INTEGRITY ★ FORTITUDE ★ EXCELLENCE

THE OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

Semiannual Report

1 OCTOBER 2025 - 31 MARCH 2026

UNCLASSIFIED REPORT

Report Availability

The Office of the Inspector General of the Intelligence Community shares reports, news releases, and information about ongoing work on its website at www.DNI.gov/ICIG.

Contents

Message from the Inspector General

I am honored to present this unclassified version of our Semiannual Report on behalf of the Intelligence Community Office of the Inspector General (IC OIG). Congress established IC OIG in 2010 to strengthen whistleblower protections, promote accountability and effectiveness, and combat fraud, waste, abuse, and misconduct. As Inspector General, I am responsible for ensuring independent oversight of programs and activities within the authority and responsibility of the Director of National Intelligence (DNI) across the Intelligence Community (IC).

This reporting period reflects a focused effort to modernize IC OIG for greater impact and enhanced agility under the "IC OIG 2.0" organizational update. We consolidated our six divisions into four integrated offices to increase investigative capacity, expand proactive work, and reduce stovepipes. We also updated our mission, vision, and values. These changes have already delivered results across all mission areas.

The Office of Audits and Inspections issued five reports with 30 recommendations to strengthen financial accountability, mission readiness, and continuity capabilities. The Office of Investigations and Intake reviewed hundreds of suspicious activity reports, conducted eight preliminary reviews, supported five joint investigations, and completed 11 investigations. The Office of Strategy and Support (OSS) delivered substantial annual savings by relocating IC OIG from a single leased commercial space to five smaller offices across ODNI facilities, improving accessibility for whistleblowers and enhancing our community presence. OSS also established the Excellence Review Team to strengthen quality across all deliverables. The Office of Legal Counsel completed 86 legal reviews and realigned the External Review Panel program for more timely adjudication.

IC OIG also remained highly responsive to the workforce. The IC IG Hotline handled 1,177 new contacts, including 318 complaints and seven "urgent concern" submissions. IC OIG worked closely with the DNI and Congress to address critical gaps, including the need for criminal investigative authority and enhanced coordination within the IC Inspectors General Forum. IC OIG also took steps to improve IC-wide handling of unauthorized disclosures, information sharing, and investigative integrity.

Looking ahead, IC OIG is positioned to deliver even greater outcomes. I extend my sincere appreciation to our workforce, our partner Inspectors General, Director Gabbard, President Trump, and the Congress for their support of our unique oversight mission. It is my privilege to serve, and I remain committed to consequential oversight that strengthens national security and earns the trust of the American people.

CHRISTOPHER R. FOX

Inspector General of the
Intelligence Community

Highlights

9 Interagency Projects

IC OIG Recommendations

30	New Recommendations
23	Closed Recommendations
84	Open Recommendations

Open Investigations

25	Unilateral Investigations
5	Joint Investigations

Partner Agencies for Joint Investigations

IC IG HOTLINE

1,177	318	134
New Contacts	Complaints Opened	Referrals to IC OIG Partners

Key IC OIG Activities

1. Restructured IC OIG to streamline operations from six divisions into four integrated offices.
2. Initiated a comprehensive, government-wide evaluation of intelligence oversight capabilities of non-IC Federal departments and agencies and select IC elements.
3. Advanced legislative efforts with Congress to obtain critical law enforcement authorities.
4. Facilitated the provision of IC badges for 41 partner agency personnel to strengthen joint oversight operations.
5. Consulted with key stakeholders to develop a thematic work plan enabling more responsive oversight aligned with national security priorities and fraud prevention efforts.

About This Report

Submission to the DNI and Other Agency Heads

Pursuant to 50 U.S.C. § 3033(k)(1)(A), the Intelligence Community Inspector General (IC IG) shall submit to the DNI a classified, and, as appropriate, an unclassified semiannual report by 31 October and 30 April of each year summarizing IC OIG's activities during the immediately preceding six-month period. The IC IG is also required to provide any portion of this report involving a component of an agency to the head of that agency.

Transmittal to Congress

Within 30 days of receipt, 50 U.S.C. § 3033(k)(1)(C) requires the DNI to transmit this report to the congressional intelligence committees, along with any comments the DNI considers appropriate. Additionally, the DNI must submit any portion of this report involving a component of an agency to the committees with jurisdiction over that agency simultaneously with transmittal to the congressional intelligence committees. In February 2026, Congress included a new requirement in the classified annex to the *Department of Defense Appropriations Act, 2026*[1] for the DNI to provide this report to the defense appropriations subcommittees concurrently with intelligence committees.

Classified and Unclassified Versions

Historically, IC OIG submitted an unclassified semiannual report accompanied by a classified annex containing only information that could not be included in the unclassified report. Beginning with the semiannual report for the second half of fiscal year (FY) 2025, IC OIG now submits both an unclassified and a classified version of the report as standalone products, rather than a single report with an annex. This change ensures that each version is independently comprehensive and readable without reference to the other.

About IC OIG

Statutory Authority

Prior to 2010, oversight of U.S. intelligence agencies was conducted by individual Inspectors General (IG) within each agency, including the IGs for the Central Intelligence Agency (CIA), National Security Agency (NSA), and other IC elements. Among those individual agency IGs was the Office of the Director of National Intelligence (ODNI) IG, whose jurisdiction was limited exclusively to ODNI. While these agency IGs provided valuable oversight within their respective agencies, no single IG possessed authority to oversee interagency issues, examine cross-cutting IC matters, or provide independent oversight of programs and activities under the authority and responsibility of the DNI.

[1] Division A of Public Law 119-75, 139 Statute 731.

In 2010, recognizing this critical gap and the evolving complexity of 21st century intelligence operations, Congress amended the *National Security Act of 1947*, 50 U.S.C. § 3001 et seq., to disestablish the ODNI IG and establish the IC IG with significantly expanded authority. Codified at 50 U.S.C. § 3033, this landmark legislation created an independent IC IG with statutory authority across all IC elements to address oversight gaps, enhance interagency accountability, and establish a centralized, trusted oversight and reporting mechanism for all IC personnel.

IC OIG has the statutory duty and responsibility to independently conduct, and issue reports on, audits, inspections, investigations, and reviews relating to programs and activities within the responsibility and authority of the DNI. IC OIG also receives and investigates complaints or information from whistleblowers and claims of reprisal. With our multi-disciplinary workforce, IC OIG advances economy, efficiency, and effectiveness across the IC and strengthens national security. The core duties and responsibilities of IC OIG align with the President's priorities for improving government accountability and performance across the Executive Branch.

Mission, Vision, and Values

IC OIG delivers objective, unbiased, and independent oversight of the IC. We ensure operational excellence, fiscal responsibility, and compliance with the Constitution. We protect whistleblowers, combat misconduct, and collaborate with Federal partners to safeguard the integrity of intelligence operations. In March 2026, we updated our seal, mission, vision, and values to better reflect what we do, why we do it, and how we do it.

Mission

To be a vanguard of integrity and excellence for the Intelligence Community through consequential oversight that strengthens national security, protects whistleblowers, and ensures accountability to the American people.

Vision

One Intelligence Community, fully accountable to those we serve.

Values

- Integrity
- Fortitude
- Excellence

Old IC OIG Seal

New IC OIG Seal

IC Inspectors General Forum

Under 50 U.S.C. § 3033(h)(2), the IC IG serves as the statutory chair of the Intelligence Community Inspectors General Forum, a collaborative body comprised of all 12 Inspectors General with oversight responsibility for one or more of the 18 IC elements.

Statement of Independence

The IC IG is appointed by the President of the United States, by and with the advice and consent of the Senate. By statute, the IC IG must be nominated based on integrity, experience, and demonstrated ability, and without regard to political affiliation. Accordingly, IC OIG conducts its duties with unwavering independence, objectivity, and impartiality. Our findings and conclusions remain free from bias or external interference, grounded solely in facts, applicable law, and established standards.

Oversight Standards

All IC OIG audits are conducted in accordance with standards set by the Government Accountability Office (GAO), to include generally accepted government auditing standards (GAGAS), or other applicable professional standards. All inspection and investigative activities conform to applicable standards adopted by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Organizational Structure

Transition to IC OIG 2.0

As ODNI evolved under "ODNI 2.0" to realign resources for greater efficiency and effectiveness, IC OIG undertook a similar modernization effort. As part of "IC OIG 2.0," we have streamlined from six divisions into four offices, as shown in Figure 1. This organizational update has already resulted in enhanced collaboration across oversight functions, more capacity for proactive and discretionary work, and opportunities to achieve greater impact. IC OIG 2.0 is also intended to facilitate more diverse missions, leverage interdisciplinary teams, and expand professional development opportunities.

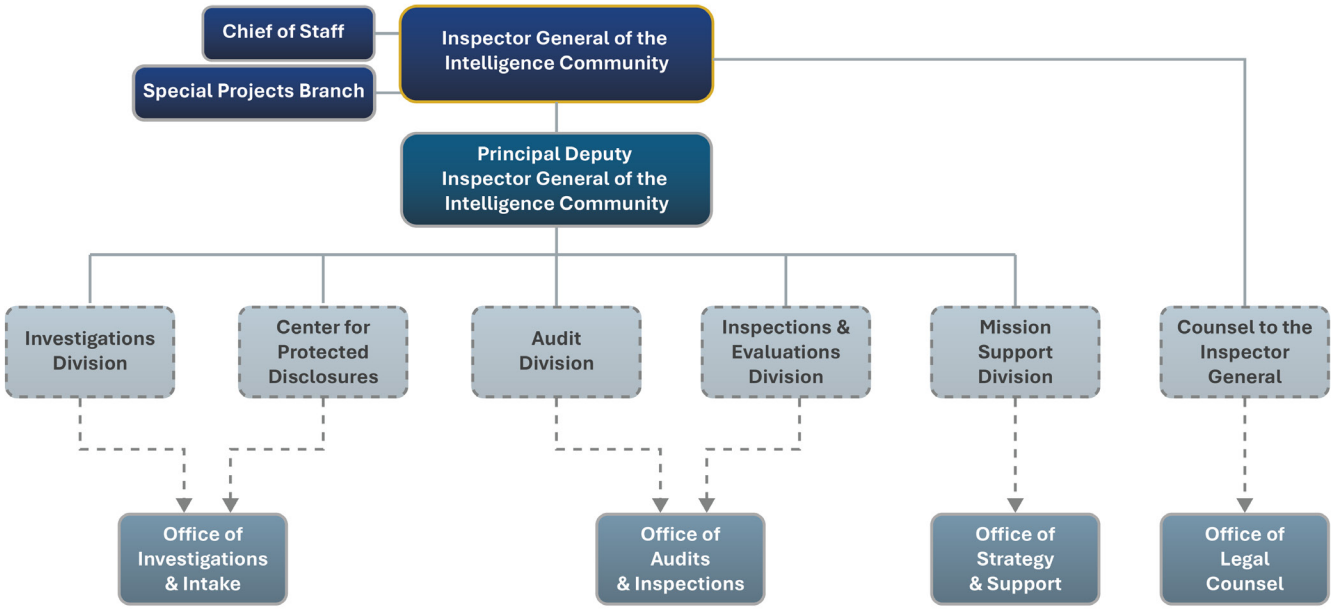

Figure 1: IC OIG 2.0

Office of Audits and Inspections

The Office of Audits and Inspections (OAI) is a consolidation of the Audit Division and the Inspections and Evaluations Division. The new OAI construct brings together the expertise of both divisions for more effective and efficient audits, inspections, evaluations, and reviews. OAI delivers evidence-based findings and actionable recommendations that drive meaningful improvements, informs decision-making, and results in impactful change. OAI leads community working groups and collaborates closely with counterparts across the IC.

During the reporting period, OAI issued five reports and 30 recommendations. Once implemented, OAI's recommendations will strengthen continuity of government and continuity of operations capabilities, and enhance ODNI's ability to achieve an unqualified opinion on its financial statements. OAI also provided results from its *Federal Information Security Modernization Act of 2014* audit to the IC Chief Information Security Officer Committee and IC Zero Trust Subcommittee. Additionally, OAI's previous engagement with Congress regarding ODNI's integration of artificial intelligence (AI) led to several new provisions on AI in the *Intelligence Authorization Act for Fiscal Year 2026*.

Office of Investigations and Intake

The Office of Investigations and Intake (OII) is a merger of the Center for Protected Disclosures and the Investigations Division. OII conducts administrative investigations and manages the IC IG Hotline, while safeguarding those who report wrongdoing. During the reporting period, OII completed 11 investigations, conducted eight preliminary reviews, and participated in five joint investigations with other Offices of Inspector General (OIGs), the Department of Justice, and the United States Attorney's Office (USAO) for the Eastern District of Virginia (EDVA). OII investigators also supported Federal partners in criminal investigations of anti-trust violations, conflicts of interest, misconduct, abuse of authority, and other potential violations of law. As of 31 March 2026, OII had 30 open investigations, and recovered $58,757 during the reporting period.

Additionally, OII conducts suspicious activity report (SAR) reviews, leveraging *Bank Secrecy Act* data to prevent terrorist attacks, disrupt criminal activities, and strengthen coordination among federal, state, and local law enforcement agencies. During the reporting period, OII reviewed hundreds of SARs for potential financial crimes in partnership with the USAOs serving EDVA and the Districts of Maryland and Columbia.

The Hotline handled 1,177 new contacts during the reporting period. Of those contacts, 318 were categorized as complaints. This represented a slight increase from prior reporting periods.

Office of Strategy and Support

The Office of Strategy and Support (OSS), formerly the Mission Support Division, is responsible for integrated, OIG-wide initiatives including strategic planning, resource allocation, data analytics, and administrative support. OSS leads mission support functions spanning planning, budget, human capital, technology, information management, executive coordination, and innovation.

During the reporting period, OSS led IC OIG's cost-saving relocation from Reston to Liberty Crossing. OSS also established a program for the issuance of IC badges to OIG partners, strengthening collaborative oversight across the IC. As of 31 March 2026, IC OIG had already sponsored 41 IC badges under this program. OSS also coordinated with each IC OIG office to identify technology innovation priorities and develop the *2026 Annual Work Plan*. Additionally, OSS established the Excellence Review Team (ERT) to ensure quality control, legal sufficiency, and classification reviews on all IC OIG deliverables.

Office of Legal Counsel

The Office of Legal Counsel (OLC), formerly the Counsel Division, provides independent legal advice to the Inspector General and ensures IC OIG oversight activities comply with applicable laws and policies. OLC has been refocused on core legal functions, transitioning away from its previous role as a catch-all for administrative tasks and final product edits. In February 2026, the External Review Panel (ERP) program was transferred from OII to OLC for better alignment with IC OIG's statutory requirements under 50 U.S.C. §§ 3233, 3234, and 3341. The placement of the ERP program under dedicated OLC oversight strengthens whistleblower protections and ensures more rigorous administrative law analysis.

During the reporting period, OLC accomplished a significant volume of work despite critical staffing challenges. OLC attorneys completed 86 internal legal reviews, delivered technical assistance on draft legislation, and provided direct support to the IC IG for several congressional engagements with Members and staff.

Special Projects Branch

The Special Projects Branch (SPB) is an interdisciplinary team that conducts special reviews and time-sensitive activities at the IC IG's direction without diverting resources from other ongoing activities. SPB has also been tasked with reviewing IC OIG matters that have remained open for extended periods to assist the IC IG in determining which cases warrant continued oversight activity and which may be appropriate for administrative closure.

IC OIG Staffing Overview

IC OIG employs an elite workforce consisting of cadre, detailees, and contractors. New hires slightly outpaced departures during the reporting period. As of 31 March, IC OIG had several hiring actions in progress. Many of these candidates were pending security.

Additional personnel details are available in the classified version of this report.

Statutory Reporting Requirements

Pursuant to 50 U.S.C. § 3033(k)(1), the semiannual report must certify whether the IC IG had full and direct access to all information relevant to the performance of the functions of the Office, describe the exercise of subpoena authority under 50 U.S.C. § 3033(g)(5) during the reporting period, and include such legislative recommendations as the IC IG considers appropriate to promote economy, efficiency, and effectiveness in the administration and implementation of programs and activities within the responsibility and authority of the DNI, and to detect and eliminate fraud and abuse in such programs and activities.

Collectively, these statutory requirements ensure that this report provides Congress and the DNI an assessment of systemic risk, corrective action, access to information, use of compulsory process, and any legislative changes needed to strengthen independent oversight across the IC.

Access to Information

Under 50 U.S.C. § 3033(g)(2)(B)–(D), IC OIG shall have access to any employee or contractor in the IC and "direct access" to all information necessary to fulfill its oversight responsibilities, regardless of classification or compartmentation. During the reporting period, IC OIG encountered substantive delays in obtaining information from IC elements and associated OIGs relevant to performance of statutory duties.

Despite the "direct access" authorized by statute, IC OIG lacks organic technical access to most records and information held by IC elements outside ODNI. For lawful access required in support of investigations, audits, inspections, and reviews, IC OIG must often rely on components of IC elements that may be closely associated with or even led by subjects of the very activity necessitating access, creating opportunities for concealment or obstruction. While Inspectors General Forum OIGs generally work collaboratively, such cooperation remains subject to each OIG's competing priorities and resource constraints.

Secure systems and pathways for direct access require development, deployment, and funding. Without such systems to facilitate truly direct access, IC OIG will likely continue to face intentional or unintentional delays that impair full and timely completion of oversight activities, including “urgent concern” matters. IC OIG is committed to working with the DNI, IC elements, and Congress to develop technical solutions that operationalize the direct access authority Congress has provided.

Additional details related to IC OIG’s substantive delays in obtaining information are available in the classified version of this report.

Subpoenas

IC OIG did not issue any subpoenas under its 50 U.S.C. § 3033(g)(5) authority during the reporting period. However, IC OIG supported the Department of Justice (DOJ) and other external agencies in obtaining eight grand jury subpoenas for matters IC OIG had previously referred or supported through joint investigative activities.

Unauthorized Disclosure of Classified Information

Intelligence Community Directive (ICD) 701, *Unauthorized Disclosures of Classified National Security Information* (22 December 2017), designates IC OIG as the central coordination hub for unauthorized disclosure matters across the IC. Under ICD 701, IC elements must notify IC OIG within seven business days of opening a preliminary inquiry into a suspected unauthorized disclosure, provide copies of any Crimes Reports submitted to DOJ, notify IC OIG when internal investigations are initiated and concluded, and furnish case reports for independent review. ICD 701 also requires IC OIG to maintain a repository of notifications, preliminary inquiries, Crimes Reports, and related submissions through final disposition. ICD 701 uses a three-tiered reporting process, as shown in Figure 2.

Tier	Description	IC Element Action	IC OIG Role
Tier 1	Element determines investigation not warranted, usually when information already widely disseminated.	Submit Crimes Report to DOJ.	Receives copy of Crimes Report.
Tier 2	Preliminary inquiry indicates internal investigation is appropriate.	Submit Crimes Report to DOJ; DOJ concurrence required for internal investigation.	Receives copy of Crimes Report; receives notification when internal investigation begins and ends.
Tier 3	Preliminary inquiry indicates criminal investigation should occur based on circumstances/severity of disclosure.	Submit Crimes Report to DOJ requesting Federal Bureau of Investigation (FBI) investigation.	Receives copy of Crimes Report; briefs DNI, as appropriate.
Post-Declination	FBI declines investigation, or DOJ declines prosecution.	Coordinate with IC OIG.	Reviews case to determine whether administrative investigation is appropriate.

Figure 2: ICD 701 Reporting Process

Since ICD 701 took effect in December 2017, IC OIG has identified significant opportunity to strengthen IC-wide implementation. IC OIG has been engaging with stakeholders to clarify jurisdiction, strengthen coordination protocols, and improve information sharing to achieve fuller ICD 701 compliance. Enhanced coordination will enable IC OIG to ensure appropriate deconfliction, preserve investigative integrity, reduce duplicative activities, and prevent the loss of relevant evidence. Through robust implementation and an integrated approach, IC OIG expects to enhance accountability and consistency in handling unauthorized disclosure matters.

Additional details related to IC OIG's receipt of notifications and submissions from IC elements are available in the classified version of this report.

Legislative Recommendations

Criminal Investigative Authority

Congress directed under 50 U.S.C. § 3033(g)(3)(A) that IC OIG receive and investigate "complaints or information from any person concerning the existence of an activity within the authorities and responsibilities of the Director of National Intelligence constituting a *violation of laws*, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and *specific danger to the public health and safety* (emphasis added)." This mandate extends across approximately 120,000 employees, contractors, and military personnel, and roughly $100 billion in programs and activities spanning the 18 IC elements. Unlike peer statutory Inspectors General with comparable enterprise-wide oversight responsibilities, IC OIG investigators lack explicit statutory law enforcement authority to execute traditional GS-1811 criminal investigator functions. This statutory gap materially constrains IC OIG's ability to conduct timely, independent, and comprehensive criminal investigations, creating a structural disadvantage relative to peer OIGs with similar jurisdiction and scope.

IC OIG therefore strongly recommends that Congress expressly authorize the IC IG to confer appropriate law enforcement authority on designated personnel. Any legislative solution should, at a minimum, authorize the employment of GS-1811 criminal investigators with law enforcement authority, subject to appropriate controls, to execute warrants, make arrests, and carry firearms; and provide access to law enforcement databases and systems necessary to conduct criminal investigations. Such authorities would complement IC OIG's existing authority to administer oaths under 50 U.S.C. § 3033(g)(4), issue subpoenas under 50 U.S.C. § 3033(g)(5), and report potential federal crimes to the Attorney General under 50 U.S.C. § 3033(k)(6). Criminal investigators would also strengthen whistleblower protection and improve the quality, speed, and prosecutorial viability of criminal referrals.

Whistleblower Complaint Notification System

Section 5334 of Division E of the *National Defense Authorization Act for Fiscal Year 2020*[2] required IC OIG, in consultation with the Forum, to establish a system under which IC OIG is notified of whistleblower complaints submitted to IC element OIGs that relate to programs and activities under the jurisdiction of the DNI, as well as information relating to those complaints and actions taken on them. Section 5334 also required implementation guidance that protects whistleblower privacy, enables IC OIG to oversee whistleblower policies and practices across the IC, and avoids imposing inappropriate resource burdens on IC element OIGs.

In July 2023, then-IC IG Thomas Monheim issued initial implementation guidance to the Forum. However, the current process consists of manually aggregated reports from the few participating OIGs and has not produced sufficiently timely or actionable notifications to meet statutory requirements. A secure, scalable system that partially or wholly automates cross-agency transmissions is needed. This shortfall limits IC OIG's ability to identify systemic issues, detect related matters spanning multiple IC elements, and ensure consistent oversight of IC whistleblower matters.

IC OIG is addressing this deficiency through updated Forum policy and modernized technology. An integrated case management system could satisfy this requirement while also enabling seamless integration on joint activities and referrals between OIGs. Express Congressional authorization or appropriation of funds for such a capability would reinforce these efforts and ensure full Section 5334 compliance.

[2] Pub. L. No. 116-92, div. E, § 5334(a), 133 Stat. 1198, 2141 (2019), amended by *Intelligence Authorization Act for Fiscal Year 2024*, Pub. L. No. 118-31, div. G, title III, § 7327(a), 137 Stat. 136, 1044 (2023).

IC Inspectors General Forum Coordination

Congress established the IC IG under 50 U.S.C. § 3033(h)(2)(A)-(B) as the Chair of the IC Inspectors General Forum, which consists of all statutory or administrative inspectors general with oversight responsibility for an IC element. The Forum is intended to inform its members of work of common interest and to address questions of jurisdiction or access that may involve more than one OIG. Where a matter falls within the jurisdiction of two or more IC Inspectors General, 50 U.S.C. § 3033(h)(1)(A) directs them to "expeditiously resolve" which office will conduct the investigation, inspection, audit, or review in order to avoid unnecessary duplication. The statute, at Section 3033(h)(3) further requires the OIG that conducts the matter to provide the results to any other OIG with jurisdiction that did not conduct it, including IC OIG.

In practice, these mechanisms have often proved insufficient. Limited staffing, fragmented information-sharing practices, and the absence of binding procedural authority can impede timely deconfliction and coordinated oversight. If the affected inspectors general cannot resolve a dispute with the assistance of the Forum, they must submit the question to the DNI and the head of the affected department or agency for resolution pursuant to Section 3033(h)(1)(B). That mechanism does not provide a practical means to compel timely compliance and is not well suited to routine oversight coordination across multiple departments, agencies, and security domains.

IC OIG therefore recommends that Congress amend 50 U.S.C. § 3033(h) to provide the IC IG with limited, process-oriented coordination authorities analogous to those exercised by the Department of War Inspector General with respect to component oversight under 5 U.S.C. § 4208(d). At a minimum, Congress should authorize the IC IG to issue binding coordination procedures for matters of overlapping jurisdiction, require timely notice of oversight activities that may implicate another Forum member's jurisdiction, establish deadlines and mechanisms for sharing completed oversight products, and designate a lead OIG where multiple offices have concurrent jurisdiction. Properly framed, these authorities would preserve the independence of each OIG while supplying the procedural discipline necessary for a federated oversight system to function effectively.

IC IG Fox and PDIG Shelton brief DNI Gabbard and DHS Secretary Mullin on IC OIG priorities and capabilities.

Audits, Inspections, and Evaluations

OAI conducts audits, inspections, and evaluations. Each product assesses programs or operations for compliance, internal controls, and efficiency and effectiveness, and each may result in findings and recommendations. Audits generally involve more extensive testing and analysis and therefore often require more time to complete. Inspections and evaluations are inherently more flexible in scope and methodology, and can often be completed more quickly.

The principal distinction among these products is the professional standard under which they are performed. Audits are conducted in accordance with GAO's GAGAS (commonly known as the Yellow Book). Inspections and evaluations are conducted in accordance with the CIGIE Quality Standards for Inspection and Evaluation (commonly known as the Blue Book). Although the standards overlap in important respects, Yellow Book audits generally require more extensive evidence and analysis, including more developed support for findings and root causes. The choice of product depends on the objective, available resources, and urgency of the work.

During the reporting period, OAI completed five projects and had 12 ongoing projects.

Completed Projects

AUD-2025-001: Interagency Joint Report on Compliance with the Cybersecurity Information Sharing Act of 2015 *(Congressionally Directed)*

On 18 December 2015, Congress enacted the *Cybersecurity Information Sharing Act of 2015* (CISA), 6 U.S.C. § 1501 et seq., to strengthen cybersecurity through improved sharing of cyber threat indicators and defensive measures. CISA requires the Inspectors General of the Departments of Commerce, War, Energy, Homeland Security, Justice, and the Treasury, together with the IC IG, in consultation with the Council of the Inspectors General on Financial Oversight, to submit a joint biennial report to Congress on Executive Branch implementation of CISA during the preceding two-year period.

In the most recent reporting cycle, the participating OIGs found that Executive Branch sharing of cyber threat information and defensive measures continued to improve, and that access to shared information expanded. During calendar years 2023 and 2024, entities continued to share unclassified cyber threat information through the Automated Indicator Sharing (AIS) capability and TOP SECRET cyber threat information through the Intelligence Community Analysis and Signature Tool (ICOAST), along with other mechanisms, including email, written reports, websites, and face-to-face engagements.

AUD-2025-005: Fiscal Year 2025 Audit of the Office of the Director of National Intelligence's Financial Statements *(Congressionally Directed)*

Under 50 U.S.C. § 3108, the DNI must ensure ODNI conducts a full financial audit annually and take all reasonable steps necessary to ensure that the audit contains an unqualified opinion of ODNI's financial statements.

IC OIG oversaw an independent public accounting (IPA) firm that was engaged to audit ODNI's consolidated financial statements. The IPA firm disclaimed an opinion on ODNI's consolidated financial statements because it could not obtain sufficient audit evidence to provide a bases for an audit opinion on the financial statements. In planning and performing the audit, the IPA firm considered ODNI's internal control over financial reporting as a basis for designing audit procedures as appropriate for expressing an opinion. The IPA firm did not express an opinion on the effectiveness of ODNI's internal control.

The IPA firm also performed tests of ODNI's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements, non-compliance with which could have a direct and material effect on the determination of the financial statement amounts and disclosures, including the provisions referred to in Section 803(a) of the *Federal Financial Management Improvement Act of 1996* (FFMIA). The IPA firm did not provide an opinion on compliance with those provisions, but did provide results of its tests of compliance with FFMIA.

Additional details on this project are available in the classified version of this report.

INS-2024-006: Classification Review of the Office of the Director of National Intelligence for FY 2023 *(Congressionally Directed)*

Pursuant to section 6721 of the *National Defense Authorization Act for Fiscal Year 2020*[3] , IC OIG is required, through fiscal year 2026, to conduct a biennial review of ODNI's classification and declassification processes and report the results to the congressional intelligence committees. The statute directs IC OIG to assess: (1) the accuracy of ODNI's application of classification and control markings on a representative sample of finished intelligence reports, including compartmented reports; (2) ODNI's compliance with declassification procedures; and (3) the effectiveness of ODNI's processes for identifying topics of public or historical importance that warrant prioritization for declassification review. This is IC OIG's third such review and covers fiscal year 2023.

Additional details on this project are available in the classified version of this report.

[3] Pub. L. No. 116-92, div. E, § 6721, 133 Stat. 1198, *as amended* by Section 6811(f) of the *Intelligence Authorization Act for Fiscal Year 2023*, Pub. L. No. 117-263, div. F, § 6811(f).

INS-2026-003: Inspection of the Office of the Director of National Intelligence Continuity and Operations Support Office *(IC OIG Priority)*

Based on information received on the IC IG Hotline, IC OIG conducted an inspection of ODNI's Continuity and Operations Support Office (COSO) in advance of the President's State of the Union Address on 24 February 2026. This inspection was conducted in accordance with 50 U.S.C. § 3033(e) to assess ODNI's compliance with Federal continuity requirements, and the effectiveness and workplace conditions of COSO.

IC OIG made nine recommendations to the ODNI Chief Operating Officer (COO) to strengthen COSO's operational readiness and improve its workplace environment. The COO concurred with the recommendations, and had already implemented several corrective measures in response to IC OIG's interim feedback prior to the State of the Union address. The COO provided a description of these completed actions and additional steps underway to fully address all recommendations.

Additional details on this project are available in the classified version of this report.

Peer Review of the National Reconnaissance Office OIG's Office of Audit *(Required by Government Oversight Standards)*

In March 2026, IC OIG issued its external peer review of the National Reconnaissance Office (NRO) OIG's Office of Audit. IC OIG conducted the review in accordance with *Government Auditing Standards* and CIGIE's *Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General*.

Additional details on this project are available in the classified version of this report.

Ongoing Projects

AUD-2024-005: Audit of the Office of the Director of National Intelligence Hiring Process *(IC OIG Priority)*

This audit assesses the effectiveness of ODNI's hiring and selection process, including whether it maximizes the pool of qualified applicants and supports the fair selection of the best-qualified candidates.

Additional details on this project are available in the classified version of this report.

AUD-2026-001: Review of ODNI's Compliance with the Payment Integrity Information Act of 2019 for FY 2025 *(Congressionally Directed)*

The *Payment Integrity Information Act of 2019* (PIIA) requires Inspectors General to review and report on their agency's compliance with statutory improper payment requirements. In response, IC OIG will assess ODNI's compliance with PIIA reporting and disclosure requirements as reflected in the *Office of the Director of National Intelligence Fiscal Year 2025 Agency Financial Report*.

AUD-2026-002: Fiscal Year 2026 ODNI Federal Information Security Modernization Act Evaluation *(Congressionally Directed)*

Inspectors General are required to annually evaluate their agencies' information security programs and practices under the *Federal Information Security Modernization Act of 2014* (FISMA). IC OIG will oversee a contracted independent assessment of the effectiveness and maturity of ODNI's information security program and practices for fiscal year 2026 using the Inspector General FISMA reporting metrics.

AUD-2026-003: Fiscal Year 2026 Audit of the Office of the Director of National Intelligence's Financial Statements *(Congressionally Directed)*

Under 50 U.S.C. § 3108, the DNI is required to ensure that a full financial audit of ODNI is conducted annually, and the DNI must take all reasonable steps necessary to ensure the audit contains an unqualified opinion on the financial statements of ODNI. The law also requires the ODNI Chief Financial Executive (CFE) to submit a report on the audit to the congressional intelligence committees.

IC OIG will oversee the IPA firm engaged to audit ODNI's financial statements and provide an opinion on whether they are fairly presented, in all material respects, in accordance with U.S. generally accepted accounting principles. The audit will also assess internal control over financial reporting, compliance with applicable laws and regulations, and the status of prior-year findings. This work supports the integrity and reliability of ODNI's financial management and reporting.

INS-2024-005: Assessment of Overt Human and Open-Source Intelligence Collection Programs Established by the Department of Homeland Security's Office of Intelligence and Analysis (IC OIG Priority)

Pursuant to Section 7324(d) of the *Intelligence Authorization Act for Fiscal Year 2024*, IC OIG submitted a report to the congressional intelligence committees on 31 December 2024 regarding Department of Homeland Security (DHS) Office of Intelligence and Analysis collection programs. IC OIG will conduct a follow-on activity related to this report.

Additional details on this project are available in the classified version of this report.

INS-2025-001: Review of the Federal Bureau of Investigation's Confidential Human Source Program *(Congressionally Directed)*

Pursuant to Section 7323 of the *Intelligence Authorization Act for Fiscal Year 2024*, IC OIG is conducting a review of the policies and procedures governing the FBI's Confidential Human Source Program and assessing the FBI's compliance with those requirements, including the *Attorney General's Guidelines Regarding the Use of Confidential Human Sources* and ICD 304, *Human Intelligence*. IC OIG is conducting this work in coordination with the DOJ OIG.

INS-2025-003: Evaluation of Intelligence Community Information Sharing Activities *(IC OIG Priority)*

On 16 January 2025, the DNI issued *ICD 406, Strengthen, Expand, and Diversify Intelligence Community Engagements with and Prioritize Work on Non-State Entities*, to improve the flow of information to and from non-state entities, including private industry and other non-governmental partners. IC OIG will evaluate the efficiency and effectiveness of IC information sharing with the private sector, including whether IC elements are implementing the directive in a manner that strengthens efforts to warn of and disrupt threats to the U.S. homeland.

INS-2026-001: Sensitive Inspection *(IC OIG Priority)*

IC OIG will conduct an inspection of a sensitive IC program.

Additional details on this project are available in the classified version of this report.

INS-2026-002: Evaluation of Intelligence Oversight Capabilities in Non-Title 50 Departments and Agencies and Select Intelligence Community Elements *(IC OIG Priority)*

IC OIG will assess the oversight capabilities of non-IC federal departments and agencies and select IC elements, to include the ability to access and safeguard classified national security information and any challenges to provide oversight of intelligence activities.

Additional details on this project are available in the classified version of this report.

Multiple Projects: Reviews of Insider Threat Policy Compliance and Effectiveness *(Congressionally Directed)*

Insider threats arise when IC employees, contractors, detailees, assignees, or fellows misuse authorized access, intentionally or otherwise, in ways that harm U.S. national security. Since insider threat risk evolves over time, IC policies and programs require continuing oversight. The classified annex accompanying the *Intelligence Authorization Act for Fiscal Year 2023* directs the IC OIG to conduct audits of IC element's compliance with insider threat policies. IC OIG will assess whether selected IC elements' insider threat policies are consistent with applicable IC standards and whether those elements are implementing those policies effectively.

Inspection of the Cybersecurity Posture of Certain National Security Systems *(IC OIG Priority)*

IC OIG will conduct an inspection of the cybersecurity posture of certain national security systems.

Additional details on this project are available in the classified version of this report.

Peer Review of the National Security Agency OIG's Inspections and Evaluations Program *(Required by Government Oversight Standards)*

During the reporting period, IC OIG initiated an external peer review of NSA OIG's Inspections and Evaluations program in accordance with applicable professional standards.

Investigations

OII conducts independent and objective investigations into potential violations of law, rule, or regulation related to programs and activities within the responsibility and authority of the DNI. The investigative process begins with an intake procedure in which allegations received through the Hotline and other sources are screened and clarified to capture the full scope of the complaint or information. OII officers assess the credibility and substantive merit of the information, identify potential witnesses, and determine the availability of corroborating evidence. The IC IG oversees the progression of these matters and approves referrals to ODNI management or partner entities, the conversion of initial contacts into preliminary reviews, and the escalation of preliminary reviews into formal investigations, as warranted.

Preliminary reviews involve targeted investigative actions to expeditiously test the allegation. If the results support further inquiry, a formal investigation may be initiated. Throughout this process, the IC IG applies criteria established in law, IC OIG policy, and DOJ procedures to determine the appropriate course of action and ensure efficient and effective use of IC OIG resources.

Completed Investigations

OII completed 11 investigations during the reporting period, including two in which allegations were substantiated and nine in which allegations were unsubstantiated or unfounded. Overviews are provided below.

Contract and Procurement Fraud

22-0016-IN: Alleged Improper Contracting Actions

- **Allegation(s)**: Two ODNI employees improperly advocated for a vendor based on personal relationships and provided proprietary government information to give the vendor a competitive bidding advantage.
- **Finding(s):** Unsubstantiated
- **Result(s):** Referral to the ODNI COO with two recommendations for action.

Contractor Misconduct

23-0008-IN: Fraudulent Project Management Professional Certifications

- **Allegation(s):** A former ODNI contractor assisted other contractors in fraudulently obtaining their Project Management Professional (PMP) certifications, which may have enhanced their qualifications to be selected for or to serve in certain positions. According to the complaint, an ODNI contractor, in return for payment, ensured that individuals passed the PMP certification test without actually taking it.
- **Finding(s):** Substantiated
- **Result(s):** Referral to the ODNI COO with three recommendations for action.

Reprisal

23-0015-IN: Alleged Reprisal Against ODNI Employee

- **Allegation(s):** An ODNI employee alleged that ODNI senior officials and his/her first-line supervisor took two adverse personnel actions against him/her after the employee informed ODNI senior officials that information collected by the Office of Personnel Management contained classified information.
- **Finding(s):** Unsubstantiated
- **Result(s):** No further action at this time.

23-0017-IN: Alleged Reprisal Against CIA Employee

- **Allegation(s):** CIA was operating an Office of Equal Employment Opportunity (OEEO) program that violates Equal Employment Opportunity Commission law, the former CIA IG acted without independence and engaged in misconduct, and the employee was subjected to unlawful personnel actions in reprisal for protected disclosures, including protected disclosures to IC OIG in the "urgent concern" process.
- **Finding(s):** Unsubstantiated
- **Result(s):** No further action at this time.

23-0018-IN: Alleged Reprisal Against CIA Employee[4]

- **Allegation(s):** CIA was operating an OEEO program that violates Equal Employment Opportunity Commission law, the former CIA IG acted without independence and engaged in misconduct, and the employee was subjected to unlawful personnel actions in reprisal for protected disclosures, including protected disclosures to IC OIG in the "urgent concern" process.
- **Finding(s):** Unsubstantiated
- **Result(s):** No further action at this time.

23-0022-IN: Alleged Reprisal Against ODNI Contractor Employee

- **Allegation(s):** Two ODNI employees retaliated against a contractor working for ODNI by revoking his/her access to ODNI computer systems, making decisions about his/her organizational affiliation, recommending that the prime contractor terminate the complainant's contract, and blocking him/her from undergoing an expanded scope polygraph, all in reprisal for the contractor's protected disclosures.
- **Finding(s):** Unsubstantiated
- **Result(s):** No further action at this time.

24-0008-IN: Alleged Reprisal Against ODNI Employee

- **Allegation(s):** An ODNI cadre employee was allegedly uncompensated for certain work performed and denied promotion twice in retaliation for a protected disclosure.
- **Finding(s):** Partially substantiated
- **Result(s):** Referral to the ODNI COO with one recommendation for action.

[4] IC OIG Case No. 23-0017-IN and 23-0018-IN involved different complainants.

25-0003-IN: Alleged Reprisal Against ODNI Employee

- **Allegation(s):** An ODNI employee alleged that a senior ODNI official took disciplinary actions against him/her and significantly changed his/her job duties and responsibilities in reprisal for nine protected disclosures.
- **Finding(s):** Unsubstantiated
- **Result(s):** No further action at this time.

Conflict of Interest

25-0009-IN: Alleged Conflict of Interest – Part-Time Contractor Work

- **Allegation(s):** A former ODNI cadre employee may have committed policy and legal violations by working part-time as a government contractor while employed by the U.S. Government.
- **Finding(s):** Unsubstantiated
- **Result(s):** Referral to the ODNI COO with one recommendation for action.

Employee Misconduct

25-0001-IN: Alleged Wrongful Denial of Reimbursement

- **Allegation(s):** An ODNI employee alleged that an ODNI office wrongfully denied his/her request for reimbursement for an academic program that cost over $80,000, despite receiving supervisor approval to attend.
- **Finding(s):** Unsubstantiated
- **Result(s):** Referral to the ODNI COO with two recommendations for action.

25-0010-IN: Misuse of Government Computer for Personal Business

- **Allegation(s):** An ODNI cadre employee used a TOP SECRET level information system to promote his/her for-profit business.
- **Finding(s):** Substantiated
- **Result(s):** Referral to the ODNI COO with one recommendation for action.

Open Investigations

At the end of the reporting period, IC OIG had 30 open investigations, as shown in Figure 3. The majority of these cases involved alleged whistleblower retaliation, employee misconduct, and time and attendance fraud.

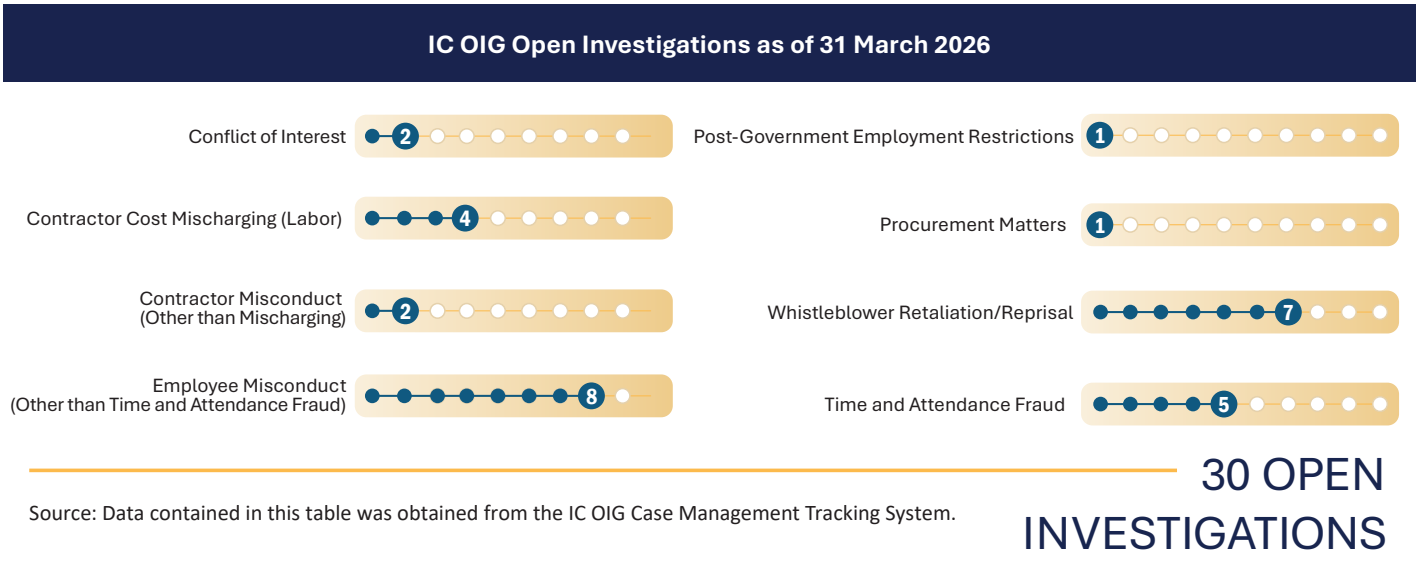

Figure 3: IC OIG Open Investigations as of 31 March 2026

IC IG Fox addresses the workforce at an ODNI Town Hall with General Counsel John "Jack" Dever and Ricky Gill, Director of the Office of Economic Security and Emerging Technologies.

Intake and Referrals

IC IG Hotline

The IC IG Hotline is accessible via classified and unclassified email, phone lines, USPS mail, fax, secure web submissions, walk-ins, and drop boxes at select ODNI facilities (see Figure 4). OII investigative analysts assisted complainants by explaining reporting options and legal protections.

Figure 4: Six Ways to Report Concerns

A contact is any engagement by an individual or entity with the IC IG Hotline that has been received, tracked, and processed during the reporting period. Contacts include complaints, referrals, general inquiries, and other engagements. A complaint is a contact in which an individual reports a specific allegation or information that raises potential concern under the oversight authority of IC OIG.

OII receives and tracks contacts from IC personnel, other government employees and contractors, and private citizens. During the reporting period, OII processed 1,177 new contacts, of which 318 were processed as complaints (see Figures 5, 6, and 7).

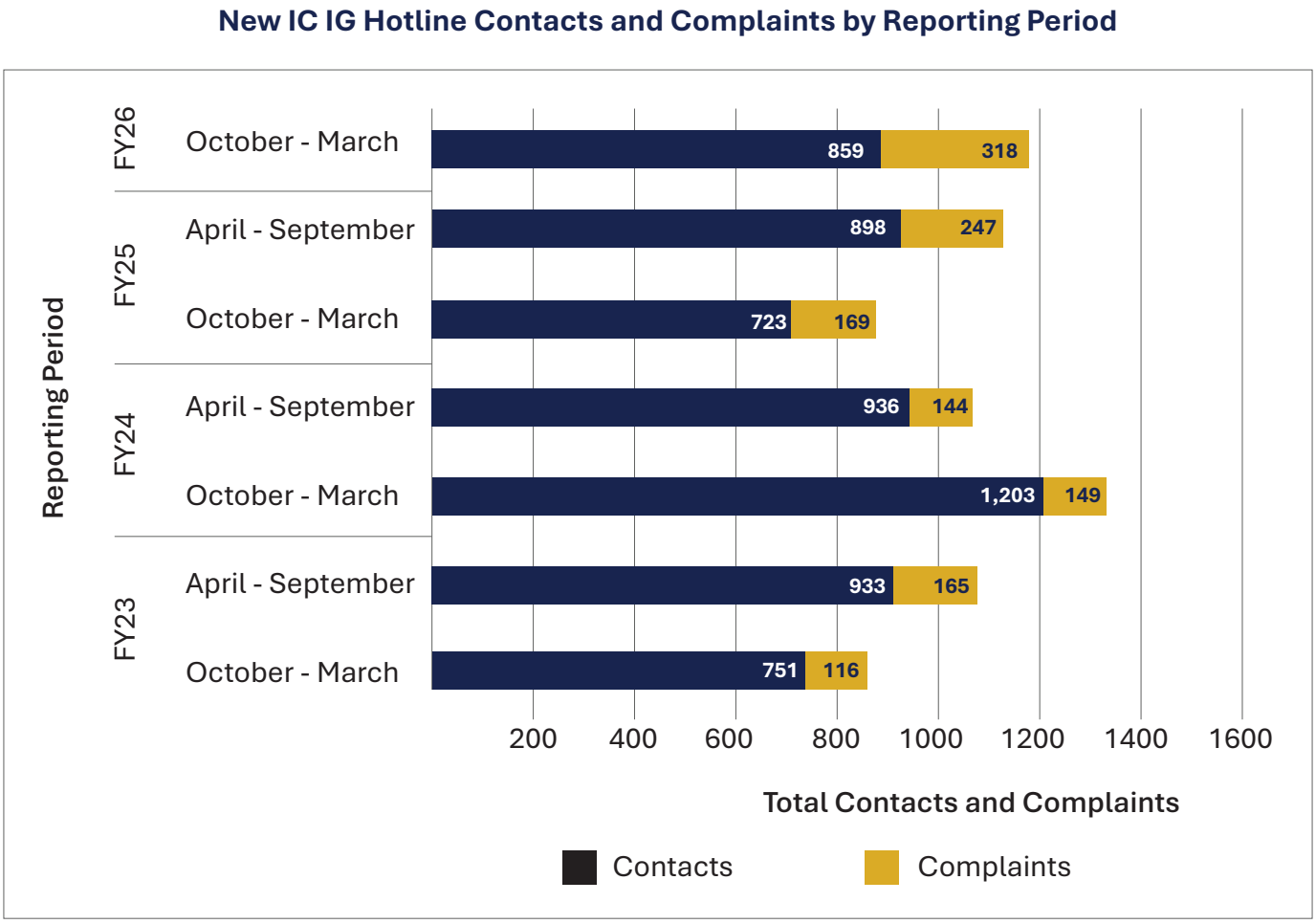

Figure 5: New IC IG Hotline Contacts and Complaints by Reporting Period (FY 2023 – FY 2026)

Status of IC IG Hotline Complaints Received During Report Period

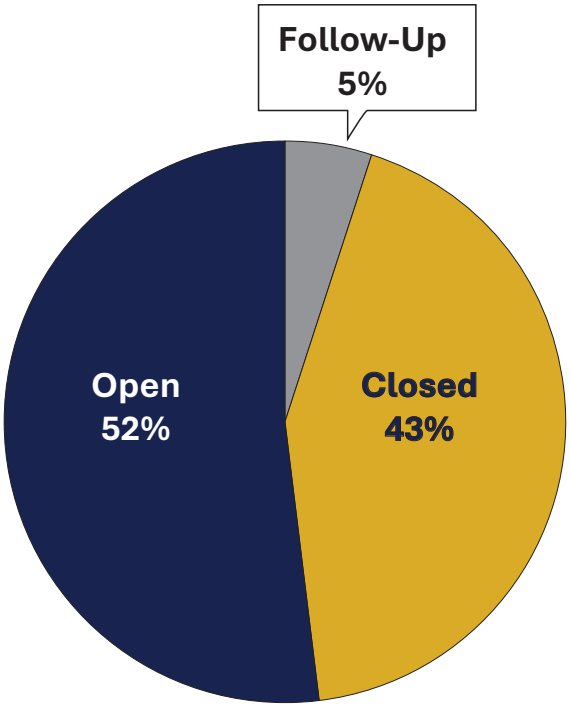

Figure 6: Status of IC IG Hotline Complaints received, 1 October 2025 – 31 March 2026

IC OIG promotes fraud awareness at ODNI.

New IC IG Hotline Complaints by Organization

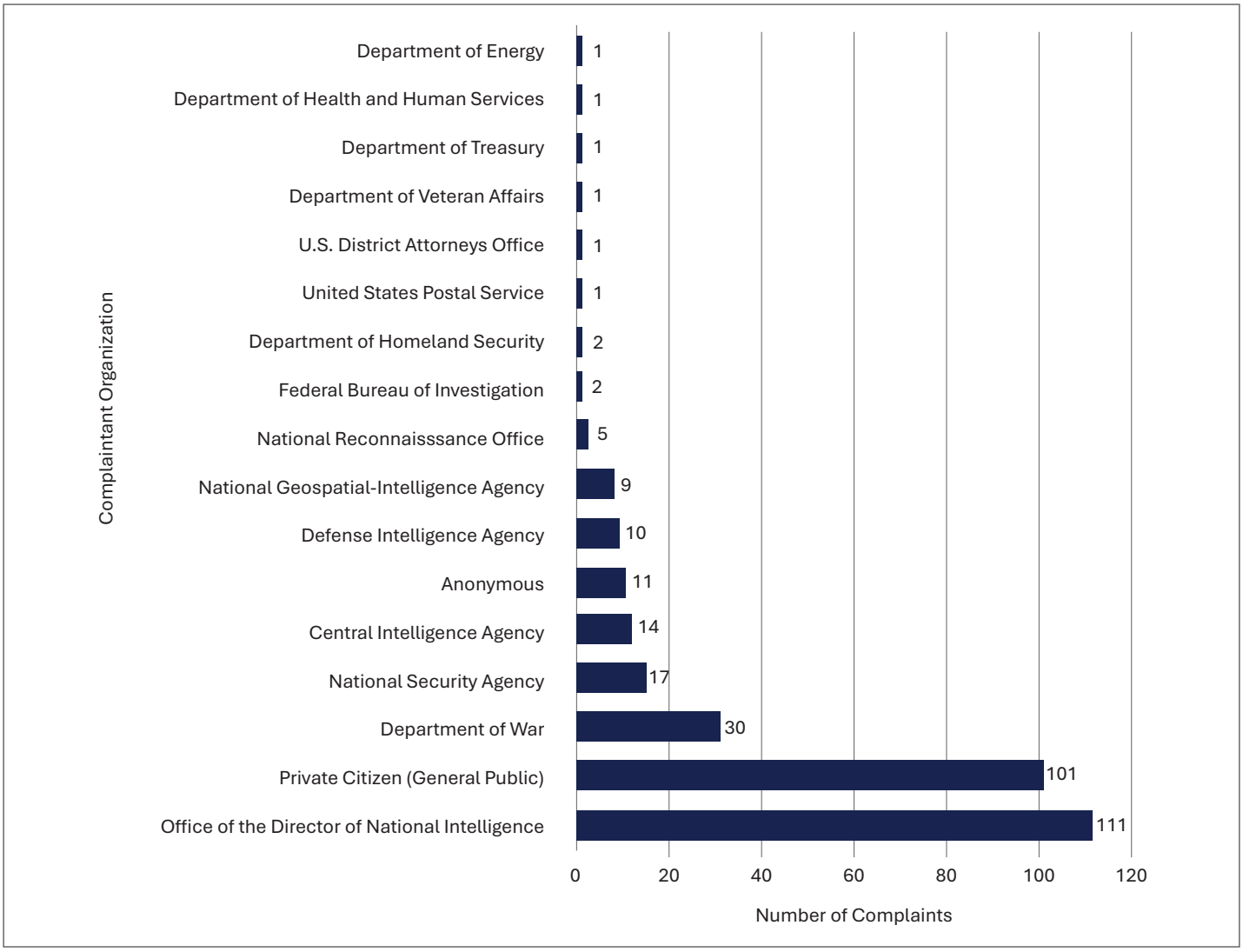

Figure 7: New IC IG Hotline Complaints by Organization, 1 October 2025 – 31 March 2026

External Review Panel Requests

IC OIG processes ERP requests pursuant to 50 U.S.C. § 3236 and Presidential Policy Directive-19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*, from IC employees and contractors seeking review of reprisal allegations after exhausting their home IC element's whistleblower protection processes. In appropriate cases, IC OIG may convene an ERP to consider whether the original reprisal complaint decided pursuant to 50 U.S.C. § 3234, *Prohibited Personnel Practices in the Intelligence Community* or 50 U.S.C. § 3341(j), *Retaliatory Revocation of Security Clearances and Access Determinations*, constituted clear error potentially warranting a different decision. During the reporting period, IC OIG processed five new ERP requests, closed three, and continued reviewing 28 (see Figure 8). One ERP remains open, pending panel-member assignment notification.

External Review Panels: 1 October 2025 - 31 March 2026	
New Requests	5
Requests Closed	3
Requests Under Evaluation	28

Figure 8: External Review Panels

"Urgent Concern" Complaints

IC OIG receives and processes "urgent concern" complaints under the *Intelligence Community Whistleblower Protection Act* (ICWPA), 50 U.S.C. § 3033(k)(5). The ICWPA ensures whistleblowers are protected when they elect to disclose information to the congressional intelligence committees about allegations of serious abuses, law violations, or deficiencies related to intelligence activities (see Figure 9).

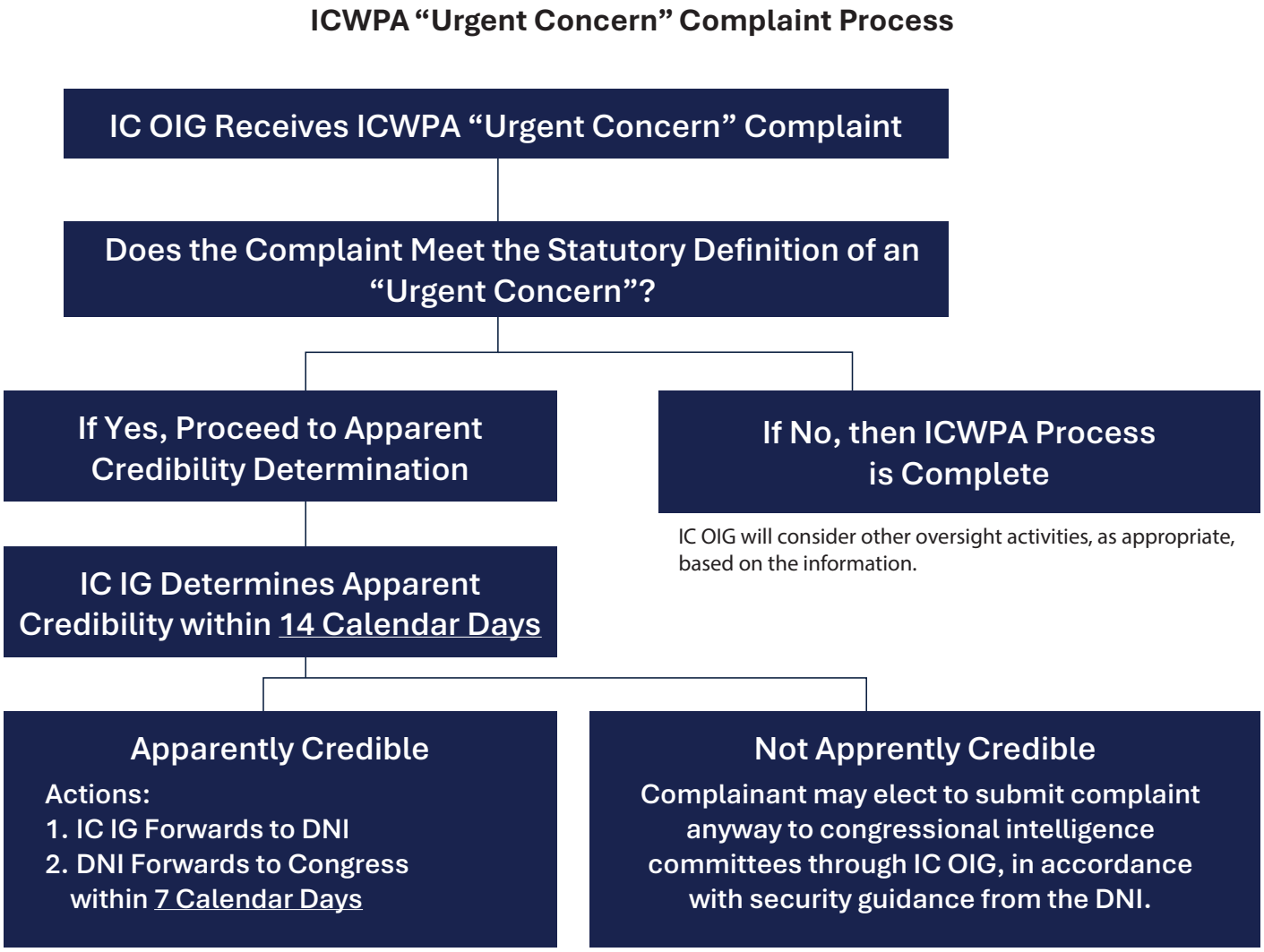

Figure 9: ICWPA "Urgent Concern" Complaint Process

During the reporting period, IC OIG received seven ICWPA "urgent concern" complaints (see Figure 10). The IC IG determined that allegations in the three complaints did not meet the statutory definition of an "urgent concern." One complaint is ongoing and not included in this report.

ICWPA "Urgent Concern" Complaints: 1 October 2025 - 31 March 2026			
Determination	**No Further Action Required Under the ICWPA***	**Transmitted to the DNI**	**Transmitted to the Congressional Intelligence Committees**
Urgent; Appears Credible	0	0	0
Urgent; Does Not Appear Credible	0	0	0
Not Urgent; Does Not Appear Credible	3*	0	0
Withdrawn by Complaintant	1	0	0
Open	1	0	0
Ineligible; Lacked Standing	2	0	0
* Complaints determined to be neither "urgent" nor apparently credible under the ICWPA may still be subject to other oversight activities.			

Figure 10: ICWPA Urgent Concern Complaints, 1 October 2025 – 31 March 2026

25-0012-CD: Alleged Improper Collection Tasking Against U.S. Persons by IC Employee

- **Allegation(s):** A former IC employee allegedly directed a subordinate to conduct collection against U.S. persons in violation of Executive Order 12333 and applicable Attorney General Guidelines.
- **Determination:** The IC IG determined the matter did not constitute an "urgent concern" under 50 U.S.C. § 3033(k)(5)(G) based on: (1) no collection occurred according to complainant and witness testimony; (2) the alleged tasking, if made, may have constituted deliberative discussion rather than operational tasking; (3) witness statements contradicting the complainant's characterization; (4) absence of corroborating records from the relevant IC element; and (5) lack of evidentiary support for the alleged conversation.
- **Action Taken:** The complainant was notified per 50 U.S.C. § 3033(k)(5)(E). IC OIG retains authority to conduct further oversight if additional evidence emerges.

25-0013-CD: Alleged Misuse of Classified Information and Fraudulent Foreign Sales of Intelligence-Derived Products

- **Allegation(s):** A defense contractor allegedly defrauded the U.S. Government by improperly using derivative TOP SECRET information to produce purportedly UNCLASSIFIED analytical products marketed and sold to foreign militaries as “open-source intelligence” in violation of 18 U.S.C. § 287 and Executive Order 13526.
- **Determination:** No determination under 50 U.S.C. § 3033(k)(5)(G) was required because the complainant lacked standing under the ICWPA. The "urgent concern" mechanism under 50 U.S.C. § 3033(k)(5)(A) is limited to current and former employees and contractors of IC elements as defined in 50 U.S.C. § 3003(4). The complainant’s employer did not qualify, placing the matter outside IC OIG's ICWPA jurisdiction.
- **Action Taken:** The complainant was notified of their lack of standing per 50 U.S.C. § 3033(k)(5)(E). IC OIG referred the matter to Department of War OIG and two federal law enforcement agencies for action within their respective jurisdictions.

26-0001-CD: Alleged Procedural Misconduct in External Review Panel Process

- **Allegation(s):** A former IC employee alleged that an IC officer committed misconduct by improperly denying a complainant’s request to convene a panel to rectify a retribution claim following home agency denial.
- **Determination:** No determination under 50 U.S.C. § 3033(k)(5)(G) was required because the complainant lacked standing under the ICWPA.
- **Action Taken:** The complainant was notified of their lack of standing. Separately, IC OIG conducted an internal review of the ERP process identifying opportunities to improve administration by realigning duties from OII to OLC.

26-0002-CD: Alleged Abuse of Authority by IC Employees

- **Allegation(s):** Employees of an IC element allegedly engaged in arbitrary or capricious exercise of authority in violation of Executive Order 12333 and internal agency regulations.
- **Determination:** The IC IG determined the matter did not constitute an “urgent concern” under 50 U.S.C. § 3033(k)(5)(G) based on the following factors: (1) the complainant lacked direct, firsthand knowledge of officials’ intent; (2) the complainant’s assertions were predominantly based on speculation of motives rather than objective evidence; and (3) the absence of documentary communications, policy violations, or witness corroboration establishing a reasonable basis that the conduct constituted a “serious or flagrant problem, abuse, violation of law or Executive order, or deficiency” under 50 U.S.C. § 3033(k)(5)(G)(i).
- **Action Taken:** The complainant was notified per 50 U.S.C. § 3033(k)(5)(E). IC OIG subsequently received additional evidence not available during the initial 14-day review period and may conduct further oversight activities using broader authorities under 50 U.S.C. § 3033.

26-0003-CD: Alleged Abuse of Authority and Misuse of Intelligence Functions

- **Allegation(s):** An IC element employee allegedly abused authority and misused intelligence functions in violation of Executive Order 12333 and agency policy.
- **Determination:** No determination under 50 U.S.C. § 3033(k)(5)(G) was made because the complainant withdrew their intent to report to Congress. The ICWPA requires both the submission of the complaint to IC OIG and the complainant's intent to report to Congress.
- **Action Taken:** The complainant was notified that the urgent concern determination process was terminated based on the withdrawal of their intent to report to Congress. The allegations remain under review through IC OIG's separate oversight activities.

26-0004-CD: Alleged Mishandling of Equal Employment Opportunity Matter

- **Allegation(s):** An IC element's Office of Equal Employment Opportunity (EEO) allegedly mishandled an EEO complaint and improperly disclosed protected information that directly influenced adverse performance actions against an EEO complainant in violation of 29 C.F.R. § 1614.108(d) and internal agency regulations.
- **Determination:** The IC IG determined the matter did not constitute an "urgent concern" under 50 U.S.C. § 3033(k)(5)(G) because the allegation concerned an individual employment grievance rather than a matter relating to funding, administration, or operation of an intelligence activity under 50 U.S.C. § 3033(k)(5)(G)(i). Furthermore, the complainant did not establish a nexus between the alleged wrongdoing and any element of the statutory definition of a matter of "urgent concern."
- **Action Taken:** The complainant was notified per 50 U.S.C. § 3033(k)(5)(E) and informed of alternative remedies including Equal Employment Opportunity Commission processes, PPD-19 complaints if alleging retaliation for protected whistleblowing, or other applicable administrative or judicial forums. IC OIG retains discretion to conduct oversight inquiries into systemic EEO issues should information emerge suggesting broader problems implicating intelligence programs or activities.

Referrals

IC OIG often receives complaints or allegations best addressed by other entities, including those posing security risks that require further coordination. During the reporting period, IC OIG referred 134 complaints to other entities.

New Recommendations

The following section lists IC OIG recommendations for corrective actions addressing significant problems, abuses, or deficiencies in intelligence programs and activities.[5]

Audit: Fiscal Year 2025 Audit of the Office of the Director of National Intelligence's Financial Statements

2026-FSA-001: For the ODNI COO: Include, in all Interagency Agreements (IAAs) with Other Government Agencies (OGAs), the minimum details the OGA is required to provide as part of the invoice, as identified in ODNI's Internal Process Document 40.04a.

2026-FSA-002: For the ODNI COO: Should not approve IAA expenses until: (a) The OGA provides the minimum information required, per the IAA; and (b) they have completed the Reviewer's Checklist.

2026-FSA-003: For the ODNI COO: Continue to perform periodic OGA intragovernmental expense compliance reviews to verify that Contracting Officer's Technical Representatives are completing the Reviewer Checklist and attaching supporting documentation provided by the OGA to the transaction recorded in the financial management system.

2026-FSA-004: For the ODNI COO: Continue implementing the OGA Form with additional OGAs.

2026-FSA-005: For the ODNI COO and ODNI Chief Information Officer (CIO): Ensure the process owner for Internal Use Software (IUS) assets has the appropriate authority to establish processes and controls to enforce ODNI's compliance with IUS financial reporting requirements.

2026-FSA-006: For the ODNI COO and ODNI CIO: Identify a complete population of IUS assets.

2026-FSA-007: For the ODNI COO and ODNI CIO: Review and revise requirements for all ODNI components to capture and maintain documentation to substantiate IUS assets and balances.

2026-FSA-008: For the ODNI COO and ODNI CIO: Review and update policies and procedures to account for and report IUS assets in accordance with Federal requirements and standards, including internal controls and procedures that regularly validate the accuracy and completeness of the population.

2026-FSA-009: For the ODNI COO and ODNI Facilities and Logistics (F&L): Continue to develop and implement procedures and internal controls to verify that ODNI is capturing, reporting, and maintaining sufficient documentation to support all capital purchases and improvements related to real property.

2026-FSA-010: For the ODNI COO and ODNI F&L: Continue to develop and implement procedures to identify and appropriately report leases, including consideration of factors identified in Statement of Federal Financial Accounting Standards (SFFAS) No. 54, such as: (a) right to control an asset, including the right to economic benefit associated with the asset or the right to control economic benefits of the asset; (b) explicit or implicit identification of an asset; and (c) period of time of control.

[5] IC OIG does not have any status updates to provide on significant recommendations described in previous semiannual reports.

2026-FSA-011: For the ODNI COO and ODNI F&L: Perform a full review of ODNI's lease population against the current SFFAS No. 54 standards. Ensure that all supporting documentation needed to substantiate the lease population, including documentation to support the value of previously acquired leases, is sufficient and maintained to document the accuracy and completeness of financial reporting and disclosures.

2026-FSA-012: For the ODNI COO and ODNI F&L: Ensure the necessary posting models are available in the financial system to record lease transactions in compliance with the Treasury Financial Manual and the U.S. Standard General Ledger at the transaction level.

2026-FSA-013: This recommendation is available in the classified version of this report.

2026-FSA-014: This recommendation is available in the classified version of this report.

2026-FSA-015: This recommendation is available in the classified version of this report.

2026-FSA-016: For the ODNI COO: Finalize Internal Process Document 64.04f.

2026-FSA-017: For the ODNI COO: COO/Facilities & Mission Services complete its efforts to identify all potential heritage assets at all ODNI locations.

2026-FSA-018: For the ODNI COO: On a regular basis, at least annually, COO/Facilities & Mission Services in coordination with the applicable component, prepare Internal Process Document 64.04f Appendix B, whether in draft or finalized, for all new potential heritage assets and submit to the COO.

2026-FSA-019: For the ODNI COO: On a regular basis, at least annually, the COO should review any Internal Process Document 64.04f Appendix B forms submitted by components and make a determination as to whether potential heritage assets shall be accessioned into ODNI's heritage asset collection.

2026-FSA-020: This recommendation is available in the classified version of this report.

2026-FSA-021: This recommendation is available in the classified version of this report.

Inspection: Inspection of the Office of the Director of National Intelligence Continuity and Operations Support Office

2026-COSO-001: This recommendation is available in the classified version of this report.

2026-COSO-002: This recommendation is available in the classified version of this report.

2026-COSO-003: This recommendation is available in the classified version of this report.

2026-COSO-004: This recommendation is available in the classified version of this report.

2026-COSO-005: This recommendation is available in the classified version of this report.

2026-COSO-006: This recommendation is available in the classified version of this report.

2026-COSO-007: For the ODNI COO: Conduct an independent workplace environment review, such as a climate assessment, to determine areas for improvement.

2026-COSO-008: This recommendation is available in the classified version of this report.

2026-COSO-009: For the ODNI COO: After corrective actions, conduct an independent workplace environment review to determine whether results improved.

Abbreviations and Acronyms

AI	Artificial Intelligence
AIS	Automated Indicator Sharing
CFE	Chief Financial Executive
CIA	Central Intelligence Agency
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISA	Cybersecurity Information Sharing Act of 2015
COO	Chief Operating Officer
COSO	Continuity and Operations Support Office
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOJ	Department of Justice
EDVA	Eastern District of Virginia
EEO	Equal Employment Opportunity
ERP	External Review Panel
ERT	Excellence Review Team
F&L	Facilities & Logistics
FBI	Federal Bureau of Investigation
FFMIA	Federal Financial Management Improvement Act of 1996
FISMA	Federal Information Security Modernization Act of 2014
FO	Front Office
FTE	Full-Time Equivalent
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	General Accountability Office
IAA	Interagency Agreement
IC	Intelligence Community
ICD	Intelligence Community Directive
ICOAST	Intelligence Community Analysis and Signature Tool

Abbreviations and Acronyms

IC IG	Inspector General of the Intelligence Community
IC OIG	Intelligence Community Office of the Inspector General
ICWPA	Intelligence Community Whistleblower Protection Act
IG	Inspector General
IPA	Independent Public Accounting
IUS	Internal Use Software
NRO	National Reconnaissance Office
NSA	National Security Agency
OAI	Office of Audits and Inspections
ODNI	Office of the Director of National Intelligence
OEEO	Office of Equal Employment Opportunity
OGA	Other Government Agency
OIG	Office of Inspector General
OII	Office of Investigations and Intake
OLC	Office of Legal Counsel
OSS	Office of Strategy and Support
PIIA	Payment Integrity Information Act of 2019
PMP	Project Management Professional
PPD	Presidential Policy Directive
SAR	Suspicious Activity Report
SPB	Special Projects Branch
USAO	United States Attorney's Office

IC IG HOTLINE

855-731-3260 • WWW.DNI.GOV/ICIG

REPORT SUSPECTED FRAUD, WASTE, AND ABUSE