

The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting





OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

July 6, 2022

MEMORANDUM FOR: The Honorable Kenneth L. Wainstein
Under Secretary
Office of Intelligence and Analysis

FROM: Joseph V. Cuffari, Ph.D. **JOSEPH V CUFFARI**
Inspector General

SUBJECT: *The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting Process*

Digitally signed by
JOSEPH V CUFFARI
Date: 2022.07.05
15:22:21 -04'00'

Attached for your action is our final report, *The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving the program's overall effectiveness. Your office concurred with all four recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 and 2 open and resolved. Once your office has fully implemented the open recommendations, please submit a formal closeout letter to us within 30 days so that we may close these recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Recommendations 3 and 4 are resolved and closed.

Please send your response or closure request to
OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

The Office of Intelligence and Analysis Needs to Improve Its Open Source Intelligence Reporting Process

July 6, 2022

Why We Did This Audit

The Department of Homeland Security must be prepared to respond to potential threats to the United States. To identify and mitigate threats, I&A shares intelligence and analysis with decision makers. We conducted this audit to determine the extent to which I&A has an effective process for collecting, managing, and protecting OSINT for operational and intelligence purposes.

What We Recommend

We made four recommendations to improve the efficiency and effectiveness of I&A's OSINT process.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Office of Intelligence and Analysis (I&A) is improving its process for collecting, managing, and protecting open source intelligence (OSINT) for operations and intelligence. We acknowledge I&A's recent efforts to address known challenges related to insufficient guidance and technology, but additional process improvements are needed to ensure intelligence reporting is effective. Additionally, stakeholder feedback indicated further improvements are needed to issue open source intelligence reports in a timely manner.

We attributed these challenges to insufficient policies and procedures to guide staff in their daily work, inadequate internal controls and training to promote adherence to standards and requirements, and reliance on an outdated and unreliable information technology system to create and disseminate reports. During our fieldwork, I&A began to resolve some of these challenges by drafting new policies, revising training, and upgrading its technology.

To accomplish its core mission of identifying and mitigating threats to the Nation, I&A must produce intelligence reports that are relevant, timely, and in line with evolving threats. The deficiencies identified by I&A and confirmed through this audit hinder I&A's ability to effectively inform decision makers about potential threats.

I&A Comments

I&A concurred with all four of our recommendations. Based on progress made following this audit, we are closing two of the four recommendations.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Table of Contents

Background	1
Results of Audit	3
I&A Has Taken Steps to Correct Known Deficiencies in Its Open Source Intelligence Process.....	4
Intelligence Reporting Timeliness Was Not Tracked	8
Multiple Factors Hinder Intelligence Reporting Process.....	10
Conclusion.....	15
Recommendations.....	15

Appendixes

Appendix A: Objective, Scope, and Methodology	19
Appendix B: I&A Comments to the Draft Report.....	21
Appendix C: I&A Organizational Structure	27
Appendix D: Summary of I&A's 2020 Internal Reviews	28
Appendix E: Office of Audits Major Contributors to This Report	29
Appendix F: Report Distribution	30

Abbreviations

CETC	Current and Emerging Threats Center
Cookbook	Open Source Collection Operations Cookbook
COVID-19	coronavirus disease 2019
HOST	Homeland Open Source Tool
I&A	Office of Intelligence and Analysis
IT	information technology
OSCO	Open Source Collection Operations
OSINT	open source intelligence
OSIR	open source intelligence report



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

The Department of Homeland Security must be prepared to respond to an ever-evolving landscape of potential threats facing the United States.¹ For example, terrorist groups attempt to mobilize people in the United States to exploit public fears associated with the coronavirus disease 2019 (COVID-19) pandemic and the post-2020 election period. State and non-state actors may also attempt to target our critical infrastructure and information networks to launch cyberattacks.² Timely, reliable intelligence and information is critical for DHS to keep the Nation safe, secure, and resilient.

Within DHS, the Office of Intelligence and Analysis (I&A) provides intelligence to its customers, including the DHS Intelligence Enterprise,³ the Intelligence Community,⁴ and state and local partners. I&A is the only Intelligence Community entity statutorily charged with delivering intelligence to state, local, tribal, territorial, and private sector partners, and with developing intelligence from those partners for the Department and the Intelligence Community.⁵ I&A has approximately 700 employees organized into five mission centers and three intelligence-related groups, including the Current and Emerging Threats Center (CETC). See Appendix C for I&A's organizational structure.

I&A shares unique intelligence and analysis to identify and mitigate threats to the Nation. I&A does this by providing its partners with products, including open source intelligence reports (OSIR).⁶ OSIRs are raw intelligence reports that include information related to active intelligence collection requirements.⁷ Some OSIRs are immediate warnings to law enforcement partners, while others

¹ *Homeland Threat Assessment*, October 2020, https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.

² The Intelligence Community's Election Threat Update from August 2020 and Microsoft's announcement of cyberattacks from China, Russia, and Iran provide evidence of this cyber threat. Cybercriminals also may target our networks to steal information, hold organizations hostage for ransom payment, and harm American companies for their own gain.

³ The DHS Intelligence Enterprise supports the unified collection, processing, analysis, production, and dissemination of national and departmental intelligence, both within the Department and by providing support to the Homeland Security Enterprise and the Intelligence Community. See <https://dhsconnect.dhs.gov/ie/Pages/default.aspx>.

⁴ The Intelligence Community is made up of 18 member organizations, including the Central Intelligence Agency, the Office of the Director of National Intelligence, and the National Security Agency.

⁵ IA-1000, *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines*.

⁶ Open source intelligence is publicly available information, such as social media and internet articles with unrestricted access.

⁷ Intelligence collection requirements are identified information gaps that justify the collection of specific intelligence data. I&A's Collection Management Division updates the active intelligence requirements regularly, in line with changing intelligence needs. Collection requirements that are no longer topical or needed are removed from the active list.



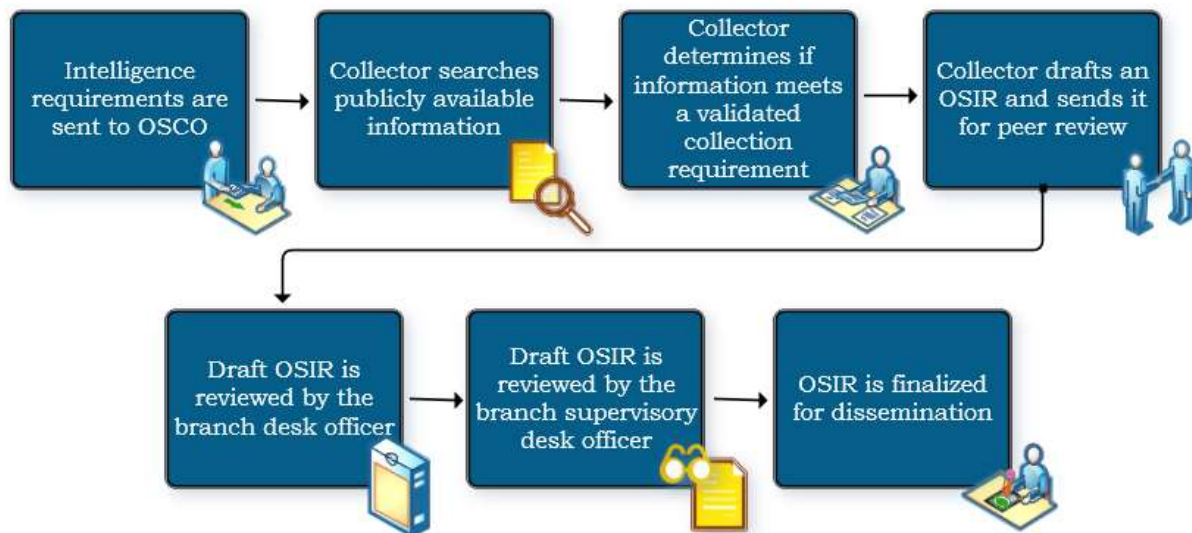
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

are pieces of raw intelligence that, when combined with other pieces of intelligence, provide a more long-term analysis product. From fiscal years 2018 to 2021,⁸ I&A disseminated an average of about 1,100 OSIRs per year.⁹ These OSIRs provided intelligence on bomb threats to major airlines, potential violence around the 2020 election, and a threat to the United States Embassy in Iraq, among others.

CETC's Open Source Collection Operations (OSCO) team collects and disseminates open source intelligence (OSINT). The process begins when CETC's Collection Management Division provides open source collection requirements to OSCO. Once OSCO determines that publicly available information meets a collection requirement, the collector drafts an OSIR. The OSIR is then reviewed by an OSCO peer, a branch desk officer, and a branch supervisory desk officer. After edits, comments, and questions are fully resolved, the supervisory desk officer disseminates the OSIR to the Intelligence Community; DHS components; and state, local, tribal, and territorial partners as needed. Until September 2021, collectors drafted OSIRs in the Homeland Open Source Tool (HOST), a database designed and maintained by I&A. Figure 1 shows the process for collecting OSINT and producing OSIRs for dissemination.

Figure 1. I&A's Open Source Intelligence Process



Source: DHS Office of Inspector General-generated based on I&A documentation

⁸ Due to the timing of our audit, FY 2021 data did not include September 2021.

⁹ In this report, dissemination refers to the publication of intelligence on classified or unclassified networks.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Executive Order 12333, which governs intelligence collection,¹⁰ establishes overarching goals and guidelines for the entire Intelligence Community to ensure that the United States receives the best intelligence possible. At the DHS level, guidelines for collecting, retaining, and disseminating information concerning U.S. persons are documented in the *Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines* (IA-1000).¹¹ These guidelines state that I&A personnel may collect, retain, and disseminate intelligence or information where they have a reasonable belief that viewing the intelligence or information would further one or more national or departmental missions.

In July 2020, DHS received a considerable amount of attention alleging I&A lacked respect for civil rights and civil liberties after it compiled reports on American journalists covering protests in Portland, Oregon. This created a “perception problem” for I&A, according to one former senior official, because I&A should not “be collecting and disseminating intelligence products on U.S. journalists” as part of its mission to protect the Nation. I&A withdrew these reports, issued to DHS and its partners, later in July 2020. This prompted I&A’s Intelligence Enterprise Standards Division to conduct an internal review of the OSINT process and an internal audit of its OSIRs in the second half of 2020. See Appendix D for more information on this review and audit.

We conducted this audit from January to August of 2021 to determine the extent to which I&A has an effective process for collecting, managing, and protecting OSINT for operational and intelligence purposes.

Results of Audit

I&A is improving its process for collecting, managing, and protecting OSINT for operations and intelligence. We acknowledge I&A’s recent efforts to address known challenges related to insufficient guidance and technology, but additional process improvements are needed to ensure intelligence reporting is effective. Additionally, stakeholder feedback indicated further improvements are needed to issue OSIRs in a timely manner.

We attributed these challenges to insufficient policies and procedures to guide staff in their daily work, inadequate internal controls and training to promote adherence to standards and requirements, and reliance on an outdated and

¹⁰ Executive Order 12333, *United States Intelligence Activities*, 46 Federal Register (FR) 59941, Dec. 4, 1981.

¹¹ For I&A’s purposes, a U.S. person is a U.S. citizen, a legal permanent resident, an unincorporated association made up primarily of citizens or legal permanent residents, or a corporation legally incorporated in the United States, except for corporations controlled by foreign governments. U.S. persons’ information receives additional privacy protections.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

unreliable information technology system to create and disseminate reports. During our fieldwork, I&A began to resolve some of these challenges by drafting new policies, revising training, and upgrading its technology.

To accomplish its core mission of identifying and mitigating threats to the Nation, I&A must produce intelligence reports that are relevant, timely, and in line with evolving threats. The deficiencies identified by I&A and confirmed through this audit hinder I&A's ability to effectively inform decision makers about potential threats.

I&A Has Taken Steps to Correct Known Deficiencies in Its Open Source Intelligence Process

I&A recently took steps to improve key aspects of its intelligence collection and reporting process. Specifically, in response to a preliminary inquiry by I&A's Intelligence Oversight Officer, I&A conducted an internal review and an audit in 2020 and determined that intelligence reporting, dissemination, production, policies, and training needed improvement.¹² The Intelligence Enterprise Standards Division identified several challenges in the review. I&A made the most notable progress in addressing two of the five deficiencies identified in the review:

- Lack of an overarching collection policy framework, which could result in increased risk of noncompliance, nonstandard processes and practices, and unclear roles and responsibilities.
- Lack of cohesive collection operation and requirement management in I&A, which could result in duplication of efforts and uncoordinated collection.

In a separate 2020 audit, the Collection Management Division of the Intelligence Enterprise Standards Division found several errors in OSIRs related to collection requirements. We concurred with I&A's identification of these deficiencies, and during our audit, we observed and noted I&A's efforts to address them.

Creation of an Overarching Collection Policy Framework

Based on the 2020 review, I&A concluded it had no overarching collection policy framework, without which there was an increased risk of noncompliance with policies, nonstandard processes and practices, and unclear roles and responsibilities. We noted this challenge during our audit — OSCO personnel

¹² During this audit, we did not have sufficient data to analyze specific causes for delays in OSIR production. For more information on I&A's internal audit and review, see Appendix D.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

were not well-equipped to ensure their OSIRs complied with applicable privacy protections and intelligence guidance.

In April 2017, the DHS Privacy Office issued the *Privacy Policy Guidance Memorandum*¹³ on collecting, using, retaining, and disseminating personally identifiable information. This guidance requires DHS employees to comply with applicable laws and guidance¹⁴ to ensure privacy protections for all people, regardless of immigration status, whose personally identifiable information is collected, used, retained, or disseminated by DHS.

Even after their initial training, collectors we spoke with were not certain whether, in their day-to-day operations, they adhered to privacy protections and protected speech. Also, some collectors could not easily determine whether the information in their OSIRs met the threshold for reportable intelligence.¹⁵ Other I&A staff stated they needed guidance on what personally identifiable information should be reported for statements that are likely hyperbolic and thus not reportable.¹⁶

Additionally, collections staff were uncertain about open source products containing U.S. persons' information. The Undersecretary for Intelligence and Analysis approved a DHS-wide instruction that was issued on February 24, 2020, implementing an Intelligence Community-wide mandate establishing the responsibilities, procedures, and standards for responding to requests for the identities of U.S. persons in disseminated intelligence reports.¹⁷ In May 2020, I&A's Intelligence Oversight Officer asked the Associate General Counsel for Intelligence for more guidance on a recently revised directive, but handling U.S. persons' information remained a source of confusion and concern for collections staff as recently as June 2021.

¹³ Memorandum Number 2017-01, April 25, 2017.

¹⁴ The 2017 memorandum refers to more than 15 pieces of applicable guidance, law, and policy. These include the Fair Information Practice Principles, the U.S. Constitution, the *Privacy Act of 1974*, the *Federal Records Act of 1950*, and the *Homeland Security Act*, among others.

¹⁵ According to the Open Source Collection Operations Cookbook, to meet the threshold for reportable intelligence, information in OSIRs must (1) be associated with an authorized intelligence mission and adhere to privacy, civil rights, and civil liberties protections; (2) meet a valid collection requirement; (3) be generally unavailable through the mainstream media; and (4) be of interest or value to DHS or one of its partners.

¹⁶ According to I&A's Intelligence Oversight Guidelines, U.S. persons' information is not reportable unless there is a reasonable belief that reporting the information would assist in fulfilling a lawful intelligence, counterterrorism, law enforcement, or other homeland security related function.

¹⁷ *Requests for Identities of U.S. Persons in Disseminated Intelligence Reports*. Instruction Number 264-01-010.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Although our audit did not reveal evidence of privacy violations, we concurred with the 2020 review that additional guidance was needed to prevent future violations. In March 2021, I&A began issuing additional guidance and policies to help collectors better consider privacy protection by informing all I&A personnel of available resources. According to the procedures, while collecting OSINT and drafting, reviewing, and disseminating OSIRs, all I&A staff may directly seek and receive advice from the Collection Management Division and relevant oversight offices.

Further, to address the need for an overarching collection policy framework, I&A established a central approach to its policy development in May 2021.¹⁸ This new guidance emphasizes the need for comprehensive policies and procedures, as well as a robust policy framework that can translate priorities and requirements into clear, understandable guidance and standards. As part of its new approach to policy development, in June 2021, I&A published guidelines¹⁹ to help OSCO determine the appropriate audience and scope of dissemination for OSIRs.

Finally, I&A's Privacy and Intelligence Oversight Branch sought to provide additional assistance with privacy and intelligence matters. Although a small office with seven staff members,²⁰ the branch assigned an intelligence officer to CETC in May 2021. The intelligence officer is a dedicated resource for OSCO staff when they need more guidance, such as answers to questions about collection and dissemination.

Improvements to Collection Operation and Requirement Management

In its 2020 review, the Intelligence Enterprise Standards Division concluded that collection staff gathered intelligence and published reports on a wide variety of topics instead of gaining subject matter expertise by focusing on one intelligence area and its associated collection requirements. I&A's Collection Management Division updates active intelligence collection requirements regularly based on changing intelligence needs. For example, around the presidential election in November 2020, there were 43 active collection requirements and 17 recently retired requirements. By June 2021, the number of active requirements had decreased to 36 due to the Intelligence Community's changing needs. Tracking fluctuations in intelligence requirements is more difficult when a collector works across all areas rather than focusing on one subject matter at a time.

¹⁸ *Roles, Responsibilities, and Procedures for Developing and Managing Policy as the Office of Intelligence and Analysis*, May 2021.

¹⁹ *Dissemination Guidelines for Intelligence Enterprise Operations*.

²⁰ By March 2021, the Privacy and Intelligence Oversight Branch onboarded a total of four new assistant intelligence oversight officers. The office had seven staff as of August 2021.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In a 2020 audit, the Collection Management Division found many errors in OSIRs related to collection requirements. Specifically, of 348 OSIRs published between May 24 and September 2, 2020, the division identified 103 assigned to the wrong collection requirements, missing essential elements of information,²¹ or having other administrative errors. The division also found that another 11 OSIRs were not aligned with any active collection requirement.

We agreed that collectors need additional guidance to prevent future collection requirement errors. This position was also supported by I&A's internal audit, as the Collection Management Division found that 23 of the audited OSIRs had intelligence oversight violations²² or fell below the threshold for reporting. However, in September 2020, an I&A official issued a memo focusing on the violations identified by the Collection Management Division's independent audit and concluded that the division's findings were incorrect and that only 1 of the 23 OSIRs in question had not met the reporting threshold. The I&A official explained that "the citing of requirements is subjective and requires the insight of the collector at the time of collection and therefore further review is not warranted as threshold for reporting and oversight requirements were met."

To address the identified challenges with collection requirements, I&A sought to better organize intelligence collection activities. In June 2021, I&A restructured its open source collection operations workforce into five subject-matter-based work groups, as shown in Figure 2. Previously collectors were not aligned to a specific subject matter. The new work groups are meant to align with and provide dedicated collection support to I&A's mission centers. I&A anticipates this restructuring would result in a better-defined subject matter area of concentration for each group, enabling them to focus on one area at a time. I&A expects the realignment to improve collector expertise in specific subject areas, improve the staff's ability to know what information to prioritize, and prevent collectors from producing duplicate work on the same event or the same social media posts.

²¹ An essential element of information is a refined, specific aspect of an intelligence problem or gap that can be collected by one or more intelligence disciplines because it is both observable and reportable. Essential elements of information, like collection requirements, are required for every OSIR, as they allow the collector to collect intelligence on topics vital to the homeland security mission.

²² Intelligence oversight violations include missing necessary markings when a U.S. person's information is used and not being in line with the essential elements of information selected for the report.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 2. Open Source Collection Operation's Restructured Work Groups*



Source: DHS OIG-created based on information from I&A

* OSCO also supports CETC's WATCH operations, which provide emerging threat indications and warnings that allow DHS leadership to gauge and mitigate threats. A small number of collectors are assigned to WATCH support.

Intelligence Reporting Timeliness Was Not Tracked

Executive Order 12333 states that timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and people is essential to the national security of the United States.²³ OSIRs are an essential element of I&A's mission to equip the Department with the intelligence and information it needs to keep the Nation safe. A security threat related OSIR's value is largely based on the timeliness of its delivery to stakeholders before a potential threat escalates. For example, issuing an OSIR after a planned protest may serve little to no purpose, although it may assist in long-term intelligence missions. However, as of August 2021, I&A faced challenges ensuring OSIRs were issued in a timely manner. I&A also does not record enough OSIR milestone data to track timeliness.

Aside from stating that OSIRs should be timely, OSCO has not defined how long it should take to complete an OSIR (from the date information is collected to the date of report creation). OSCO also does not track or document the

²³ Executive Order 12333, *United States Intelligence Activities*, 46 FR 59941, Dec. 4, 1981.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

length of time it takes to complete the end-to-end OSINT process. Instead, OSCO tracks the last date OSINT was collected for a specific OSIR and when the OSIR was first created.

We determined that two factors affected the timeliness and efficiency of OSIRs: the length of time between gathering OSINT and creating reports and the length of time between creating reports and reviewing them prior to publication.

First, we reviewed timeline information for 694 OSIRs created between October 1, 2020, and August 13, 2021. We determined the average time from collection of OSINT to creation of a report was over 2 weeks. In addition, we noted:

- For almost 50 percent of the OSIRs we reviewed, collectors had intelligence for a week or more before they created a report.
- For 10 percent of the OSIRs we reviewed, 30 days or more passed between when the intelligence was collected and a report was created.
- The reports that took more than 2 weeks included threats to Government, public safety, and first responder facilities; and white supremacists discussing “trophy” obtained during civil unrest.

Second, we reviewed timeline information for 62 OSIRs awaiting dissemination review as of August 12, 2021. We determined that 27 (44 percent) had been created before June 2021, more than 2 months prior. These reports included information on potential threats to critical infrastructure, the sharing of guides to make explosives, the sale of confidential Government documents, and threats to state and Federal Government leaders.²⁴

Intelligence report stakeholders also emphasized a decrease in OSIR timeliness. To determine timeliness, OSCO sends out and receives information from stakeholder surveys. According to these surveys, OSCO’s timeliness rating steadily declined between FY 2019 and FY 2021. Specifically, I&A stakeholders’ responses indicated report timeliness declined by almost 40 percent from FY 2019 (when stakeholders said almost 80 percent were timely) to FY 2021 (when stakeholders said only 42 percent were timely).

The process for issuing OSIRs was time-consuming in part due to the need to enter data manually. To store the information needed to create an OSIR, staff manually entered much of the data into HOST (I&A’s prior system for compiling OSIR data)²⁵ from separate information technology (IT) systems. This was because HOST did not have prepopulated dropdown lists with the mandatory

²⁴ Data provided by I&A did not indicate whether these reports were time sensitive and needed immediate release.

²⁵ I&A transitioned to a new system after the conclusion of our fieldwork in September 2021.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

information needed, such as the intelligence collection requirements and the associated elements of information. Collectors explained that collection requirements were maintained on an Excel spreadsheet outside HOST, and they would enter each manually into their OSIRs in HOST. These steps increase the risk of mistakes when copying over the nine-digit requirement. In an internal summer 2020 review, I&A noted OSIRs incorrectly tagged to a requirement or essential elements of information, and during an August 2021 demonstration of the process, we observed a mistyped requirement. Additionally, HOST's formatting contained errors that had to be manually deleted in each report.

Creating and disseminating OSIRs was also a time-consuming task for I&A personnel because they must use various IT systems, such as MS Outlook, MS Word, Adobe, shared network drives, and HOST to consolidate information in reports. The unclassified dissemination process was so complex that one OSCO supervisor created a six-page step-by-step guide for unclassified dissemination.²⁶ The guide notes challenges such as regular restarts and includes troubleshooting instructions. An OSCO supervisor estimated it could take 40–60 minutes to disseminate a single report; however, during our observation it took over 90 minutes to disseminate one report.

Lastly, according to I&A, intelligence reports are sometimes deleted if they become outdated, such as when supervisory dissemination review is delayed, and a report is deemed no longer relevant. In such cases, a collector may submit a report for publishing only for it to remain in a queue for weeks or months awaiting review. Then, according to OSCO leadership, when a report is deemed “overcome by events” the supervisor will ask the collector to delete the delayed report from the record. Because I&A does not maintain records of the number of reports created and deleted, we could not determine how often this occurs.

Multiple Factors Hinder Intelligence Reporting Process

We attribute the delays in OSINT collection and production, as well as untimely OSIR dissemination, to I&A having non-comprehensive policies and procedures, inadequate internal controls, training deficiencies, and an outdated and unreliable in-house IT system for creating and disseminating OSIRs. As mentioned earlier in the report, I&A began addressing some of these areas during this audit.

²⁶ OSCO also disseminates classified OSIRs across several other systems. The classified dissemination process and related systems are not covered in this report.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Policies and Procedures Are Not Adequate to Carry Out Day-to-Day Functions

I&A does not have comprehensive policies and procedures to ensure its employees effectively collect OSINT and adhere to privacy protections. I&A developed and released interim guidance in March 2021²⁷ to help carry out day-to-day activities, but OSCO staff told us they were often not aware of the guidance. OSCO staff also said they relied on their initial training course and a reference guide covered during that training. The reference guide is known as the *Open Source Collection Operations Cookbook* (Cookbook). The Cookbook covers information such as the IT systems collectors use, classification of information, and elements of OSIRs.

However, the Cookbook is not an official policy and specifically states it is not intended to replace established policies, directives, instructions, or other official documents. Although the Cookbook provides guidance to help ensure OSIRs meet reporting thresholds, such as by including intelligence that meets a valid collection requirement and information generally not available in mainstream media, it does not discuss how to differentiate between a true threat that meets a collection requirement and political hyperbole. For example, staff said they struggle with determining whether a statement is hyperbole or reportable as an actual threat.²⁸

In the first quarter of FY 2021, I&A initiated the Collection Enhancement Project, which aims to expand instructions and standard operating procedures for collection management. Due to limited staffing, however, I&A said it could not move forward with this initiative until the summer of FY 2021. In August 2021, to make up for its limited staff, I&A brought in additional resources to support policy development and coordination by scoping, researching, developing, facilitating, reviewing, coordinating, and disseminating new and revised policies. Based on projected timelines and the audit team's communication with I&A leadership, I&A's efforts are projected to continue into FY 2022.

²⁷ *Standard Operating Procedures for Collecting, Reviewing, and Disseminating Open Source Intelligence Reports*, March 2021.

²⁸ IA-1000, *Office of Intelligence and Analysis Intelligence Oversight Programs and Guidelines*, does not permit I&A personnel to 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. The use of these characteristics, in combination with other information, is permitted where such use (1) is intended and reasonably believed to support one or more of the national or departmental missions and (2) is narrowly focused in support of that mission (or those missions).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Intelligence Reporting Process Did Not Have Consistent Internal Controls

The OSINT process lacked sufficient internal controls for effective oversight. According to the Government Accountability Office's *Standards for Internal Controls in the Federal Government*, internal controls help Government organizations comply with applicable laws and regulations. Part of maintaining sufficient internal controls is monitoring for and resolving deficiencies. An internal control deficiency occurs when an organization cannot achieve its objectives and address related risks. In OSCO's case, internal controls should help the organization ensure it releases intelligence reports that adhere to privacy and intelligence guidance.

We determined that OSCO does not have a structured oversight process for supervisory review of OSIRs before dissemination. Supervisory review provides oversight and reduces risk of violating privacy and intelligence guidance. However, increases in supervisory workload and limited supervisory staff in OSCO make in-depth supervisory reviews rare or nonexistent. Instead, collectors rely on peer reviews and self-made checklists to review their own reports. In an August 2020 internal review, I&A's Privacy and Intelligence Oversight Branch stated that high employee turnover in OSCO led to inexperienced collectors peer reviewing OSIRs. High turnover continued in OSCO throughout our audit, with more than 30 percent of positions vacant as of August 2021.

Although I&A has several oversight bodies that review and help control risks for other types of intelligence, I&A does not have detailed guidance for OSIR reviews. For example, collectors who peer review OSIRs said they do not receive any guidance to help identify issues. In addition, OSCO supervisors told us they often do not receive sufficient training in their personnel and management responsibilities. One supervisor said they had no time to complete required annual training. According to a member of CETC leadership, CETC is failing OSCO's supervisors by not training them adequately.

I&A also does not require formal intelligence oversight and legal reviews of OSIRs before they are disseminated. In the past, raw intelligence, including OSIRs, received a formal pre-dissemination review, but the volume of raw intelligence made the requirement for this pre-dissemination review unmanageable. Instead, collectors and reviewers rely on their best judgment when deciding whether to involve I&A's oversight offices in reviews of raw intelligence.²⁹ In May 2021, I&A tried to add more oversight of raw intelligence

²⁹ By contrast, I&A has detailed guidance for finished intelligence products: *Procedures for Finished Intelligence Product Review During Exigent Circumstances*, July 2020. Finished intelligence is to contain 10 specific elements, which are subject to oversight.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

by encouraging collectors to seek prepublication guidance for OSIRs and increasing collection staff's access to an intelligence officer, as previously mentioned. However, prepublication review is not required, leaving OSCO subject to noncompliance with important guidance such as privacy protection guidelines.

We also determined that frequent leadership transitions and acting leaders made it less likely for staff working on OSINT to get consistent guidance. For instance, in addition to turnover in collections staff, CETC experienced high turnover in its leadership in 2020 and 2021, with its current director being the fourth person in that role in just 1 year. In addition, OSCO's branch chief departed in August 2021, leaving OSCO with an acting branch chief. Some employees were concerned that the lack of permanent leadership affected day-to-day operations, including oversight.

OSINT Training Does Not Ensure Adherence to Privacy Requirements and Intelligence Standards

In its internal 2020 review, the Intelligence Enterprise Standards Division noted deficiencies in training. Specifically, the division documented concerns that an incomplete collections training curriculum could result in deficient collections-related skills. We concurred with this assessment and determined that the training provided did not help staff improve their skills and adhere to privacy requirements and intelligence standards.

Training offered to open source collections staff was primarily limited to a 3-day course on basic open source fundamentals. Before July 2021, staff also attended an "OSCO Bootcamp" run by CETC. The bootcamp presented several topics, such as CETC's broad responsibilities, specific roles and responsibilities of open source collectors, the OSCO Cookbook, IT systems, the intelligence cycle, and the relationship between collectors and other I&A staff. However, the bootcamp was not standardized or certified, the training varied depending on the teacher, and it was not certified by the Intelligence Training Academy. Further, a 2021 internal I&A survey showed that nearly half of the collectors believed training was inadequate and did not meet their needs. From junior collectors new to the Intelligence Community to members of OSCO management, employees rely on on-the-job training to fill gaps left by inadequate formal training.

I&A's Intelligence Training Academy has been working to improve training for OSCO staff. After the 2020 internal review by the Intelligence Enterprise Standards Division, the academy took over the OSCO bootcamp to formalize, standardize, and provide accreditation for OSINT training. In July 2021, the academy launched its first session of the new, standardized bootcamp, with



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

four collectors attending. CETC intends to require all collectors to attend the updated bootcamp.

I&A's IT System for Creating and Disseminating OSIRs Was Inefficient

I&A's IT system for creating and disseminating OSIRs, HOST, did not support the efficient generation and dissemination of OSIRs. Staff reported issues such as pervasive system slowness, system crashes, and broken links that required them to maintain needed information on their own. The system's problems were evident during our observations. For example, we saw system latency and crashing during an August 2021 demonstration of HOST.

HOST was built by a CETC staff member in 2017 to help automate the reporting process. Although the system was created only 4 years ago, Microsoft no longer supports the application on which HOST was built. After the staff member who created HOST left OSCO in March 2020, other employees could not fix problems that arose with the system. For example, outdated macros³⁰ created prepopulated fields that were no longer relevant, requiring staff to correct each OSIR manually before it could be disseminated.

As part of our audit, we conducted a technology security review to ensure proper security authorizations were in place for the systems used for collecting, managing, and protecting OSINT. We determined that I&A obtained the appropriate authorization for HOST to operate within DHS in September 2018.³¹

As mentioned previously, in September 2021, OSCO shifted OSIR creation and dissemination from HOST to a new system, the Better Open Source System. This system was designed to allow collectors to create OSIRs more easily and content managers to disseminate them in fewer steps. The Better Open Source System also received the appropriate authorization to operate within DHS in April 2020.³² However, at the time of this audit, OSCO staff did not yet know whether the new system would improve the process for creating and disseminating OSIRs.

³⁰ A macro is a short rule or command that is created in a system to automate a repetitive action or actions.

³¹ Authorization to operate, also known as Authority to Operate, is a formal security authorization declaration that adequate security controls have been implemented in the IT system and that the system has a satisfactory level of security. HOST is covered by the Microsoft Office Software as a Service Authority to Operate.

³² Better Open Source System was approved for use by I&A's Chief Information Officer with an April 2020 Authorization to Operate memorandum. The Better Open Source System is covered by the Dynamics Online as a Service Authority to Operate.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Conclusion

I&A's core mission is to share intelligence and analysis to identify and mitigate threats to the Nation. To be effective, intelligence reports must be relevant, timely, and in line with evolving threats. The deficiencies identified by I&A and confirmed through this audit hinder I&A's ability to effectively inform decision makers about potential threats. Primarily, OSCO staff continue to be challenged to ensure timely completion and dissemination of intelligence reports. For example, as we noted in a recent report,³³ OSCO did not release a single OSIR related to the January 6, 2021 insurrection at the U.S. Capitol until 2 days later, on January 8.

In addition, the inadequate policies, procedures, and OSIR review that we identified could lead to manipulation or politicization of the OSINT process.³⁴ This potential was illustrated in the summer of 2020, when the intent and appropriateness of I&A's coverage of U.S. journalists in three OSIRs was called into question. The absence of standardized training on Intelligence Oversight Guidelines and privacy protection may impede efficiency and increase the risk of violating regulations.

Establishing and improving key internal controls — formal policies and procedures, adequate oversight and review, comprehensive training, and an efficient IT system for creating and disseminating OSIRs — will strengthen I&A's ability to provide objective and timely intelligence and achieve its mission to protect the Nation from potential threats.

Recommendations

Recommendation 1: We recommend the Deputy Under Secretary for Intelligence Enterprise Operations 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.

Recommendation 2: We recommend the Deputy Under Secretary for Intelligence Enterprise Operations establish a standard process to determine whether additional oversight or review is needed for open source intelligence reports before their dissemination.

Recommendation 3: We recommend the Deputy Under Secretary for Intelligence Enterprise Readiness develop and implement initial and ongoing,

³³ *I&A Identified Threats Prior to January 6, 2021, but Did Not Issue Any Intelligence Products before the U.S. Capitol Breach* (Redacted), OIG-22-29, March 4, 2022.

³⁴ DHS OIG also recently reported on process challenges with finished intelligence reports in OIG-22-41.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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.

Recommendation 4: We recommend the Deputy Under Secretary for Intelligence Enterprise Readiness implement the IT system improvements needed to promote efficiency and enhance Open Source Collection Operations' ability to produce and disseminate OSIRs.

Management Comments and OIG Analysis

We provided DHS with a draft of this report on April 15, 2022, for its review and response. I&A responded with complete technical comments on May 19, 2022. I&A formally responded to our draft report on June 3, 2022.

I&A concurred with all four recommendations and officials stated they had made progress addressing each of the report recommendations since the completion of our fieldwork. A summary of I&A's responses and our own analysis follows. We have included a copy of the comments in their entirety in Appendix B.

I&A's Comments to Recommendation 1: Concur. Officials stated that I&A published interim guidance for CETC and OSCO (*Interim Policy Guidance: Standard Operating Procedures for Collection, Reporting and Dissemination of Open Source Intelligence Reports*) in February 2021. This guidance established the current process steps to ensure quality OSIRs are produced and disseminated. I&A is in the process of finalizing guidance based on the interim policy.

OIG's Analysis: We acknowledge I&A's interim guidance for OSIRs. We believe I&A's plan to publish a final standard operating procedure based on the interim policy guidance is a positive step toward fulfilling the intent of this recommendation. We look forward to reviewing the procedure when it is finalized and implemented. We consider this recommendation open and resolved.

I&A's Comments to Recommendation 2: Concur. Officials stated that I&A's interim guidance (referenced in Recommendation 1) established the current process by which collectors can identify and raise issues requiring additional review. The interim guidance also permits leadership to pre-determine whether certain issues or circumstances warrant additional review prior to dissemination. In situations where operational or policy requirements warrant additional or more stringent review, such as during national election periods, I&A senior leadership may impose changes to the standard process. These changes are communicated in writing to the workforce including details such



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

as: additional steps required, content thresholds necessitating additional review, and a sunset date for process modifications.

Additionally, I&A's existing policies (such as the *Office of Intelligence and Analysis, Intelligence Oversight Process and Guidelines*) provide an effective foundation for oversight and expresses the need for intelligence officers at all levels to exercise sound, independent judgement in matters of oversight and policy application. I&A officials request that OIG consider this recommendation resolved and closed, as implemented.

OIG's Analysis: We agree that the interim policy guidance helps to establish a standard process for determining whether OSIRs need additional oversight or review before their dissemination. However, the interim nature of the policy does not represent or provide evidence of a finalized and implemented process, nor does it guarantee long-term standardization. Therefore, we will consider this recommendation open and resolved until I&A formalizes a final policy and communicates and implements it across the workforce.

I&A's Comments to Recommendation 3: Concur. Officials stated that, beginning in January 2021, I&A took numerous steps to enhance training, competency, and managerial oversight of the OSINT program to ensure that standardized training adheres to all oversight parameters set forth in I&A's Intelligence Oversight Guidelines. Specifically, the Intelligence Training Academy conducted multiple reviews of the various types of training content provided to open source personnel. These reviews also included meetings with Intelligence Community partners to align with tradecraft best practices. The Intelligence Training Academy also coordinated with internal stakeholders prior to developing curriculum updates that should deliver the most up-to-date principles for an OSINT practitioner. As of December 2021, all OSCO personnel have taken the updated training and as of April 2022, all certified release authorities and content managers have received content release authority training. The Intelligence Training Academy has continual courses scheduled through the rest of 2022 and can adjust their content and training timing based on OSINT program needs. I&A officials request that OIG consider this recommendation resolved and closed, as implemented.

OIG's Analysis: We commend the steps I&A has taken to enhance the training and oversight of the OSINT program to align with its Intelligence Oversight Guidelines. We also recognize that I&A has assigned OSCO officers to work directly under OSINT content manager supervision. Given that I&A has scheduled future sessions of its training courses as well as refresher trainings, we consider this recommendation closed and resolved.

I&A's Comments to Recommendation 4: Concur. Officials stated that, in August 2021, I&A deployed the Better Open Source System to modernize its



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

processing of OSIRs. Implementation of the new system improved efficiency, effectiveness, and tracking of OSINT report production. I&A continues to make improvements to the Better Open Source System and considers the implementation of the system, as well as the improvements to efficiencies, sufficient to address the nature of the recommendation. I&A officials request that OIG consider this recommendation resolved and closed, as implemented.

OIG's Analysis: We recognize I&A's improvements in efficiency and ease of work following the implementation of the Better Open Source System. We also observed a system demonstration and reviewed user feedback gathered following this audit. Given that the new system does increase automation and usability for collections staff and content managers, we consider this recommendation closed and resolved.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine the extent to which I&A has an effective process for collecting, managing, and protecting OSINT for operational and intelligence purposes. To accomplish our objective, we did the following:

- We identified and reviewed pertinent I&A training material, policies and procedures, and internal memorandums, including:
 - *Interim Guidance: Standard Operating Procedures for Collecting, Reviewing, and Disseminating Open Source Intelligence Reports*
 - *Dissemination Guidelines for Open Source Intelligence Reports*
 - *Roles, Responsibilities, and Procedures for Developing and Managing Policy at the Office of Intelligence and Analysis*
 - *Improving Raw Intelligence Functions within the Office of Intelligence and Analysis*
- We obtained more than 450 documents, congressional testimony, raw data, and news articles on I&A's intelligence collection, management, and protection.
- We reviewed published Government Accountability Office and DHS OIG reports to identify prior findings and recommendations.

We used this information to establish a data collection approach consisting of interviews with relevant stakeholders, focused information gathering, documentation analysis, and site visits.

In addition, we worked directly with I&A personnel and its stakeholders:

- We held more than 30 meetings.
- We participated in teleconferences with DHS' Privacy Office; I&A's Privacy Intelligence Oversight Branch and Strategy, Plans, and Policy Branch; CETC; MITRE Corporation; Intelligence Enterprise Standards; and I&A's Chief Information Office, Intelligence Training Academy, and Collection Management Division.
- We met with OSCO senior desk officers and intelligence collection specialists.
- We visited I&A personnel in Washington, DC, in August 2021 to observe IT systems and processes used for OSIR creation and dissemination.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We used the work of IT specialists from the OIG Office of Innovation's Cybersecurity Risk Assessment Division to test the security posture of OSINT information systems. IT specialists reviewed security authorization documentation to assess systems and application architecture. IT specialists also reviewed IT security policies and procedures required by *DHS Sensitive Systems Policy Directive 4300A*, for DHS unclassified sensitive systems, and *DHS National Security Systems Policy Directive 4300B*, for DHS national security systems that collect, generate, or process unclassified, confidential, secret, top secret, and special access program national security information.

We conducted this performance audit between January and August 2021 pursuant to the *Inspector General Act of 1978, as amended*, and according to 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

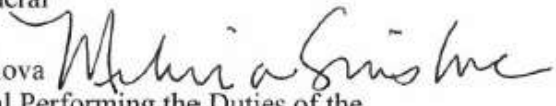
Appendix B
I&A Comments to the Draft Report



**Homeland
Security**

June 3, 2022

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Melissa Smislova 
Senior Official Performing the Duties of the
Under Secretary for Intelligence and Analysis

SUBJECT: Management Response to Draft Report: "The Office of
Intelligence and Analysis Needs to Improve Its Open Source
Intelligence Reporting Process"
(Project No. 21-002-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) Office of Intelligence and Analysis (I&A) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

I&A is pleased to note OIG's recognition that I&A took steps to address previous challenges in its intelligence collection and reporting process, including creation of an overarching collection policy framework and improvements to collection operations and requirements management. In a meeting on May 11, 2022, OIG also acknowledged that I&A accurately assessed challenges and has taken action to improve its Open Source Intelligence (OSINT) program. To that end, I&A completed a number of key improvements to the OSINT mission over the last 18 months—some of which occurred since OIG ended its fieldwork—that have a bearing on the audit's findings, including:

- Updating OSINT training curriculum and ensuring 100 percent of open source personnel were trained by the end of 2021;
- Hiring a full-time expert OSINT instructor to develop and teach courses;
- Developing and deploying a new information technology (IT) system for OSINT reports that has reduced the collection-to-publication time by 43 percent;
- Embedding a dedicated Assistant Intelligence Oversight Officer within the Open Source Collection Operations (OSCO) Branch to advise on privacy and intelligence oversight matters;



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Issuing additional legal and oversight guidance for collectors and revising dated policy guidance on open source collection and dissemination;
- Hiring three experienced leaders to manage the I&A Current and Emerging Threats Center (CETC) and OSCO; and
- Responding to dynamic collection requirements responsive to I&A's National and Departmental missions, as outlined in I&A's Intelligence Oversight Guidelines¹, and annually producing an average of 1,100 Open Source Intelligence Reports (OSIRs) between fiscal years 2018 and 2021.

However, I&A believes that this draft report lacks sufficient context regarding the timeliness of publishing OSIRs, as it is important to recognize that factors other than efficiency, such as the completeness, complexity, or quality of information, also determine how fast an OSIR can, or should, be published. I&A's objective is to publish reporting that meets quality and tradecraft standards, while retaining its intelligence value. Accordingly, the time from collection to publication is not always the primary factor for OSIR publication, and to consider it so would be inconsistent with intelligence tradecraft. In some cases, for example, OSCO managers prioritize and quickly publish a report because it is time-sensitive and/or responds to exigent operational circumstances. In other cases, OSIRs fill gaps by contributing to strategic or operational analysis and are not perishable within a short window. Consequently, imposing a fixed time standard on these reports would constrain I&A's ability to prioritize urgent, perishable reporting by issuing less urgent reports according to a more deliberate timeline determined by the senior collection officer, as appropriate.

The draft report contained four recommendations, with which I&A concurs. Enclosed, please find our detailed response to each recommendation. I&A previously submitted technical comments addressing accuracy, contextual, sensitivity and other issues under a separate cover for OIG'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.

Enclosure

¹ <https://www.dhs.gov/publication/office-intelligence-and-analysis-intelligence-oversight-program-and-guidelines>.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Enclosure: Management Response to Recommendations Contained in 21-002-AUD-DHS

The OIG recommended that the Deputy Under Secretary for Intelligence Enterprise Operations (DUSIEO):

Recommendation 1: 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.

Response: Concur. The DUSIEO published guidance for the CETC and OSCO, "Interim Policy Guidance: Standard Operating Procedures for Collection, Reporting and Dissemination of Open Source Intelligence Reports" (Interim Policy Guidance), dated February 18, 2021. This guidance established the current process for ensuring steps are in place, at the correct level, to ensure quality OSIRs are produced and disseminated. I&A's Intelligence Enterprise Operations is in the final stages of promulgating a final Standard Operating Procedure (SOP) based on I&A's interim guidance. Estimated Completion Date: September 30, 2022.

Recommendation 2: Establish a standard process to determine whether additional oversight or review is needed for open source intelligence reports before their dissemination.

Response: Concur. The DUSIEO's Interim Policy Guidance establishes the current process by which OSINT collectors can identify and raise issues requiring additional review. The Interim Policy Guidance also permits leadership to pre-determine whether certain issues or circumstances warrant additional review prior to dissemination. OSCO collectors may also elevate questions or concerns to: (1) Desk Officers or Supervisory Desk Officers in OSCO; (2) the embedded Assistant Intelligence Oversight Officer who sits with OSCO; or (3) oversight offices (including DHS' Offices for Privacy, Civil Rights and Civil Liberties, and General Counsel) for further review prior to dissemination. In situations where operational or policy requirements warrant additional or more stringent oversight review, such as during national election periods, I&A senior leadership, including the Under Secretary for Intelligence and Analysis, the DUSIEO, or the CETC Director, may impose changes to the standard process. Such deviations are communicated in writing to the workforce, and include specific details such as the additional steps required, content thresholds necessitating additional review, and a sunset date for any process modifications.

I&A's existing policies, including IA-1000, "Office of Intelligence and Analysis, Intelligence Oversight Program and Guidelines," dated January 19, 2017, continue to provide an effective foundation for oversight, and articulate the need for intelligence



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

officers at all levels to exercise sound, independent judgement in matters of oversight and policy application. Consequently, the most effective approach to ensuring legal, intelligence oversight, privacy, civil rights, and civil liberties policies and protections are applied in a high-volume process, like open source reporting, is to ensure effective training, access to oversight advisors, and clear policies and procedures.

I&A requests OIG consider this recommendation resolved and closed, as implemented.

The OIG recommended that the Deputy Under Secretary for Intelligence Enterprise Readiness:

Recommendation 3: 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.

Response: Concur. Beginning in January 2021, I&A took numerous steps to enhance the training, competency, and managerial oversight of the OSINT program to ensure that standardized training adheres to all oversight parameters set forth in I&A's Intelligence Oversight Guidelines, including the protection of privacy, civil rights, and civil liberties, prepares the practitioner to succeed. Specifically, in January 2021, the Acting Under Secretary for I&A requested that the DHS Intelligence Training Academy (ITA) conduct a review of its current OSINT training to more effectively support OSCO personnel. By March 2021, ITA conducted a comprehensive review of its OSINT training, which included outreach to Intelligence Community (IC) agencies with open source programs, as well as the Open Source Working Group that reports to the IC's Open Source Governance Board, to seek best practices for OSINT training. In the spring of 2021, ITA reviewed classified OSINT tradecraft material (e.g. standards, policies, training curriculum, etc.) provided by IC agencies and modified its OSINT course curriculum to align with IC OSINT tradecraft best practices, as appropriate. In addition to consultation with IC partners, I&A also coordinated the development of its open source training with I&A's Collection Management Division and Privacy and Intelligence Oversight Branch. It was also reviewed by the Office of General Counsel-Intelligence Law Division and the DHS Office of Civil Rights and Civil Liberties.

In September 2021, curriculum updates were completed to deliver the most up-to-date principles for an OSINT practitioner. The current OSINT training program includes: (1) a three-day "OSINT Course" featuring tradecraft, best practices, and tools; and (2) a two-week "Open Source Intelligence Report Workshop"² that details the collection and exploitation of open source information and development of OSIRs. Both courses

² In February 2021, ITA took control of the OSCO "Bootcamp" training to add rigor and formalize the training curriculum consistent with ITA's standards. This course was renamed "OSIR Workshop," the first of which was held in July 2021 with four more iterations through December 2021.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

include intelligence oversight, privacy, and legal principles, taught by the respective experts from those functional areas. All I&A personnel assigned to open source collection duties within OSCO are required to complete this OSINT training program.

Beyond classroom training, new OSCO officers are assigned under the direct supervision of OSINT Content Managers after completing these courses to facilitate the practical application of learning objectives addressed in the training courses, as well as to ensure a comprehensive understanding of collection requirements and the generation of reports. Further, senior OSCO officers responsible for releasing OSIRs are required to attend raw intelligence release authority training via the OSIR Certified Release Authority (CRA) course. These senior OSCO officers then participate in an on-the-job training period before receiving OSIR release authority certification from OSCO management.

As of December 2021, 100 percent of OSCO personnel received the updated training outlined above. In addition, as of April 2022, 100 percent of certified release authorities and content managers have received the CRA training. For the remainder of calendar year 2022, ITA will deliver 14 OSINT Courses and 2 OSIR Workshops, and will schedule an OSIR CRA when needed. This training schedule ensures ample training capacity for new hires, and ITA will adjust timing and offerings to meet adjustments in the OSINT program capacity.

I&A requests OIG consider this recommendation resolved and closed, as implemented.

Recommendation 4: Implement the IT system improvements needed to promote efficiency and enhance Open Source Collection Operations' ability to produce and disseminate OSIRs.

Response: Concur. In August 2021, the I&A Chief Information Officer worked with the CETC to deploy the Better Open Source System (BOSS), which modernized I&A's processing of OSIR by transitioning from the previous tool known as Homeland Open Source Tool (HOST). HOST consisted of shared drives and a database that was difficult to access and made processing large volumes of data a challenge, to include historical records dating back to 2009.

However, implementation of BOSS improved the efficiency, effectiveness, and tracking of OSINT report production, compared to the prior HOST system. For example, a review of the processing time for all OSIRs produced via BOSS from August 2021 through December 2021 (n=198), showed a 17 day average time from collection to publication of the report, which is a 43 percent reduction from 30 days under HOST. When examining the subset of reports focused on domestic terrorism, OSCO was able to use BOSS to produce reports on average in nine days from collection to publication.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Although I&A will continue to leverage and make enhancements to the BOSS system as needed, I&A considers implementation of BOSS, as well as the improvements and efficiencies to producing and disseminating OSIRs, sufficiently addresses the intent of this recommendation.

I&A requests OIG consider this recommendation resolved and closed, as implemented.



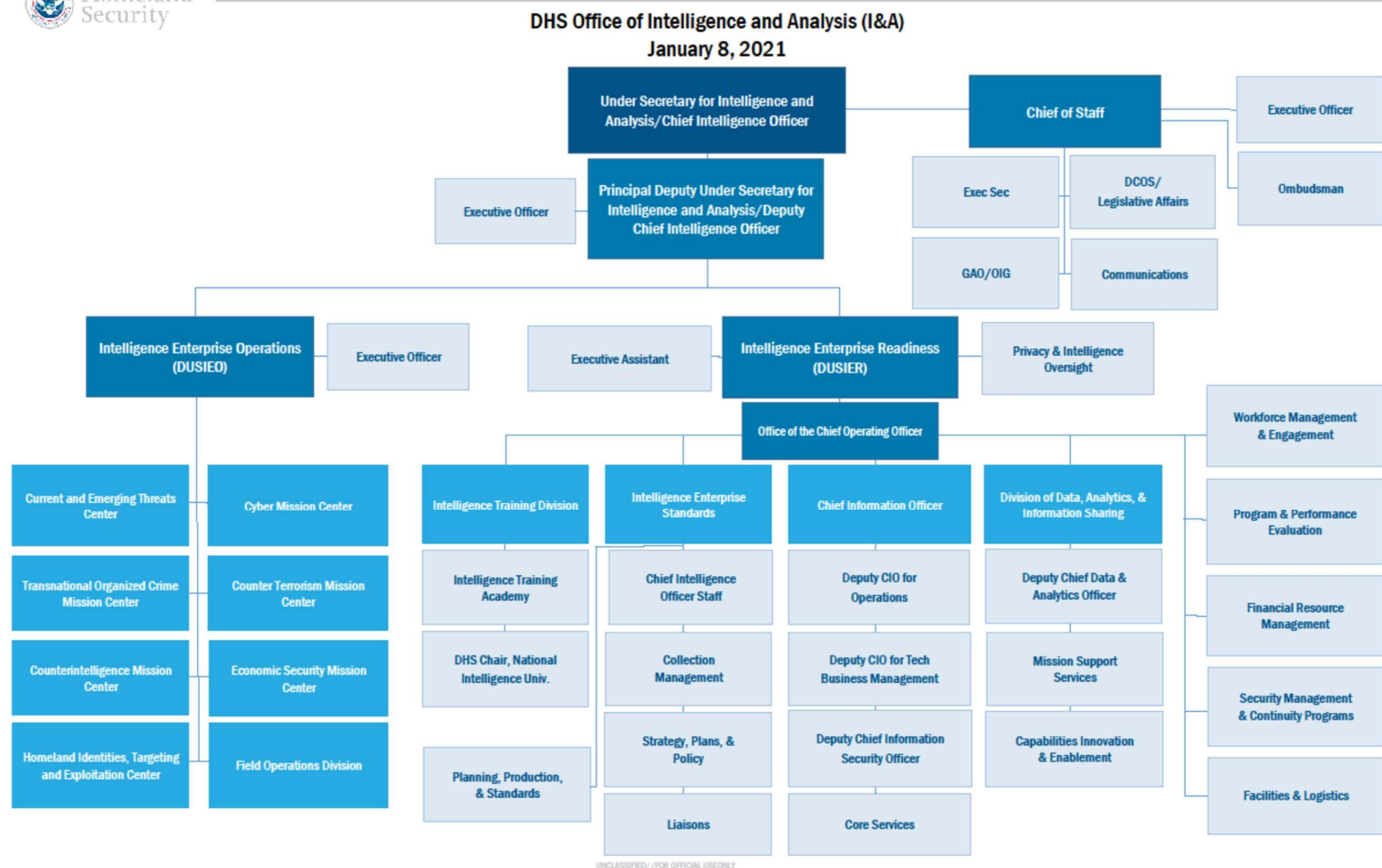
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix C: I&A Organizational Structure



Homeland
Security



Source: OIG-generated based on I&A documentation



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix D

Summary of I&A's 2020 Internal Reviews

Intelligence Enterprise Standards Division Review

In response to a preliminary inquiry by I&A's Intelligence Oversight Officer, in the late summer of 2020, the Intelligence Enterprise Standards Division completed a review of the collection and reporting environments, including processes, policies, audits, operations, and dissemination. In its review, the division found I&A needed to improve raw intelligence reporting, dissemination, production, policy, and training. In response, I&A developed an action plan, the Collection Enhancement Project, to mitigate risks and close the following five key gaps, the first two of which are discussed on pages 4 through 8 of our report:

1. Lack of an overarching collection policy framework results in increased risk of noncompliance, unstandardized processes and practices, and unclear roles and responsibilities.
2. Lack of cohesive collection operation and requirement management within I&A results in duplication of efforts and uncoordinated collection.
3. An incomplete collections training curriculum in I&A and the DHS Intelligence Enterprise presents risks such as unmet collection needs and deficient collection-related skills.
4. Inconsistent oversight processes for raw intelligence production do not provide assurance for identifying compliance issues or providing feedback to improve deficiencies.
5. Reporting systems are not all in the same IT framework, which hinders operation and maintenance and oversight and auditing functions.

Collection Management Division Audit of OSIRs

As noted on pages 6 and 7 of our report, in a September 2020 audit of OSIRs, the Collection Management Division found errors in 114 of 348 OSIRs reviewed. Eleven of those errors were significant and did not align with any active collection requirement. The errors in the remaining 103 OSIRs were deemed administrative misalignment of the collection requirement.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix E

Office of Audits Major Contributors to This Report

Craig Adelman, Director
Anna Hamlin, Audit Manager
Corinn King, Auditor in Charge
Saajan Paul, Program Analyst
Telogia Moore, Auditor
Jessica Garcia, Program Analyst
Ashley Wilson, Program Analyst
Jason Dominguez, Information Technology Specialist
Gaven Ehrlich, Senior Data Analyst
Scott Schwemin, Program Analyst
Susan Parrott, Communications Analyst
Darrel Francis, Independent Referencer



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix F

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
I&A Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at:
www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General
Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.



OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305