U.S. political process.

Source: Department of Homeland Security Office of Intelligence and Analysis, Intelligence Oversight Guidelines (Washington, D.C.: Jan. 2017) | GAO-23-105475

[1]In addition to these policies, several other entities have issued policies and guidance that I&A personnel, among others, are to follow to protect privacy, civil rights, and civil liberties. These entities include the Office of the Director of National Intelligence, the DHS Office of the General Counsel, the DHS Privacy Office, and the DHS Office for Civil Rights and Civil Liberties. This appendix does not summarize policies and guidance developed by other entities because they were outside the scope of our review.

Note: The Intelligence Oversight Guidelines do not apply I&A personnel conducting activities for non-intelligence purposes, such as administrative or oversight activities, reporting a crime, or responding to a Freedom of Information Act request.

[a]Overt collection consists of activities that are openly acknowledged by or readily attributable to the U.S. government or that would be acknowledged in response to a direct inquiry. Information is publicly available if it was published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event open to the public.

[b]U.S. persons information is either a single item of information or information that, when combined with other available information, is reasonably likely to identify one or more specific U.S. persons. A U.S. person is: (1) A U.S. citizen, (2) a foreign national known by the intelligence element to be a lawful permanent resident, (3) an unincorporated association substantially composed of U.S. citizens or permanent residents, or (4) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 3.5(k).

[c]The First Amendment to the U.S. Constitution protects the freedoms of speech, press, association, and assembly, among others. U.S. Const. amend. I. The government generally may not prohibit speech because of its message, ideas, subject matter, or content—even speech that may be viewed by some as offensive or disagreeable. The Privacy Act of 1974 also restricts the ability of agencies that maintain a system of records to maintain records describing how any individual exercises First Amendment rights unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity. 5 U.S.C. § 552a(e)(7). The First Amendment does not protect certain categories of activity, such as "advocacy intended, and likely, to incite imminent lawless action," "so-called 'fighting words,'" and "true threats." United States v. Alvarez, 567 U.S. 709, 717 (2012) (citing Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam); Chaplinsky v. New Hampshire, 315 U.S. 568, 571-72 (1942); Watts v. United States, 394 U.S. 705, 708 (1969) (per curiam)).

For example, I&A personnel are authorized to collect information only via overt collection methods or from publicly available sources. Overt collection consists of activities that are openly acknowledged by or readily attributable to the U.S. government or that would be acknowledged in response to a direct inquiry. Publicly available information, in general, is information that is published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, or is available to the public by subscription or purchase.[2] In addition, I&A personnel are authorized to engage in intelligence activities only when they have a reasonable belief that such activities would further one or more national or departmental missions (see table 6).

[2]In addition, publicly available information includes information that could be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event open to the public. Social media sites and other electronic fora that limit access by use of criteria that cannot generally be satisfied by members of the public are not considered publicly available sources.

Table 6: Office of Intelligence and Analysis (I&A) National and Departmental Missions

I&A personnel are authorized to engage in intelligence activities when they have a reasonable belief that doing so would support one or more national or departmental missions.[a]

National Missions	Departmental Missions
Assist executive branch officials in developing and conducting foreign, defense, and economic policies, or protecting national interests from foreign security threats. Foreign security threats include • international terrorism; • the development, proliferation, or use of weapons of mass destruction; • intelligence activities directed against the U.S.; • international criminal drug activities; and • other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents. National missions may also include assisting Congress, as appropriate.	Assist public or private sector entities in identifying protective and support measures regarding threats to homeland security. Such threats include domestic terrorism; threats to critical infrastructure and key resources; significant threats to national economic security, public health, or public safety; major disasters and other catastrophic acts; and severe, large-scale threats whose response is beyond the capabilities of affected state and local governments. Departmental missions also include support provided to DHS officials, offices, or elements in the execution of their lawful missions. For example, I&A supports U.S. Customs and Border Protection's inspection of travelers at U.S. ports of entry.

Source: Department of Homeland Security Office of Intelligence and Analysis, Intelligence Oversight Guidelines (Washington, D.C.: Jan. 2017). | GAO-23-105475

[a]I&A's Intelligence Oversight Guidelines define reasonable belief as a belief based on facts and circumstances such that a reasonable person would hold that belief. A reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge as applied to particular facts and circumstances. According to I&A officials, this definition is consistent across the U.S. Intelligence Community.

Further, I&A personnel may disseminate information about U.S. persons only when there is a reasonable belief that doing so would help the recipient of that information fulfill one or more of its lawful intelligence, counterterrorism, law enforcement, or other homeland-security-related functions. In addition, I&A personnel are to receive training about the safeguards in the guidelines. Further, I&A is to conduct certain activities to monitor the extent to which its personnel are implementing the guidelines appropriately.

Policies Regarding the Review of Intelligence Products

Review Process for Finished Intelligence Products

Finished intelligence products contain the analytic assessments and judgments of I&A analysts and are intended to be disseminated outside of

DHS. Under I&A policy, all finished intelligence products that contain U.S. persons information are to be reviewed by several entities internal and external to I&A before they can be disseminated outside of I&A.[3] These reviews are to serve several purposes, one of which is to help ensure appropriate protections of individuals' privacy, civil rights, and civil liberties (see fig. 8).[4]

Figure 8: Review Process for Office of Intelligence and Analysis (I&A) Finished Intelligence Products

Source: Department of Homeland Security Office of Intelligence and Analysis, Policy Instruction IA-901: Office of Intelligence and Analysis Production of Finished Intelligence (Revision 3), Aug. 25, 2022. | GAO-23-105475

[a]These criteria are that the product: (1) addresses or describes populations discernible by race, ethnicity, gender, religion, sexual orientation, gender identity, country of origin, or nationality; (2) references or describes the activities of minors (under 18) individually or as a discernible population; (3) includes personally identifiable information or identifies an individual by context; (4) reflects analysis based upon or derived from a bulk data collection containing information about U.S. persons; (5) names elected government officials, candidates for elected office, or U.S. political parties; (6) references or describes the political, religious, ideological, or Constitutionally protected speech or activity of a U.S person or person in the U.S.; or (7) meets any additional criteria promulgated in writing by the Deputy Under Secretary in coordination with the Oversight Offices.

[3]Department of Homeland Security, Office of Intelligence and Analysis, *Office of Intelligence and Analysis Production of Finished Intelligence,* Policy Instruction IA-901 (Revision 3) (Washington, D.C.: Aug. 25, 2022).

[4]These reviews also aim to ensure that I&A's finished intelligence products (1) are issued in a timely manner; (2) conform to I&A's authorized missions, analytic tradecraft and qualitative standards, and legal, policy, and regulatory requirements; (3) respond to the requirements of I&A customers; and (4) maintain the integrity of the intelligence process.

If any of the oversight offices identified in figure 8 determines that a finished intelligence product does not adequately protect privacy, civil rights, or civil liberties, the relevant I&A analytic office is to address this either by (1) identifying a resolution that is mutually acceptable to the I&A personnel responsible for the product and the Oversight Office that identified the issue, or (2) elevating the issue to the relevant mission center director. If the mission center director is not able to resolve the issue, the matter is to be elevated to I&A's Deputy Under Secretary for review. If needed, the matter may be further elevated to the Under Secretary for Intelligence and Analysis, among others, for resolution.

Review Processes for Raw Intelligence Products

Raw intelligence products contain unanalyzed content that is the same or substantially the same as when I&A acquired it. I&A established processes for reviewing two types of raw intelligence products before these products may be disseminated: (1) Open-Source Intelligence Reports and (2) Field Intelligence Reports.[5]

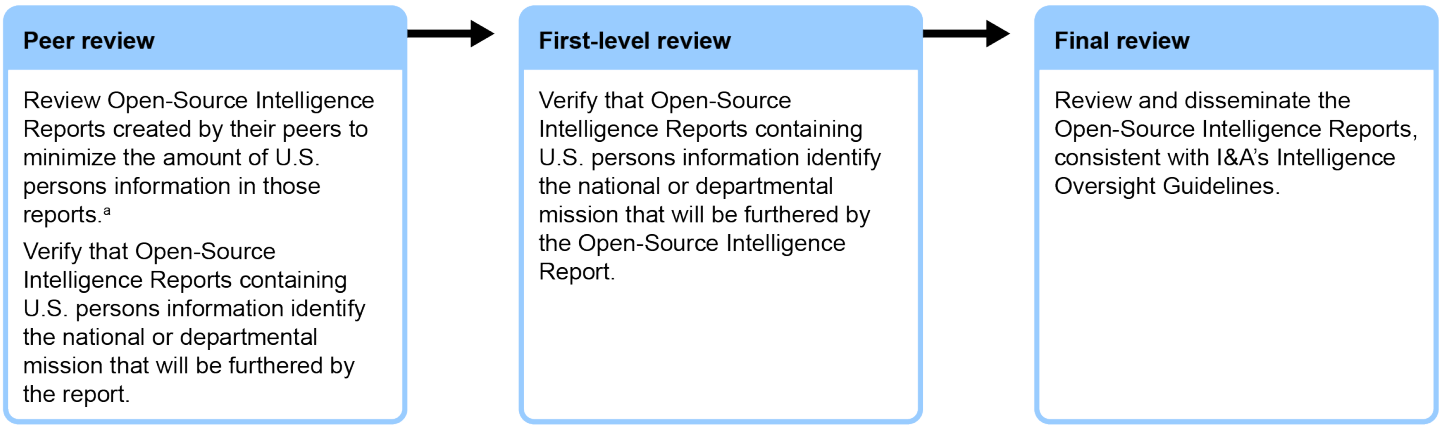
For Open-Source Intelligence Reports, I&A procedures direct personnel within its Current and Emerging Threats Center to review these products to minimize the amount of U.S. persons information in them (see fig. 9).[6] I&A personnel who collect open-source information may—with approval from their supervisors—consult the Oversight Offices when creating or reviewing Open-Source Intelligence Reports if they have concerns relating to privacy, civil rights, or civil liberties.[7]

[5]I&A officials told us that I&A also conducts a review process for a third type of raw intelligence product—called Intelligence Information Reports—in accordance with DHS policy. See Department of Homeland Security, *DHS Intelligence Information Report (IIR) Standards,* DHS Instruction 264-01-006 (Washington, D.C.: Jan. 12, 2017). We did not review this policy because it was not issued by I&A.

[6]Department of Homeland Security, Office of Intelligence and Analysis, *Current and Emerging Threats Center Standard Operating Procedure: Producing and Disseminating Open-Source Collection Operations Branch Products* (June 14, 2022).

[7]Collection Officers do not need supervisory approval to contact the Oversight Offices in the case of a potential questionable intelligence activity.

Figure 9: Review Process for Office of Intelligence and Analysis (I&A) Open-Source Intelligence Reports



Source: Department of Homeland Security Office of Intelligence and Analysis, *Current and Emerging Threats Center Standard Operating Procedure: Producing and Disseminating Open-Source Collection Operations Branch Products*, June 14, 2022. | GAO-23-105475

[a]For the purposes of intelligence activities, a U.S. person is: (1) a U.S. citizen, (2) a foreign national known by the intelligence element to be a lawful permanent resident, (3) an unincorporated association substantially composed of U.S. citizens or permanent residents, or (4) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended, ¶ 3.5(k).

For the Field Intelligence Reports, I&A's policy states that designated personnel are to review these products before they are disseminated to ensure they comply with applicable law and policy and appropriately protect individuals' privacy, civil rights, and civil liberties.[8] These personnel need to have completed specialized training and be authorized by the Under Secretary for Intelligence and Analysis to review and release Field Intelligence Reports. If a Field Intelligence Report is not reviewed by these personnel, it is to be reviewed by the Intelligence Law Division of DHS's Office of the General Counsel and I&A's Intelligence Oversight Officer prior to its release.[9]

[8]Department of Homeland Security, Office of Intelligence and Analysis, *Office of Intelligence and Analysis Field Intelligence Report Program,* Policy Instruction IA-905 (Washington, D.C.: May 22, 2017).

[9]If a Field Intelligence Report will be disseminated outside of DHS, it is to be reviewed by these two offices and, in some cases, the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office prior to its release.

Policies Regarding Sources from Which I&A May Collect Information

Social Media Platforms

I&A's policy instruction regarding the use of publicly available information states that only certain I&A personnel are authorized to collect information from social media platforms.[10] Among other requirements, these personnel must receive training regarding privacy, civil rights, and civil liberties; intelligence oversight; and applicable legal authorities prior to being permitted to review information or intelligence from social media sources. In addition, personnel may not engage with any social media users, such as by friending, interviewing, chatting, or posting on the platform.

Human Sources

I&A's policy regarding its overt human intelligence collection program states that only certain I&A personnel are authorized to collect information from U.S. citizens and other persons through observation or direct engagement.[11] I&A may disseminate this information to its partners—including federal, state, local, tribal, territorial, foreign, and private sector entities—in accordance with certain requirements. For example, I&A personnel must ensure that any collection from human sources is within the scope of their authorized intelligence activities and mission.

Further, when interviewing human sources, I&A personnel must explicitly state that (1) they are an employee of the U.S. Department of Homeland Security; (2) the source's participation in the interview is voluntary; (3) the interview may be terminated by either party at any time; (4) the I&A interviewer will not exercise any preferential or prejudicial treatment in exchange for the source's cooperation; and (5) the source has no right to review, edit, or control I&A's use of any information collected and products derived from the interview, except for access rights provided by the Privacy Act and the Freedom of Information Act. I&A personnel may not direct interviewees to collect information on behalf of I&A.

[10]Department of Homeland Security, Office of Intelligence and Analysis, *Official Usage of Publicly Available Information,* Policy Instruction IA-900 (Washington, D.C.: Jan. 13, 2015).

[11]Department of Homeland Security, Office of Intelligence and Analysis, *Overt Human Intelligence Collection Program*, Policy Instruction IA-907 (Washington, D.C.: June 29, 2016).

Signals Intelligence

I&A personnel are not authorized to conduct signals intelligence—that is, they may not collect information from data transmissions, such as electronic signals that contain speech or text. However, I&A policy permits I&A personnel to retain and disseminate information (including personally identifiable information) that was obtained by other entities through signals intelligence, within certain parameters.[12] Among other requirements, such information may not be retained or disseminated solely because of the nationality or place of residence (i.e., foreign status) of the person(s) concerned and must relate to a national or departmental intelligence requirement.

Other Policies for Protecting Privacy, Civil Rights, and Civil Liberties

Safeguarding Sensitive Personally Identifiable Information

I&A policy requires that I&A personnel take measures to protect Sensitive Personally Identifiable Information.[13] Sensitive Personally Identifiable Information is personally identifiable information that—if lost, compromised, or disclosed without authorization—could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. This policy complements DHS's policy and guidance on personally identifiable information by identifying additional training requirements and supervisory responsibilities.

Safeguarding Congressional Identity Information

I&A has established policies regarding how personnel are to protect personal information about Members of Congress and congressional staff.[14] For example, I&A must mask congressional identity information—referring to it only as "U.S. Member of Congress" or "U.S. Congressional staff"—unless unmasking is approved by I&A's Intelligence Oversight Officer and DHS's Intelligence Law Division of the Office of the General Counsel. I&A personnel must notify both of these entities before

[12]Department of Homeland Security, Office of Intelligence and Analysis, *Safeguarding Personal Information Collected from Signals Intelligence Activities,* Policy Instruction IA-1002 (Washington, D.C.: Jan. 16, 2015).

[13]Department of Homeland Security, Office of Intelligence and Analysis, *I&A Handling of Sensitive Personally Identifiable Information,* Policy Instruction IA-106 (Washington, D.C.: Mar. 26, 2012).

[14]Department of Homeland Security, Office of Intelligence and Analysis, *Special Handling Requirements for Congressional Identity Information*, Instruction IA-908 (Washington, D.C.: Mar. 30, 2023)

disseminating a product with congressional identity information, regardless of whether this information is masked or unmasked.

I&A's Intelligence Oversight Officer is to submit a report biannually to the Office of the Director of National Intelligence containing, among other information, the number of intelligence products issued by I&A containing masked and unmasked congressional identity information. Further, all I&A personnel are to receive training annually on I&A's policies regarding protecting congressional identity information.

Disclosing Information about Certain Foreign Nationals

I&A has established policies regarding disclosing information about certain foreign nationals who are seeking, or have been approved for, nonimmigrant or immigrant status and who have been victims of violence or abuse.[15] I&A personnel are to record each instance where they have disclosed information about these persons and report this disclosure to I&A's Intelligence Oversight Officer as soon as is practicable.

[15]Department of Homeland Security, Office of Intelligence and Analysis, *Disclosure of Information on Applicants or Beneficiaries Falling Under T Visa, U Visa, or Violence Against Women Act Protections,* Policy Instruction IA-903 (Washington, D.C.: June 11, 2015). For background, see 8 U.S.C. § 1367 (Penalties for Disclosure of Information).

Appendix III: Office of Intelligence and Analysis Performance Measures and Strategic Goals

The Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) monitors its performance through 13 performance measures and shares this information with various entities, including DHS and the Office of the Director of National Intelligence (ODNI). In addition, according to I&A officials, I&A shares performance information throughout the organization to help the leadership of mission centers and other operational units stay on track to meet the annual performance targets that I&A sets for each measure. For example, I&A shares performance information with managers through an online dashboard and monthly and quarterly reports. In fiscal year 2022, I&A met or exceeded the targets for nine of its 10 unclassified performance measures (see table 7).

Table 7: Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) Performance Measures, Targets, and Results Reported to DHS and the Office of the Director of National Intelligence (ODNI), Fiscal Years (FY) 2020 through 2022

Measure	Reported to DHS, ODNI, or both	FY 2020		FY 2021		FY 2022	
		Target	Result	Target	Result	Target	Result
Percent of finished intelligence products rated satisfactory and useful by customers	DHS	—[a]	—	80%	90%	80%	89%
Percent of finished intelligence products shared with state, local, tribal, territorial, and private sector partners	DHS	—[a]	—	50%	41%	50%	56%
Number of finished intelligence products shared with the Intelligence Community	DHS	—[a]	—	250	308	262	232
Percent of finished intelligence products shared with the Intelligence Community	DHS ODNI	95%	93%	95%	80%	95%	96%
Percent of finished intelligence products aligned to key intelligence questions	DHS ODNI	90%	96%	80%	92%	80%	100%
Percent of finished intelligence products incorporating DHS and/or state- and local-originated data	DHS ODNI	60%	43%	60%	46%	60%	76%
Percent of raw intelligence reports shared with state, local, tribal, territorial, and private sector partners	ODNI	50%	50%	50%	37%	50%	62%
Percent of DHS I&A raw intelligence reporting evaluated	ODNI	48%	19%	48%	38%	48%	61%
Percent of DHS I&A collection aligned to the National Intelligence Priorities Framework[b]	ODNI	—[c]	—	—	—	—	—

Measure	Reported to DHS, ODNI, or both	FY 2020		FY 2021		FY 2022	
		Target	Result	Target	Result	Target	Result
Percent of essential elements of information or intelligence topic information needs against National Intelligence Priorities Framework cyber threat category (priority 1) addressed by intelligence products[d]	ODNI	—[c]	—	—	—	—	—
Percent of essential elements of information or intelligence topic information needs against National Intelligence Priorities Framework cyber threat category (priorities 2 and 3) addressed by intelligence products	ODNI	—[c]	—	—	—	—	—
Percent of cyber intelligence products that address the key intelligence questions as specified in the Cyber Unifying Intelligence Strategy	ODNI	60%	36%	60%	92%	60%	89%
Percent of cyber intelligence products that identify cyber threats to U.S. infrastructure or vital networks automatically released as "UNCLASSIFIED//FOR OFFICIAL USE ONLY"	ODNI	60%	44%	60%	53%	60%	65%

Legend:
— = not available or not included

Source: I&A. | GAO-23-105475

[a]Three of I&A's measures were new in fiscal year 2021 and thus did not have any targets or results in fiscal year 2020.

[b]The National Intelligence Priorities Framework is the system directed by the President for prioritizing national intelligence activities, managing risk, and assessing mission performance.

[c]Targets and results for these measures are classified, according to I&A officials, and thus are not reproduced here.

[d]I&A officials told us that they use the Department of Defense definition of essential elements of information, which is the "most critical information requirements regarding the adversary and the environment needed by the commander to assist in reaching a decision." They also stated that intelligence topic information needs broadly define the information that intelligence analysts and consumers need from the Intelligence Community.

Table 8 shows the alignment between I&A's strategic goals and performance measures based on our analysis of I&A's information.

Table 8: Alignment between Department of Homeland Security (DHS) Office of Intelligence and Analysis's (I&A) Strategic Goals and Performance Measures

Strategic Goals	Extent to which One or More Performance Measures Align with Strategic Goal
Cyber. Detect and understand cyber threats to identify and mitigate risks across DHS, the federal government, and the Homeland Security Enterprise.[a]	●
Information Sharing and Safeguarding. 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.	●
Operational Intelligence. Provide tailored intelligence, using unique DHS intelligence, information, and other data, and increase collaboration to enable federal, state, local, territorial, and private-sector operations to prevent threats to the U.S. homeland and interests.	●
Partnerships. Expand and strengthen partnerships to enrich intelligence, inform decisions, and enable actions throughout the Homeland Security Enterprise.	◐
Strategic Intelligence. 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.	◐
Anticipatory Intelligence. Identify new trends and changing conditions to alert customers and prepare for emerging threats to the U.S. homeland.	○
Business Functions. Enhance I&A business functions to enable mission success.	○
Counterintelligence. Expand counterintelligence coordination across DHS, state, local, tribal, territorial, private sector, and federal partners to rapidly recognize the contemporary threat environment, identify vulnerabilities, and implement appropriate countermeasures.	○
Counterterrorism. Detect terrorists and collaborate with partners on operations to prevent terrorist attacks against the U.S. homeland, U.S. persons, and U.S. interests.	○
Economic Security. Identify and understand foreign economic threats and engage DHS, other federal, and state, local, tribal, territorial, and private sector partners to inform homeland policy deliberations that preserve and enhance the competitiveness of the U.S. economy.	○
Homeland Security Enterprise Analytic and Collection Activities. Integrate analytic and collection requirements across the DHS Intelligence Enterprise to support departmental, state, local, tribal, territorial, and private sector partners.	○
Homeland Security Enterprise Integration of Personnel. Create and implement synchronized approaches to improve the skills and integration of homeland intelligence professionals.	○
People. Empower and develop all levels of the DHS intelligence workforce to build a collaborative and respectful organization dedicated to protecting the U.S. homeland.	○
Privacy, Civil Liberties, and Transparency. Protect privacy and civil liberties and strengthen transparency to foster accountability, trust, and confidence with our partners and the public.	○
Technological Innovation. Promote technological advancements, securing and modernizing systems, to increase information access and data resiliency throughout the Homeland Security Enterprise allowing peak performance.	○
Transnational Organized Crime. Enhance understanding of tactics, trends, and actors to combat transnational criminal activities that threaten the U.S. homeland and interests.	○

Legend:
● = clear alignment between strategic goal and performance measures

◐ = partial alignment between strategic goal and performance measures
○ = no alignment between strategic goal and performance measures

Source: GAO analysis of I&A information. | GAO-23-105475

[a]The Homeland Security Enterprise is comprised of federal, state, local, tribal, nongovernmental, and private sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of the U.S. and the U.S. population.

Appendix IV: GAO Leading Practices for Strategic Planning and Performance Management

GAO's prior work has identified leading practices that government agencies should follow when creating strategic plans, performance measures, and other elements of performance measurement systems. This appendix provides an overview of these practices.

Define Mission and Desired Outcomes

GAO has previously reported that strategic plans should be the starting point for an agency's performance measurement efforts.[1] Each plan should include:

- A comprehensive mission statement based on the agency's statutory requirements. The mission statement brings the agency into focus by explaining why the agency exists, what it does, and how it does it.
- A set of outcome-related strategic goals, which are an outgrowth of the mission statement. The goals explain the purposes of the agency's programs and the results that the programs intend to achieve.
- A description of how the agency intends to achieve its strategic goals.

Measure Performance

GAO's prior work shows that agencies should align their activities and resources to achieve their strategic goals by establishing clear hierarchies of performance goals and measures.[2] Under these hierarchies, agencies should link the goals and performance measures for each organizational level to successive levels and ultimately to the agency's strategic goals.

We have previously reported that measuring performance allows agencies to track the progress they are making toward their goals and gives managers information on agencies' incremental progress toward strategic goals.[3] To create effective performance measures, agencies should assess whether

- there is a relationship between the performance goals and measures and the agency's goals and mission,
- the performance measures are clearly stated,

[1]GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1, 1996).

[2]GAO/GGD-96-118.

[3]GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, GAO-03-143 (Washington, D.C.: Nov. 22, 2002).

- the performance measures have targets that allow for comparison with actual performance,
- the performance goals and measures are objective,
- the performance goals and measures provide a reliable way to assess progress,
- the performance measures sufficiently cover a program's core activities,
- there appears to be limited overlap among the performance measures,
- there appears to be a balance among the performance goals and measures, and
- the program or activity has performance goals and measures that cover governmentwide priorities.

Use Performance Information

The next key step in building successful, results-oriented agencies—after establishing a mission and goals and building a performance measurement system—is to put performance data to work. Our work has found managers should use performance information to identify problems and take corrective actions, to develop strategies and allocate resources, to recognize and reward performance, and to identify more effective approaches to program implementation and share those approaches more widely across the agency.[4]

In addition, we have identified five practices that can help ensure performance information is used in decision-making: (1) demonstrating management commitment; (2) aligning agency goals, objectives, and measures; (3) improving the usefulness of performance information to better meet management's needs; (4) developing agency capacity to effectively use performance information; and (5) frequently and effectively communicating performance information within the agency.[5]

[4]*Managing for Results*: *Enhancing Agency Use of Performance Information for Management Decision Making,* GAO-05-927 (Washington, D.C.: Sept. 9, 2005).

[5]GAO-05-927.

Appendix V: Agency Comments

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 11, 2023

Triana McNeil
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-105475, "Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Effectiveness"

Dear Ms. McNeil:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's recognition of the efforts made by its Office of Intelligence and Analysis (I&A) to implement safeguards to protect the privacy, civil rights, and civil liberties of U.S. persons, including through the conduct of preliminary inquiries into alleged violations of law or policy by I&A personnel engaging in intelligence activities. GAO also recognized DHS's efforts to incorporate input from its analytic centers and partners to prioritize threats and guide its intelligence production. I&A has various mechanisms to gather customer's interests, concerns, and feedback, including its annual Compendiums of Key Intelligence Questions, which captures state, local, tribal, territorial, and private sector partners' highest priority intelligence issues and provides a roadmap for analytic collaboration with these partners.

I&A has also taken recent steps to emphasize its commitment to protecting the rights of U.S. persons and appropriately prioritizing intelligence topics. On May 4, 2023, the Under Secretary for Intelligence and Analysis announced an internal realignment within I&A. Among other things, I&A has established a new Transparency and Oversight Program Office that consolidates and elevates I&A's transparency and oversight functions, including intelligence oversight in a single office to be led by a senior

executive reporting to the Under Secretary for Intelligence and Analysis. This will provide consistent and high-level focus on I&A's responsibility to build and maintain the policies and processes that ensure its operations comply with law and policy and fully safeguard the privacy, civil rights, and civil liberties of all Americans. As part of I&A's May 2023 internal realignment, I&A also established an Intelligence Enterprise Program Office to enhance its management and support of DHS intelligence components, including the Intelligence Enterprise's prioritization of threats.

DHS remains committed to ensuring that I&A's intelligence activities are conducted in compliance with law and policy and in a manner that protects individuals' privacy, civil rights, and civil liberties. We are equally committed to ensuring that those activities are measured in ways that align with I&A's strategic goals.

The draft report contained nine recommendations, with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2023.08.11 13:45:32 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

2

Enclosure: Management Response to Recommendations Contained in GAO-23-105475

GAO recommended that the Under Secretary for Intelligence and Analysis:

Recommendation 1: Ensure that I&A's intelligence oversight branch documents reviews conducted to verify I&A personnel's compliance with I&A's guidelines for protecting privacy, civil rights, and civil liberties.

Response: Concur. I&A's Transparency and Oversight Program Office is in the process of developing separate Standard Operating Procedures (SOPs) governing the conduct of compliance inquiries and reviews undertaken by its Privacy and Intelligence Oversight Branch. These SOPs will require I&A intelligence oversight personnel to formally document their compliance inquiries and reviews. The Transparency and Oversight Program Office anticipates issuing the SOP on compliance inquiries by October 31, 2023, and plans on issuing the SOP on compliance reviews by December 29, 2023. Estimated Completion Date (ECD): December 29, 2023.

Recommendation 2: Establish a goal for the number of compliance reviews that I&A's intelligence oversight branch is to conduct during a given period to verify personnel's compliance with I&A's guidelines for protecting privacy, civil rights, and civil liberties.

Response: Concur. On May 4, 2023, the Under Secretary for Intelligence and Analysis established a new Transparency and Oversight Program Office, to be led by a senior executive reporting to the Under Secretary who provides guidance and direction to the Intelligence Oversight Officer. As part of their duties, the director of this new office will work with the Intelligence Oversight Officer to set a goal for the number of compliance reviews to be conducted during fiscal year 2024. ECD: September 29, 2023.

Recommendation 3: Assess the intelligence oversight branch's performance against its goal for compliance reviews, including identifying any factors preventing it from meeting this goal and any needed corrective actions.

Response: Concur. As part of their duties, the director of the newly-established Transparency and Oversight Program Office will review the performance of the intelligence oversight branch against its goal for compliance reviews on a semi-annual (every six months) basis beginning in fiscal year 2024. ECD: April 30, 2024.

Recommendation 4: Establish time frames for completing I&A's standard operating procedure for conducting preliminary inquiries and finalize this procedure according to these time frames.

3

Response: Concur. I&A's Transparency and Oversight Program Office is on track for completing and issuing the SOP for conducting preliminary inquiries by October 31, 2023. ECD: October 31, 2023.

Recommendation 5: Identify who is responsible for conducting the audits of information systems and bulk data described in I&A's Intelligence Oversight Guidelines, and to whom the results of these audits should be reported.

Response: Concur. I&A's Transparency and Oversight Program Office, in coordination with its Director of Technology and Data Services and Strategy, Policy, and Plans Branch, will develop an SOP for conducting audits of information systems and bulk data. The SOP will also specify roles and responsibilities. The Transparency and Oversight Program Office anticipates issuing the SOP by February 29, 2024. ECD: February 29, 2024.

Recommendation 6: Ensure that the responsible entities conduct audits of information systems and bulk data, as described in I&A's Intelligence Oversight Guidelines.

Response: Concur. As part of their duties, the director of the newly-established Transparency and Oversight Program Office will work with the entities responsible for conducting audits of information systems and bulk data to set a goal for the number of such audits to be conducted during fiscal year 2024 upon issuance of the SOP as described in response to Recommendation 5 above. The director will then review the performance of the responsible entity against that goal twice over the remainder of the fiscal year. ECD: September 30, 2024.

Recommendation 7: Develop performance measures for I&A that clearly align with and assess progress toward its strategic goals.

Response: Concur. I&A's Chief Operating Officer Directorate will revise its performance measures to ensure that they clearly align with and assess progress towards the organization's goals in its next strategic plan, which will cover fiscal years 2025 through 2029. In the interim, I&A's Chief Operating Officer Directorate will continue to gather performance data at the strategic level, including performance aligned to I&A's current Strategic Plan, and other guidance, as appropriate. ECD: April 30, 2024.

Recommendation 8: Develop and implement a process to submit the statutorily required annual report related to customer feedback on intelligence products to relevant congressional committees.

Response: Concur. I&A, through its Chief Operating Officer Directorate, will resume submission of the statutorily required annual report related to customer feedback on intelligence products by December 29, 2023 and annually thereafter using its standard Executive Secretariat process for internal taskings. ECD: December 29, 2023.

4

Recommendation 9: Assess the extent to which customer feedback data meet its need to understand its customers' interests and, if necessary, take steps to collect more appropriate data.

Response: Concur. I&A Office of Management will assess customer feedback data report the results of this assessment to the Under Secretary for Intelligence and Analysis for their consideration. ECD: April 30, 2024.

5

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Triana McNeil, Director, Homeland Security and Justice, (202) 512-8777 or McNeilT@gao.gov

Staff Acknowledgments

In addition to the contact named above, Mona Nichols Blake (Assistant Director), Elizabeth Poulsen (Analyst-in-Charge), Nanette Barton, Benjamin Crossley, Dominick Dale, Michele Fejfar, Kaelin Kuhn, Sasan J. “Jon” Najmi, Carl Potenzieri, Eric Warren, and Christopher Zubowicz made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548