U.S. DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL

OIG-24-55 September 17, 2024

FINAL REPORT

# I&A Needs to Improve Its Security Inspection Program to Reduce the Risk of Unauthorized Access to Classified Information

# OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

*Washington, DC 20528 | www.oig.dhs.gov*


September 17, 2024

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

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.09.17 19:23:10 -04'00'

SUBJECT: *I&A Needs to Improve Its Security Inspection Program to Reduce the Risk of Unauthorized Access to Classified Information*

Attached for your action is our final report, *I&A Needs to Improve Its Security Inspection Program to Reduce the Risk of Unauthorized Access to Classified Information*. We incorporated the formal comments provided by your office.

The report contains two recommendations aimed at improving I&A's oversight of its security inspection program. Your office concurred with both recommendations. Based on information provided in your response to the draft report, we consider recommendation 1 open and unresolved. As prescribed by Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for the recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendation will be considered open and unresolved.

We consider recommendation 2 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

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 contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

# DHS OIG HIGHLIGHTS

## I&A Needs to Improve Its Security Inspection Program to Reduce the Risk of Unauthorized Access to Classified Information

**September 17, 2024**

## Why We Did This Audit

I&A specializes in sharing intelligence and analysis internally and externally to help state and local partners identify and mitigate threats to the homeland. To fulfill its mission, I&A regularly handles information that may require protection because its release or disclosure could cause damage to the Nation's security. As such, I&A must establish ways to ensure it protects this information. We conducted this audit to determine the extent to which I&A ensures protection of classified information and equipment from unauthorized access.

## What We Recommend

We made two recommendations to improve I&A's oversight of its security inspection program.

**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 Department of Homeland Security's Office of Intelligence and Analysis (I&A) has a security inspection program and conducts annual security inspections of its offices to ensure the organization complies with security requirements and safeguards classified information and equipment. However, aspects of I&A's security inspection program, such as scheduling inspections and ensuring that offices took corrective actions for identified deficiencies, have weaknesses. Specifically, from fiscal year 2020 through FY 2023, I&A did not meet its security inspection schedules; reduced the number of security inspections it conducted; and did not use a documented, risk-based approach to select the offices to inspect. Further, I&A did not maintain documentation on whether its offices implemented corrective actions after security inspections.

These conditions occurred because I&A did not allocate resources to support continued operation of its security inspection program. Additionally, I&A did not ensure its security procedure included a methodology for selecting the highest risk offices and a formal, documented process for following up with the offices it inspected.

Without adequate resources and procedures to implement the security inspection program, I&A cannot ensure that all its offices consistently adhere to security requirements, which may lead to a greater risk of unauthorized access to classified information and impact I&A's ability to meet its mission.

## I&A Response

I&A concurred with both recommendations. Appendix B contains I&A's management response in its entirety.

## Background

The Department of Homeland Security's Office of Intelligence and Analysis (I&A) is responsible for using information and intelligence from various sources to identify and assess current and future threats to the United States. I&A provides intelligence to its customers, including DHS components, the Intelligence Community, and state and local partners. The Under Secretary for I&A also serves as DHS' chief intelligence officer and is responsible to both the Secretary of Homeland Security and the Director of National Intelligence.

One of I&A's responsibilities is to obtain and disseminate intelligence.[1] Intelligence can provide insights not available elsewhere that warn of potential threats. Because the release or disclosure of intelligence could cause damage to national security, this information is often classified and available to only individuals who are appropriately vetted and have a "need-to-know."

I&A is a support component within DHS and is led by the Under Secretary for I&A.[2] Within the component, 14 offices, broken down further into sub-offices,[3] report to four Deputy Under Secretaries. Three additional offices report directly to the Under Secretary for I&A. I&A personnel are primarily located in the Washington, DC, area; personnel working outside of Washington, DC, are co-located with state and local partners in various locations. See Appendix C for I&A's organizational chart.

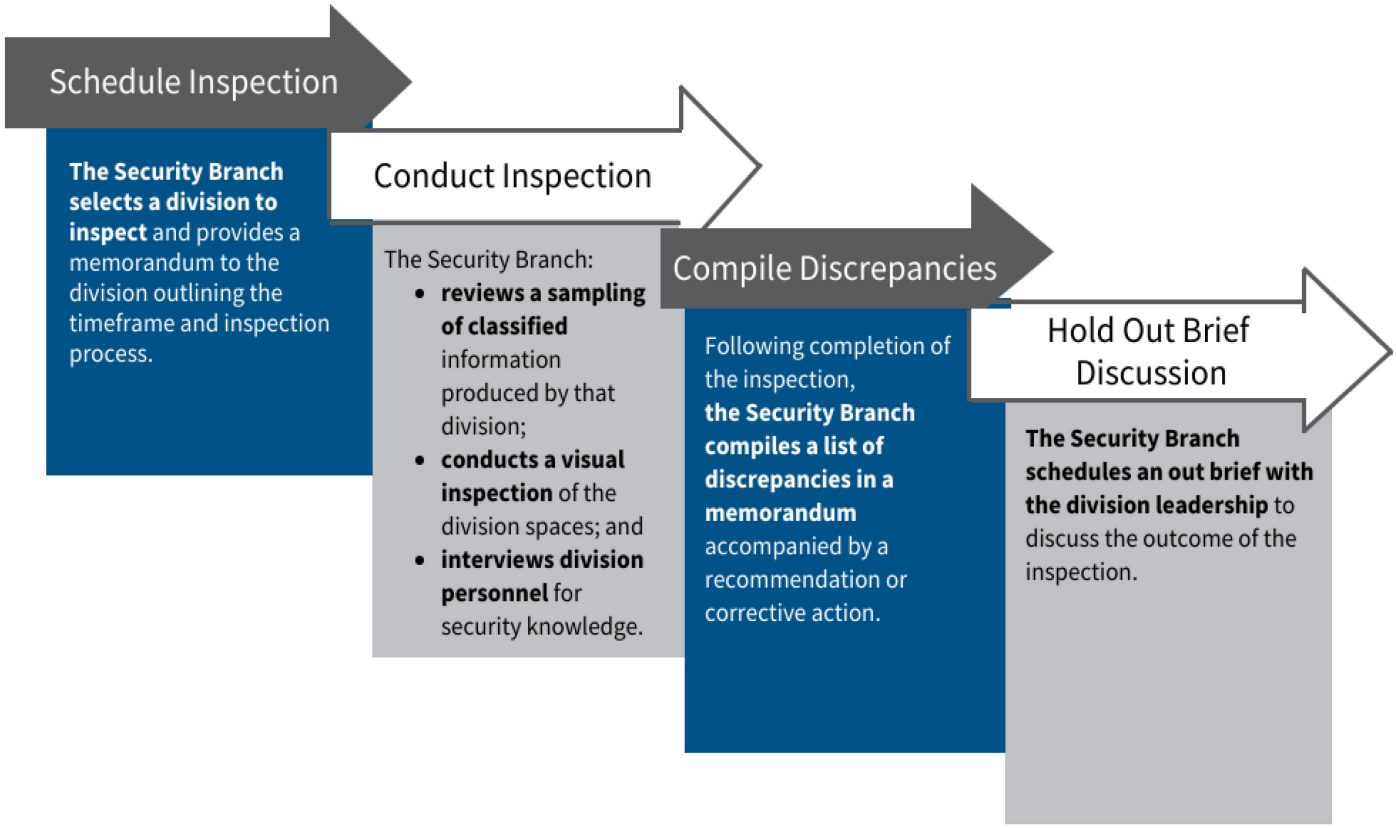
I&A's Security Management Branch (Security Branch), within the Mission Assurance Division under the I&A Chief of Staff, is responsible for all program security requirements, including protecting I&A's classified information. Among other actions, the Security Branch is responsible for managing administrative safeguards, physical access safeguards, and recurring security training programs. As of September 2023, the Security Branch was composed of a Branch Chief and 10 supporting staff. The Security Branch Chief is responsible for limiting access to classified information to those who are eligible and have a need-to-know. The Branch Chief also coordinates the security program that continuously evaluates individuals' eligibility to access classified information or be assigned to sensitive duties.

As part of its responsibilities, the Security Branch conducts a self-inspection (security inspection) program to ensure I&A offices adhere to policies and have security practices in place to protect classified information. The Security Branch maintains a standard operating procedure (security

[1] Intelligence is defined as information that involves threats to the Nation; development, proliferation, or use of weapons of mass destruction; and any other matter affecting homeland security. Source: *The Importance of Private Sector Intelligence Programs*, 2021, found at: https://www.dhs.gov/sites/default/files/publications/importance_to_private_sector_intelligence_programs.pdf.
[2] I&A realigned its organization in May 2023, which separated the intelligence mission functions of collection and analysis, and consolidated collection activities under a new Deputy Under Secretary.
[3] I&A sub-offices include centers, divisions, and program offices.

procedure) to conduct its security inspection program. Figure 1 shows the security inspection process.

**Figure 1. Security Branch's Security Inspection Process**




Source: DHS Office of Inspector General analysis of I&A security inspection process

The Security Branch Chief is ultimately responsible to the Under Secretary for I&A and the Chief of Staff for all security program requirements. The Security Branch provides the Chief of Staff with a final security inspection report that summarizes security inspection findings, including any deficiencies related to classification markings, physical security of classified equipment, and mandatory security training.

We performed this audit to determine the extent to which I&A ensures protection of classified information and equipment from unauthorized access.

## Results of Audit

### I&A Has a Security Inspection Program but Did Not Meet Its Inspection Schedules or Maintain Necessary Documentation

I&A has a security inspection program to ensure the organization safeguards classified information and equipment. However, aspects of I&A's security inspection program, such as scheduling inspections and ensuring that offices took corrective actions for identified deficiencies, have weaknesses. Specifically, I&A did not meet its inspection schedules, use a documented risk-based approach for selecting offices, or maintain documentation of corrective actions offices implemented after security inspections.

#### I&A Has a Security Inspection Program

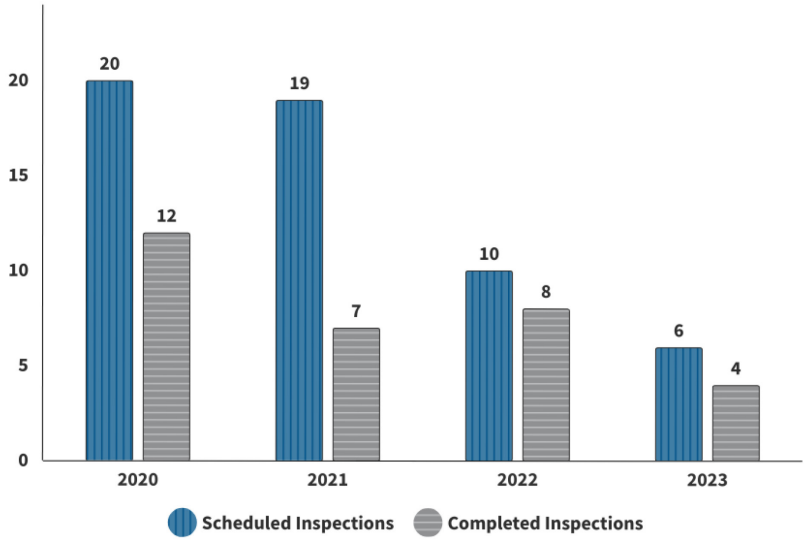
Executive Order 12968, *Access to Classified Information*, as amended on August 2, 1995, requires agencies that grant access to classified information to designate an official to direct and administer the agency's personnel security program, to include conducting annual inspections of the agency's implementation of the order. Additionally, Executive Order 13526, *Classified National Security Information*, December 29, 2009, requires agencies that handle classified information to establish and maintain an ongoing security inspection program. I&A's security inspection program includes personnel interviews, classified document reviews, and security walkthroughs.

From fiscal years 2020 through 2023, the Security Branch conducted 31 inspections and summarized its results, including recommendations to address deficiencies found, in memorandums submitted to I&A leadership. The security inspections concentrated on various topics related to whether personnel adhere to security standards. Specifically, the inspections covered issues such as missing portion markings on documents, classified information left unattended at printers and scanners, and personnel missing required security-related trainings.

#### I&A Did Not Complete All Scheduled Security Inspections and Reduced the Number of Inspections It Conducted

Although it conducted 31 inspections from FY 2020 to FY 2023, I&A had planned to conduct 55 inspections. To execute the security inspection program, the Security Branch created annual inspection schedules, which included selected offices with estimated inspection dates. The Security Branch planned to conduct 20 inspections in FY 2020, 19 inspections in FY 2021, 10 inspections in FY 2022, and 6 inspections in FY 2023. As Figure 2 shows, the Security Branch did not complete all the scheduled inspections. For example, it conducted only 7 (or 37 percent) of 19 scheduled inspections in FY 2021.

Figure 2. I&A Scheduled Security Inspections vs. Completed Security Inspections from FY 2020 through FY 2023




Source: DHS OIG analysis of I&A security inspection schedules and reports

The decline in scheduled and completed security inspections occurred because I&A leadership did not provide the Security Branch with resources to support continued operation of its security inspection program. In January 2020, I&A leadership decided to not fully renew the contract for personnel support to assist with Security Branch responsibilities. The contract previously provided staff for physical security support, which included assisting with security inspections; administrative security support, which included documenting security incidents; and information security support, which included ensuring procedures for transmission of classified material comply with agency-wide policy standards. In FY 2020, the Security Branch consisted of 13 personnel: 7 Government employees and 6 support contractors. At the beginning of FY 2023, the Security Branch consisted of 8 Government employees, representing a total staffing decline of 38 percent.

### I&A Did Not Use a Risk-Based Approach to Schedule Security Inspections

Apart from not completing all scheduled inspections, I&A did not use a documented, risk-based approach to select offices for security inspections. Per the U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government,*[4] "management should identify risks when creating and implementing processes to achieve its objectives." Risk

[4] GAO-14-704G, *Standards for Internal Control in the Federal Government*, September 2014, Principle 7 – Identify, Analyze and Respond to Risks.

identification methods may include identifying deficiencies from prior security inspections or trends in security deficiencies.

I&A personnel confirmed they did not have a formalized documented process for selecting offices for annual security inspections. Instead of using a formalized methodology, I&A personnel explained they relied on personal experience to select offices from the organization chart and schedule security inspections.

**The Security Branch Did Not Maintain Documentation for Implementation of Corrective Actions after Security Inspections**

Although the Security Branch identified 175 deficiencies from 31 inspections conducted from FY 2020 to FY 2023, the Security Branch could not provide documentation to show whether I&A offices took corrective actions. Per GAO's *Standards for Internal Control in the Federal Government,*[5] "management should complete and document corrective actions to remediate internal control deficiencies." Examples of deficiencies in the inspection reports included:

- employees interviewed were unable to identify the process for conducting a formal and informal classification challenge;
- employees interviewed were unable to identify the required markings found on a derivatively classified document;
- computers were left open or unattended; and
- emails/documents reviewed lacked some or all the required "portion markings" in accordance with Title 32 of the Code of Federal Regulations, dated June 28, 2010, section 2001.23, paragraph (b).

The recommended corrective actions to remedy the deficiencies included mandatory security refresher training for unauthorized disclosure, operations security, and derivative classification.

According to an I&A official, inspected program offices took action to implement corrective actions. However, the Security Branch did not collect and maintain documentation to confirm program offices took these corrective actions. Additionally, an official said the Security Branch would previously follow up 60 days after it performed an inspection to verify that corrective actions had been taken. Yet the branch stopped conducting follow-up activities when I&A reduced its staffing levels.

[5] GAO-14-704G, *Standards for Internal Control in the Federal Government*, September 2014, Principle 17 – Evaluate Issues and Remediate Deficiencies.

**I&A's Security Procedure Did Not Include Elements to Guide the Security Inspection Program**

The Security Branch did not use a risk-based approach when scheduling its inspections and did not maintain documentation of implemented corrective actions because I&A's Security Standard Operating Procedure[6] did not require these actions. I&A's security procedure did not include guidance for selecting or prioritizing offices to inspect based on risk factors when resources do not allow the Security Branch to inspect all I&A offices. For example, the security procedure did not include risk-based selection criteria, such as prioritizing offices that handle the most classified information, or material that will have the most significant impact to national security if an unauthorized user obtains it.

Additionally, the security procedure did not include a formalized process for the Security Branch to follow up with I&A offices to ensure they implemented corrective actions. The security procedure requires the Security Branch to compile a list of deficiencies identified during the security inspection, make recommendations to the inspected office to correct identified deficiencies, and provide a memorandum to the inspected office informing them of any identified issues. But the security procedure did not include a follow-up process to assess whether the inspected office implemented the recommended corrective actions.

## Conclusion

I&A designed its security inspection program to ensure security practices are in place to protect classified information. We found the Security Branch did not conduct all security inspections it scheduled to determine whether I&A offices properly handled classified information and equipment. As a result, I&A cannot ensure all its offices consistently adhere to security requirements, which may lead to a greater risk of unauthorized access to classified information and equipment. I&A has a responsibility to protect the information it receives from the intelligence community and disseminates to its state and local partners. If I&A did not prioritize security of classified information, it could jeopardize the integrity of its intelligence community partnerships, which could, in turn, hinder I&A from fulfilling its mission.

## Recommendations

**Recommendation 1:** We recommend the I&A Deputy Under Secretary for Management develop and implement a resource strategic plan to ensure the Security Branch is staffed to adequately schedule and conduct security inspections of its offices that handle classified information.

**Recommendation 2:** We recommend the I&A Deputy Under Secretary for Management update the Security Standard Operating Procedure to require the following:

[6] *DHS Intelligence & Analysis Standard Operating Procedures: Security Management Branch*, September 2015.

- a risk-based methodology for selecting offices to inspect annually; and
- a process to confirm inspected offices implemented corrective actions and recommendations.

## Management Comments and OIG Analysis

I&A provided management comments in response to a draft of this report. We included the comments in their entirety in Appendix B. We also received technical comments and revised the report as appropriate. A summary of I&A's response to each recommendation and our analysis follows.

**I&A Response to Recommendation 1:** Concur. I&A's Security Branch developed a risk-based strategic plan that it will implement during the FY 2025 annual security compliance self-inspections. The strategic plan incorporates three priorities that focus on classification marking, security incidents, and safeguarding classified information. I&A will incorporate this into the security procedure.

I&A will prioritize mission centers, divisions, or branches that create, handle, or disseminate classified information based on factors such as the amount of classified production, the number of security incidents, and results of previous FY inspections. At the beginning of each FY, the I&A annual self-inspection schedule will be provided to the Security Branch Chief and the Mission Assurance Division Director for review and approval. Estimated Completion Date: September 30, 2025.

**OIG Analysis of I&A Response:** These actions are partially responsive to the recommendation. Although I&A is developing a strategic plan, it did not address how it will adequately staff the Security Branch to conduct the security inspections. We consider this recommendation open and unresolved until I&A provides additional information on how its planned staffing will meet its security inspection needs.

**I&A Response to Recommendation 2:** Concur. The I&A Security Branch will update security procedure to outline the security compliance review corrective action process. Specifically, the security procedure will require mission centers, divisions, or branches that receive a significant number of discrepancies to undergo an automatic 60-, 90-, or 120-day follow up re-inspection to ensure that all corrective actions are completed. The procedure will also outline three categories to determine the priority order for follow-up inspections. Estimated Completion Date: September 30, 2025.

**OIG Analysis of I&A Response:** These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when I&A provides documentation that it updated and issued its updated security procedure.

## Appendix A:
## Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

The objective of this audit was to determine the extent to which I&A ensures protection of classified information and equipment from unauthorized access.

To achieve our objective, we reviewed Federal, Department, and I&A policies and procedures related to safeguarding classified information from unauthorized access. We also reviewed prior audits and reports pertaining to the audit objective.

We conducted a site visit to I&A headquarters in Washington, DC. We also interviewed DHS and I&A personnel from the following offices to understand their role in safeguarding I&A's classified information:

- DHS Office of the Chief Security Officer
  - National Security Services Division
  - Compliance, Standards and Training Division
- I&A Chief of Staff
  - Transparency and Oversight Division
  - Intelligence Enterprise Program Office
  - Mission Assurance Division, Security Management Branch
- Office of the Deputy Under Secretary for Analysis
  - Analytic Advancement Division
  - Counterterrorism Center
  - Cyber Intelligence Center
  - Nation-State Threat Center
  - Transborder Security Center
- Office of the Deputy Under Secretary for Collection
  - Collection Management Division
  - Homeland Identities, Targeting, and Exploitation Center
  - Open-Source Intelligence Division
- Office of the Deputy Under Secretary for Partnerships
  - Engagement, Liaison, and Outreach Division
  - Intelligence Watch and Coordination Center
  - Field Intelligence Directorate
- Office of the Deputy Under Secretary for Management
  - Directorate of Technology and Data Services

- Intelligence Training Academy

To assess whether I&A had a formalized methodology for selecting offices for annual security inspections, we analyzed the Security Branch inspection schedules from FY 2020 through FY 2023. We include our analysis and conclusions in the body of the report.

To assess whether the Security Branch adhered to the security inspection schedules, we analyzed inspection reports from FY 2020 through FY 2023 to determine which I&A offices the Security Branch inspected each year. We assessed the degree to which I&A leadership oversaw its security inspection program. We evaluated the Security Branch's inspection reports and found them to be sufficiently reliable to support our findings, conclusions, and recommendations in the report. The COVID-19 pandemic occurred during the scope of our audit. However, we did not find a correlation between the pandemic's effect on in-office I&A staff and the decline in inspections the Security Branch conducted during the pandemic.

We assessed I&A's internal controls related to our audit objective. We limited our review to specific internal control components and underlying principles that were significant to I&A's controls over classified information and equipment. Specifically, we assessed the frequency of I&A's security inspections to monitor compliance and the completeness of guidance pertaining to the security inspection program. We discussed weaknesses we identified in the body of this report. Because we limited our review to I&A's administrative controls, our assessments may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

We conducted this audit from November 2023 through June 2024 pursuant to the *Inspector General Act of 1978*, 5 United States Code §§ 401–424, 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## DHS OIG's Access to DHS Information

During this audit, I&A provided timely responses to DHS OIG's requests for information and did not delay or deny access to information we requested.

## Appendix B:
## I&A Comments on the Draft Report

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

Homeland Security

BY ELECTRONIC SUBMISSION

August 19, 2024

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

FROM: Kevin Saupp
Acting Chief of Staff and
Senior Component Accountable Official
Office of Intelligence and Analysis

Kevin Saupp, 08/19/24
KEVIN M SAUPP
Digitally signed by KEVIN M SAUPP
Date: 2024.08.20 09:54:40 -04'00'

SUBJECT: Management Response to Draft Report: "I&A Needs to Improve Its Security Inspection Program to Reduce the Risk of Unauthorized Access to Classified Information" (Project No. 24-006-AUD-I&A)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security 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 leadership is pleased to note the OIG's recognition that I&A conducts annual security inspections to ensure the organization complies with security requirements, and safeguards classified information and equipment. I&A remains committed to ensuring that classified information is protected from unauthorized disclosures.
The draft report contained two recommendations with which I&A concurs. Enclosed find our detailed response to each recommendation. I&A previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration, as appropriate.

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

**Enclosure: Management Response to Recommendations Contained in OIG 24-006-AUD-I&A**

OIG recommended that the I&A Deputy Under Secretary for Management:

**Recommendation 1:** Develop and implement a resource strategic plan to ensure the Security Branch is staffed to adequately schedule and conduct security inspections of its offices that handle classified information.

**Response:** Concur. To strategically manage resources for security inspections, the I&A Security Management Branch developed a comprehensive, risk-based strategic plan that will be implemented in the fiscal year (FY) 2025 annual Security Compliance Self-Inspections. This approach has a methodology with three priorities that focus on the areas of classification marking, security incidents, and safeguarding classified information, and will be incorporated into the "Security Management Branch Standard Operating Procedure" (Security Management SOP), dated September 2015.

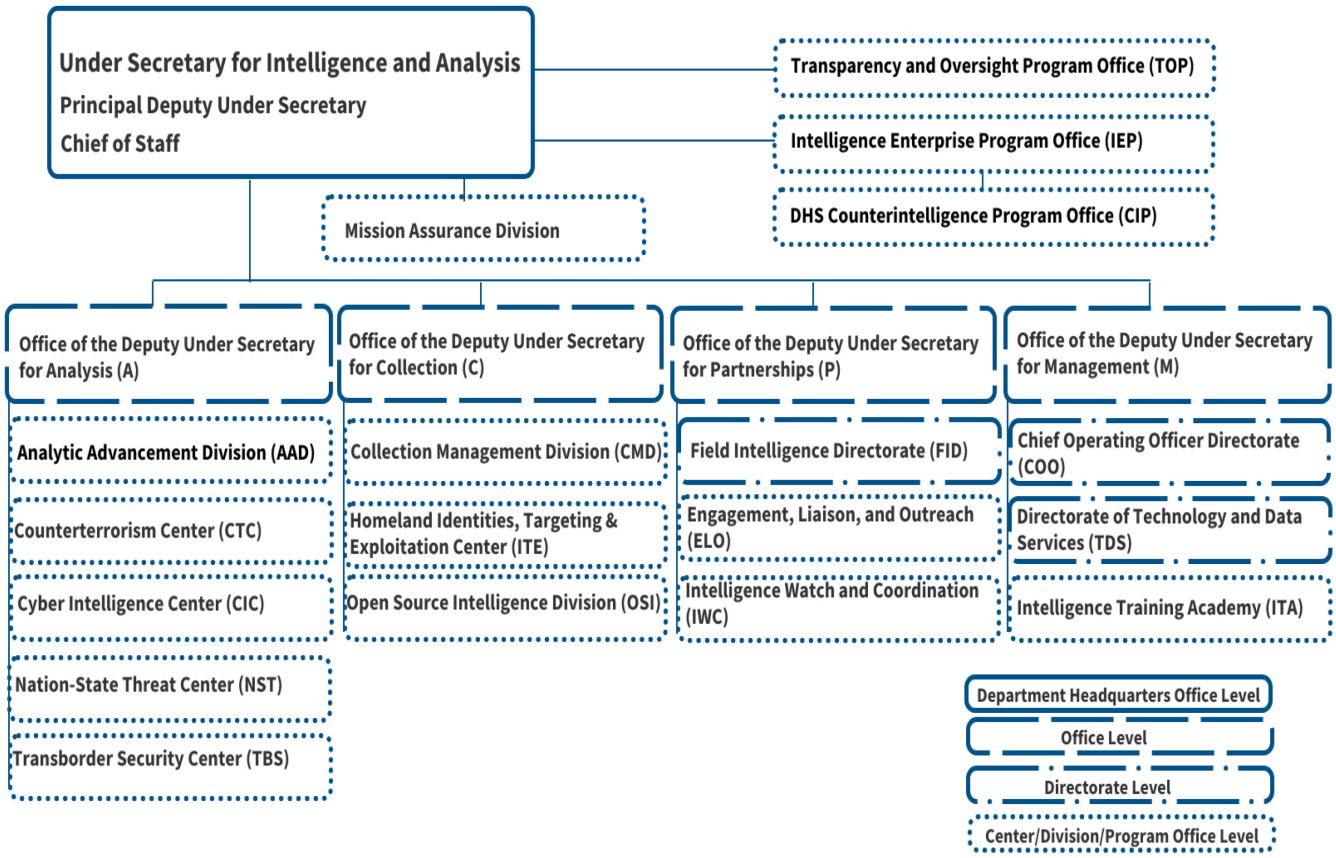
Accordingly, Mission Centers, Divisions, or Branches in I&A that create, handle, or disseminate classified information will be prioritized based on factors such as the amount of classified production, the number of security incidents, and results of previous FY inspections. At the beginning of each FY, the I&A annual self-inspection schedule will be provided to the Security Management Branch Chief and the Mission Assurance Division Director for review and approval. Estimated Completion Date (ECD): September 30, 2025.

**Recommendation 2:** Update the Security Standard Operating Procedure to require the following:

- a risk-based methodology for selecting offices to inspect annually; and
- a process to confirm inspected offices implemented corrective actions and recommendations.

**Response:** Concur. The I&A, Security Management Branch will update the Security Management SOP to outline the security compliance review corrective action process. Specifically, the Security Management SOP will require Mission Centers, Divisions, or Branches that receive a significant number of discrepancies to undergo an automatic 60, 90, or 120-day follow up re-inspection to ensure that all corrective actions are completed. The SOP will also outline three categories to determine the priority order for follow-up inspections. ECD: September 30, 2025.

## Appendix C:
## I&A Organizational Chart as of May 2023




Source: DHS OIG–created I&A organizational chart as of May 2023

## Appendix D:
## 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
DHS Component Liaison
I&A Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees

## Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

## DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

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