Office of the Inspector General of the Intelligence Community

Semiannual Report
October 2018 - March 2019

Michael K. Atkinson
Inspector General of the Intelligence Community

TABLE OF CONTENTS

MESSAGE FROM THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

On behalf of the Office of the Inspector General of the Intelligence Community (ICIG), I am pleased to submit this Semiannual Report highlighting the ICIG's objectives, achievements, and activities from October 1, 2018, through March 31, 2019. This is the second Semiannual Report I have submitted, and the first that includes a full six-month reporting period, since I was confirmed as the Inspector General of the Intelligence Community in May 2018.

The unique role of the ICIG in the Intelligence Community is to look across the intelligence landscape to help improve management, coordination, cooperation, and information sharing among the 17 agencies that comprise the United States Intelligence Community. During this reporting period, in fulfilling that role, I had the privilege of leading the U.S. delegation to Canberra, Australia, at the annual meeting with our intelligence oversight counterparts from the Five Eyes intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States. I also had the pleasure of joining the U.S. delegation in Brussels, Belgium, for the Second Annual Review of the European Union-United States Privacy Shield framework that regulates and protects personal data transferred from the EU to the U.S. for commercial purposes. I also visited multiple ground stations in the United States and abroad. In addition, I was excited to host the annual Intelligence Community Inspectors General Conference at the National Geospatial-Intelligence Agency headquarters where we welcomed a record number of Intelligence Community (IC) professionals for a day devoted to celebrating their extraordinary achievements and exchanging ideas.

An observation made at each of these events was that intelligence oversight authorities must stay current with the transformative powers of cognitive technologies, particularly artificial intelligence (AI). The United States Intelligence Community expects AI to fundamentally change the way intelligence is produced. A corollary to that expectation is that AI will fundamentally change the way intelligence oversight is conducted. This has led to the growing realization that, for intelligence oversight authorities to remain effective, there will need to be sufficient focus on and investments in oversight of AI in the Intelligence Community.

Maintaining American leadership in AI and shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities have become national security issues. In February 2019, the White House issued Executive Order 13859, *Maintaining American Leadership in Artificial Intelligence*. The President's *National Security Strategy*, the Director of National Intelligence's *National Intelligence Strategy*, and the Secretary of Defense's *National Defense Strategy*, among other high-level strategic guidance documents, also reflect the rising significance of AI as a national security issue.

There are several major AI efforts within the national security enterprise focused on this issue. For example, the Intelligence Community's *AIM Initiative: A Strategy for Augmenting Intelligence using Machines* seeks to use AI technologies to fundamentally change the way intelligence is produced. The Department of Defense's major AI efforts include establishing the Joint Artificial Intelligence Center and spearheading the Defense Advanced Research Projects Agency's AI Next Campaign. These multiple, costly, and complex efforts will pose profound challenges for intelligence oversight authorities.

Fortunately, there is a recognized need and desire for effective oversight of AI. The Executive Order

on AI established as one of its five principles that the "United States must foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application in order to fully realize the potential of AI technologies for the American people." Further, the Director of National Intelligence's 2019 *National Intelligence Strategy* included for the first time as one of its enterprise objectives safeguarding privacy and civil liberties and practicing appropriate transparency to enhance accountability and public trust in all of the IC's efforts.

As Executive Order 13859 and the *National Intelligence Strategy* recognize, Americans have reasonable expectations that the Intelligence Community will act consistently with the rule of law and American values. Reassuring statements that the IC is currently using AI technologies – and will use AI technologies in the future – in ways consistent with the rule of law and American values will not be sufficient. The IC will need to validate those statements for the American people in understandable, timely, objective, and transparent ways.

Although publicly available reports refer to planned investments of hundreds of millions of dollars in AI for the national security enterprise, there is little indication that investments in oversight of AI are currently a high priority. For instance, the Intelligence Community's *AIM Initiative* has the following four primary investment objectives: "Digital Foundation, Data, and Science & Technical Intelligence"; "Adopt Commercial and Open Source Narrow AI Solutions"; "Invest in the Gaps (AI Assurance and Multimodal AI)"; and "Invest in Basic Research Focused on Sensing Making." Although the need to invest in effective oversight of the Intelligence Community's use of AI may be implicit in some of those investment objectives, it is not explicit in any of them.

Investment asymmetry between mission performance and intelligence oversight in AI efforts could lead to an accountability deficit. Intelligence oversight authorities may lack the people, tools, and focus needed to effectively evaluate vulnerabilities in AI technologies as well as the analytic integrity and legality of AI methods, uses, and products. The unintended, but nevertheless likely, outcome of investment asymmetry in the Intelligence Community's AI efforts will be reduced trust in those efforts.

To help prevent this outcome, the ICIG has identified as one of its primary programmatic objectives the improved oversight of AI to prevent an accountability deficit. To achieve this objective, the ICIG has begun an awareness campaign with interested stakeholders. Through the Intelligence Community Inspectors General Forum, which consists of the twelve statutory and administrative Inspectors General with oversight responsibility for an element of the Intelligence Community, the ICIG has brought together thought leaders on AI and related oversight challenges to discuss these issues. The ICIG has also provided informal briefings to the Director of National Intelligence (DNI) and Congressional oversight committee Members and staff. The ICIG, in collaboration with the Forum, will collect and analyze data on the IC's implementation of AI technologies to ensure it is cohesive, comprehensive, and compliant with the rule of law and American values, while continuing to emphasize the need for appropriate investments in oversight of AI.

As the above discussion concerning the rapid proliferation of AI technologies and the need for a corresponding emphasis on oversight illustrates, it is imperative that the ICIG select those oversight initiatives that will improve the efficiency and effectiveness of the most critical areas affecting the Intelligence Community. The ICIG is unique in that it has statutory oversight authority over all of the programs and activities within the responsibility and authority of the DNI. Within that broad authority, the ICIG has substantial discretion in the programmatic reviews that its auditors, investigators, inspectors, and evaluators perform individually or jointly with other oversight authorities.

During this reporting period, the ICIG identified the following five programmatic objectives to focus upon:

1. Improving the Efficiency and Effectiveness of the IC's Cyber Posture, Modern Data Management, and IT Infrastructure;
2. Enhancing Workforce Management;
3. Championing Protected Disclosures;
4. Improving Oversight of Artificial Intelligence; and
5. Integrating the Intelligence Community.

The ICIG formatted this Semiannual Report to align its achievements and activities during the reporting period with these five programmatic objectives. As with any objective, these are subject to revisions based on changes in mission needs, adjustments to priorities, and resources.

In recognition that accomplishing these programmatic objectives requires a whole-of-government approach, the ICIG must express its appreciation for the support provided by the Office of the Director of National Intelligence's leadership and workforce. The ICIG also appreciates the collaboration, coordination, and information sharing provided by the Intelligence Community Inspectors General Forum and its collective workforce. In addition, the ICIG thanks Congress and its staff for their continued professionalism and cooperation, and looks forward to working with them to address the many challenges facing the Intelligence Community.

Finally, as always, I sincerely thank the employees, detailees, and contractors at the ICIG for their integrity, professionalism, and commitment to the ICIG's important mission.

Michael K. Atkinson
Inspector General
April 30, 2019

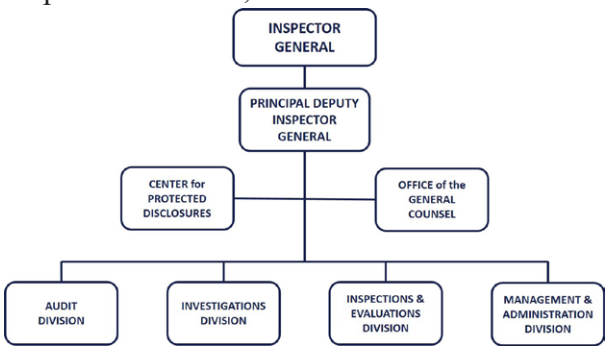
INTRODUCTION

Authority

The Office of the Inspector General of the Intelligence Community (ICIG) was established within the Office of the Director of National Intelligence (ODNI) by the Intelligence Authorization Act for Fiscal Year 2010. The ICIG has the authority to initiate and conduct independent audits, inspections, investigations, and reviews of programs and activities within the responsibility and authority of the Director of National Intelligence (DNI).

Organization

The ICIG's senior management team includes the Inspector General, Principal Deputy Inspector General, General Counsel, four Assistant Inspectors General, and one Center Director.



The principal organizational divisions are Audit, Investigations, Inspections and Evaluations, and Management and Administration. The ICIG employs a highly skilled, committed, and diverse workforce, including permanent employees (cadre), employees from other IC elements on detail to the ICIG (detailees), and contractors. Additional personnel details are listed in the classified Annex of the ICIG's Semiannual Report.

Audit Division

The Audit Division conducts independent and objective audits and reviews of ODNI programs and activities, including those nondiscretionary audits required by law, such as the annual independent evaluation of ODNI's information security program and practices required by the Federal Information Security Modernization Act (FISMA); the annual review of ODNI's compliance with the Improper Payments Elimination and Recovery Act (IPERA); the annual risk assessment of purchase and travel card programs; and the biennial report to Congress – prepared jointly with the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury – on the actions taken to carry out the Cybersecurity Act of 2015. The Audit Division participates with other federal agencies and departments in conducting joint reviews of IC programs and activities.

The Audit Division's activities improve business practices to better support the mission; help reduce fraud, waste, abuse, and mismanagement; and promote the economy,

efficiency, and effectiveness of programs and operations throughout ODNI and the IC. Audit work focuses on information technology and security, acquisition, project management, business practices, human capital, and financial management. Auditors assess whether programs are achieving intended results and whether organizations are complying with laws, regulations, and internal policies in carrying out programs.

The ICIG's audit activities are conducted in accordance with generally accepted government auditing standards.

Investigations Division

The Investigations Division conducts proactive and reactive criminal and administrative investigations into alleged violations of laws and regulations arising from the conduct of Intelligence Community personnel. As part of its work, the Investigations Division identifies and reports internal control weaknesses that could render ODNI or other IC programs and systems vulnerable to exploitation, and which could potentially be leveraged for illicit activity resulting in ill-gotten gains. The Investigations Division also plays a principal role in tracking, monitoring, and investigating unauthorized disclosures of classified information.

During this reporting period, the Investigations Division continued its efforts in investigating cross-Intelligence Community fraud, public corruption, and counterintelligence matters. The Division worked on those matters jointly with the Federal Bureau of Investigation, Intelligence Community Offices of Inspector General, the Defense Criminal Investigative Service, and other federal and local law enforcement agencies, as well as the Fraud Section and Public Integrity Section of the Department of Justice's Criminal Division, the Department of Justice's National Security Division, and the U.S. Attorneys' Offices for the Eastern District of Virginia, the District of Maryland, and the District of Columbia.

The ICIG's investigation activities conform to standards adopted by the Council of the Inspectors General on Integrity and Efficiency.

The ICIG issued one subpoena during this reporting period related to an alleged misuse of government computer systems. The investigation is ongoing.

Inspections and Evaluations Division

The Inspections and Evaluations Division works to improve the performance and integration of ODNI and the broader Intelligence Community. The Division conducts independent assessments of the design, implementation, and results of agency and community operations, programs, and policies. It issues evidence-based findings that are timely, credible, and useful for managers and other stakeholders. The Inspections and Evaluations Division often recommends improvements and identifies when administrative action is necessary.

The Inspections and Evaluations Division's findings typically focus on program, workforce, financial, contracts, and facilities management; information technology security; and integration, coordination, and sharing of information. The Division also highlights best practices and promising approaches.

The ICIG's inspection activities conform to standards adopted by the Council of the Inspectors General on Integrity and Efficiency.

Management and Administration Division

The Management and Administration Division provides full spectrum mission support to the operational divisions of the ICIG. The Division is composed of multidiscipline officers who provide expertise in financial management, human capital and talent management, facilities and logistics management, continuity of operations, administration, classification, Freedom of Information Act requests, information technology, communications, and quality assurance. The Management and Administration Division also delivers executive support to the Intelligence Community Inspectors General Forum and its associated committees.

During this reporting period, ODNI provided the ICIG adequate funding to fulfill its mission. The

budget covered personnel services and general support, including travel, training, equipment, supplies, information technology support, and office automation requirements. As the ICIG assessed IC programs and activities to promote effectiveness, economy, and efficiency, it also continued to examine its own internal operations to develop and implement greater accountability and operational efficiencies.

Office of the General Counsel

The ICIG's Office of the General Counsel (OGC) ensures that the ICIG receives independent and confidential advice and counsel that is without any conflicts of interest in fact or appearance.

It supports the Investigations Division throughout the investigative process by highlighting and providing guidance on potential legal issues meriting additional or redirected investigative efforts.

OGC supports the Audit Division and the Inspections and Evaluations Division by identifying and interpreting key policy, contract, and legal provisions relevant to reported observations, findings, and recommendations. OGC also provides legal and policy guidance, and reviews issues related to ICIG personnel, administration, training, ethics, independence, and budgetary functions.

OGC also serves as the ICIG's Congressional Liaison. During the reporting period, OGC arranged for and participated in ten congressional briefings with the Inspector General and senior ICIG leadership, including briefings to Members of Congress and over 30 bipartisan staff, responded to 8 formal congressional requests, and reported on audit and inspection reviews in response to congressional interest and legislative mandates. Engagements during this reporting period included:

- Meetings with House Permanent Subcommittee on Intelligence Chairman Adam Schiff and Ranking Member Devin Nunes to discuss several important initiatives within the ICIG, including the ICIG's Fiscal Year 2020 Annual Work Plan.
- Meetings with House Permanent Subcommittee on Intelligence and Senate Select Committee on Intelligence staff to discuss the ICIG's Annual Work Plans for Fiscal Years 2019 and 2020, recently completed ICIG reports, and other important ICIG initiatives.
- Responding to Member requests regarding constituent issues before the ICIG.
- Cooperating with the Government Accountability Office in its review of whistleblower protections in the IC.
- In person meetings, letters, and other correspondence with staff from the Senate Judiciary Committee, Senate Committee on Homeland Security and Governmental Affairs, and Senate Select Committee on Intelligence to respond to the committees' questions surrounding media reports related to the ICIG's review of emails obtained from former Secretary Hillary Clinton's non-government server as part of coordinating the IC's classification review process.

Center for Protected Disclosures

The Center for Protected Disclosures (the Center) processes whistleblower reports and supports whistleblower protections.

The Center includes the ICIG's Hotline Program, which processes allegations of fraud, waste, and abuse in the programs and activities subject to the ICIG's jurisdiction. The Hotline Program also processes allegations of "Urgent Concerns" filed pursuant to the Intelligence Community Whistleblower Protection Act.

The Center also includes a Source Support Program Manager who provides guidance to whistleblowers, as well as community outreach on whistleblower protections and training.

Finally, the Center administers requests by employees and contractors in the Intelligence Community for the ICIG to review their allegations of reprisal under Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information* (PPD-19).

INDEPENDENCE

The Inspector General of the Intelligence Community is nominated by the President and confirmed by, and with the advice and consent of, the United States Senate. The Office of the Inspector General of the Intelligence Community bases its findings and conclusions on independent and objective analysis of the facts and evidence that are revealed through exhaustive audits, investigations, inspections, and programmatic reviews. During this reporting period, the ICIG had full and direct access to all information relevant to perform its duties.

ICIG MISSION

The Inspector General of the Intelligence Community's mission is to provide independent and objective oversight of the programs and activities within the responsibility and authority of the Director of National Intelligence, and to lead and coordinate the efforts of the Intelligence Community Inspectors General Forum.

ICIG STRATEGIC GOAL

The Inspector General of the Intelligence Community's goal is to have a positive and enduring impact throughout the Intelligence Community, to lead and coordinate the efforts of an integrated Intelligence Community Inspectors General Forum, and to enhance the ability of the United States Intelligence Community to meet national security needs while respecting our nation's laws and reflecting its values.

ICIG CORE VALUES

INTEGRITY

INDEPENDENCE

COMMITMENT

DIVERSITY

TRANSPARENCY

THE INSPECTOR GENERAL COMMUNITY

Last year marked the 40th anniversary of the Inspector General Act of 1978. President Jimmy Carter signed the Act, and described the new statutory Inspectors General as "perhaps the most important new tools in the fight against fraud." The ICIG, one of 74 Inspectors General (IGs) collectively overseeing the operations of nearly every aspect of the federal government, looks forward to continuing to work with the Council of Inspectors General on Integrity and Efficiency (CIGIE) on important issues that significantly affect productivity, transparency, and accountability throughout the federal government.

Oversight.gov

Oversight.gov provides a "one stop shop" to follow the ongoing oversight work of all Offices of Inspectors General (OIGs) that publicly post reports. CIGIE manages the website on behalf of the Federal Inspector General community. The ICIG, like other OIGs, will continue to post reports to its own website as well as to Oversight.gov to afford users the benefits of the website's search and retrieval features. Oversight.gov allows users to sort, search, and filter the site's database of public reports from all CIGIE member OIGs to find reports of interest. In addition, the site features a user-friendly map that allows users to find reports based on geographic location, and contact information for each OIG's hotline. Users can receive notifications when new reports are added to the site by following @Oversightgov, CIGIE's Twitter account.

ICIG OBJECTIVES, RESULTS, AND ONGOING PROJECTS

In January 2019, the ICIG announced the first-time public release of its Annual Work Plan. The Plan identifies the ICIG's congressionally-directed mandatory and discretionary programmatic reviews for the upcoming year. Once used strictly as an internal coordination document to identify and prioritize all of the ICIG's reviews, the Plan is now accessible to the Director of National Intelligence, all 17 U.S. Intelligence Community elements, congressional members and staff, and the general public on the ICIG's webpage at www.dni.gov.

The ICIG is currently preparing its Annual Work Plan for Fiscal Year 2020, which will be released in September 2019. To identify its discretionary programmatic reviews, the ICIG has reviewed several milestone reports prepared by the IC and other stakeholders. These reports include: the *2019 U.S. National Intelligence Strategy*; the *Consolidated Intelligence Guidance for Fiscal Years 2020-2024*; the I*C2025 Vision and Foundational Priorities*, particularly the six Intelligence Community Strategic Initiatives identified by the IC Deputies Executive Committee; the Office of the Inspector General's Management and Performance Challenges reports issued in 2018 by the ICIG, as well as the Inspectors General for the Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency; the Government Accountability Office's High Risk Series reports; and the Council of Inspectors General on Integrity and Efficiency FY 2018 report, *Top Management and Performance Challenges Facing Multiple Federal Agencies*.

As projects are developed for FY 2020, the ICIG has also sought input from the Intelligence Community Inspectors General Forum Members, congressional oversight committee Members and staff, and other IC leaders.

Based on its review of the milestone reports and the information obtained from the other sources enumerated above, the ICIG identified the following five programmatic objectives to focus upon:

1. Improving the Efficiency and Effectiveness of the Intelligence Community's Cyber Posture, Modern Data Management, and IT Infrastructure;
2. Enhancing Workforce Management;
3. Championing Protected Disclosures;
4. Improving Oversight of Artificial Intelligence; and
5. Integrating the Intelligence Community.

1 Improving the Efficiency and Effectiveness of the IC's Cyber Posture, Modern Data Management, and IT Infrastructure

The Intelligence Community has identified cybersecurity as one of its most important priorities, as reflected in the 2019 *National Intelligence Strategy*, the DNI's *IC2025 Vision and Foundational Priorities*, the 2018 *Management and Performance Challenges for the Office of the Director of National Intelligence (ODNI)*, and budget requests spanning multiple fiscal years. Ongoing and future projects selected by the ICIG will review and evaluate the effectiveness of ODNI's information security and the cohesiveness of cyber and information technology (IT) integration across the Intelligence Community.

Fiscal Year 2018 Independent Evaluation of the Office of the Director of National Intelligence's Information Security Program and Practices, as Required by the Federal Information Security Modernization Act of 2014 (FISMA)

During the reporting period, the Audit Division completed an evaluation to assess the effectiveness and maturity of ODNI's information security program and practices for Fiscal Year 2018, as required by the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires an annual independent evaluation of federal agencies' information security programs and practices. The ICIG performed this evaluation using the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* developed by the Office of Management and Budget, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency. The ICIG issued 11 recommendations for improving ODNI's information security program and practices.

In addition, the ICIG collected the Executive Summaries and metric results from the Intelligence Community elements' FY 2018 FISMA reports and provided them to the Office of Management and Budget. In accordance with the Federal Information Security Modernization Act, the Director of the Office of Management and Budget is responsible for summarizing FISMA reports from the Intelligence Community elements and submitting an annual report to Congress on the effectiveness of information security policies and practices relating to national security systems.

Additional details are listed in the classified Annex of the ICIG's Semiannual Report.

Management of Privileged Users

In November 2018, the ICIG began an audit of ODNI's management of privileged users of ODNI systems. Privileged users are authorized and trusted to perform security-related functions for information systems that ordinary users are not authorized to perform. The misuse of a person's privileged user status increases the risk for compromising the confidentiality, integrity, and availability of ODNI information systems. The objective of the audit is to determine whether controls for managing information system privileged users are effective. The audit is ongoing.

Cybersecurity Information Sharing Act of 2015

In early 2019, the ICIG initiated an audit of ODNI's implementation of the Cybersecurity Information Sharing Act of 2015 (CISA). As required by § 107(b), CISA, *Oversight of Government Activities—Biennial Report on Compliance*, the Inspectors General of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury, and

the Intelligence Community, in consultation with the Council of Inspectors General on Financial Oversight, must jointly submit an interagency report to Congress. The results of the audit will be reported to ODNI and included in the interagency report.

This audit will evaluate, among other things, the sufficiency of ODNI's policies and procedures related to sharing cyber threat indicators within the federal government; proper classification of cyber threat indicators or defensive measures; actions taken by the federal government based on shared cyber threat indicators or defensive measures; and barriers to sharing information about cyber threat indicators and defensive measures. The audit of ODNI and the joint project are ongoing.

Cyber Threat Intelligence Integration Center

In January 2019, the Inspections and Evaluations Division completed an inspection of ODNI's Cyber Threat Intelligence Integration Center (CTIIC). The inspection focused on CTIIC's mission performance, management effectiveness, resource management, and enterprise oversight covering the period of February 2016 through February 2018. The inspection revealed the following:

- The functions of CTIIC and ODNI's National Intelligence Manager for Cyber are not fully consolidated. The National Intelligence Manager for Cyber is the DNI's Intelligence Community lead for cyber intelligence issues, and is responsible for the integration of the IC's collection and analysis of cyber issues. The ICIG identified the legal ramifications of, and its recommendations related to, this challenge in the classified Annex of the ICIG's Semiannual Report.
- The staffing practices by CTIIC and ODNI impeded the ICIG's ability to validate adherence to position limits. The ICIG's report identified discrepancies in certain personnel records and ODNI's use of an ambiguous term to identify staffing placement as impediments to the ICIG's ability to verify CTIIC's actual staffing number and compliance with staffing limits. The ICIG identified the legal and policy ramifications of, as well as its recommendations related to this challenge in the classified Annex of the ICIG's Semiannual Report.
- The ratio of CTIIC's Joint Duty Assignment personnel does not align with ODNI's *Strategic Human Capital Plan 2012-2017*, which identified a goal of a 50:50 ratio of cadre (or permanent) to joint duty assignment (or detailee) personnel.
- The mission for CTIIC's Threat Opportunity Section requires clarifying guidance. In order to execute its mission responsibilities, CTIIC's leadership established three separate sections: the Current Intelligence Section; the Analysis Integration Section; and the Threat Opportunity Section. The Threat Opportunity Section is charged with facilitating and supporting the United States Government's responses to cyber threats by working with policy and operational stakeholders, particularly staff on the National Security Council, to identify and integrate the range of response options, along with accompanying considerations policymakers require to determine courses of action. The ICIG recommended, among other things, that CTIIC develop and implement a comprehensive plan to maximize the Threat Opportunity Section's mission effectiveness, including the ability to measure product deliverables to the National Security Council staff or interagency stakeholders.
- The ICIG's report also commended CTIIC for its Cyber Threat Intelligence Summary, which provides threat reporting, including context, commentary, and Intelligence Community/United States Government actions, and highlights intelligence and community analysis from around the IC.

Additional details are listed in the classified Annex of the ICIG's Semiannual Report.

ODNI Oversight of IC Major System Acquisition Cybersecurity Risks

In November 2018, the ICIG launched a review to evaluate the efficiency and effectiveness of existing authorities, policies, and processes applicable to ODNI's oversight of cybersecurity risks in Intelligence Community Major System Acquisitions. A major system is a combination of elements that will function together to produce the capabilities required to fulfill a mission need. In addition, 41 U.S.C. § 109 establishes dollar thresholds for major systems. The Intelligence Reform and Terrorism Prevention Act empowered the DNI with milestone decision authority for Intelligence Community Major System Acquisitions. In accordance with Intelligence Community Directive 801, *Acquisition*, ODNI conducts acquisition oversight of National Intelligence Program-funded Major System Acquisitions. The ICIG review was initiated in response to the criticality of cybersecurity and the necessity to address it throughout the acquisition lifecycle. This review is ongoing.

2 Enhancing Workforce Management

The ICIG established this objective based on the *Right, Trusted, Agile Workforce* foundational priority as identified in the Director of National Intelligence's *IC2025 Vision and Foundational Priorities* and the People enterprise objective outlined in the *National Intelligence Strategy.* The projects highlighted below contribute to this priority by ensuring that the workforce has the necessary tools to carry out the mission of the Intelligence Community.

Security Clearance Working Group

An effective and efficient government-wide personnel security clearance process is essential, among other things, to minimize the risk of unauthorized disclosures of classified information. Further, an effective security clearance process helps ensure that security relevant information is identified and assessed in a timely manner to enable agencies to recruit and retain qualified and trusted employees and contractors. Executive Order (EO) 13467 assigns the Director of National Intelligence responsibility, as the Security Executive Agent, for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information and eligibility to hold a sensitive position.

Since the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 and EO 13467, the DNI, as Security Executive Agent, has instituted a variety of reform efforts designed to improve background investigation and adjudication timeliness, and improve the quality of information used to make security clearance decisions, compile system-wide metrics, and assess and oversee personnel security program implementation across the Executive branch.

For example, the FY 2016 Omnibus Appropriation, H.R. 2029-673, specifically required the DNI to develop a plan to eliminate the backlog of periodic reviews. In response to a December 2012 ICIG audit report, *IC Security Clearance Reciprocity*, the DNI signed Security Executive Agent Directive 7, *Reciprocity of Background Investigations and National Security Adjudications*, in November 2018. The directive establishes requirements, including timeliness, for reciprocal acceptance of background investigations and national security adjudications for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. At the direction of the Security Executive Agent, ODNI's National Counterintelligence and Security Center issued guidance in January 2019 on metrics for reciprocal security clearances, and quarterly and annual reporting requirements. Despite these reform efforts, processing of security clearances within the IC has been a long standing and continuing challenge. Last year, the Government Accountability Office (GAO) added the government-wide personnel security clearance process to its High-Risk List. Through a number of audits, GAO identified challenges related to the timely processing of security clearances, the need for implementing key initiatives of the security clearance reform effort, and the absence of performance measures related to the quality of background investigations. Timely and consistent administration of security clearance processes would facilitate filling critical national security positions in an expeditious manner.

In recognition of this continuing and critical challenge, the ICIG, in collaboration with other Intelligence Community Inspectors General Forum members, intends to examine the authorities, policies, and procedures vested in the DNI, as the Security Executive Agent, to determine their adequacy, and review organizations' efficiency and effectiveness in implementing the DNI's requirements. An ICIG working group, consisting of Audit and Inspections and Evaluations staff, issued a

memorandum in November 2018 announcing the commencement of preliminary project research. The working group has engaged with multiple entities, including ODNI's National Counterintelligence and Security Center, which is responsible for managing the DNI's Security Executive Agent authorities and responsibilities. The ICIG is currently analyzing data to determine the scope and criteria for a forthcoming evaluation.

Intelligence Community's Foreign Language Program

In February 2019, the ICIG commenced an evaluation of the effectiveness of the Intelligence Community Foreign Language Program (ICFLP) in achieving IC mission objectives. The Program was authorized via the Intelligence Authorization Act of FY 2005, with the mission "to improve the education of IC personnel in foreign languages critical in meeting the long-term intelligence needs of the United States." The DNI implemented this mandate through Intelligence Community Directive 630, *Intelligence Community Foreign Language Capability*, establishing "an integrated approach to develop, maintain, and improve foreign language capabilities across the IC." This evaluation marks the first Inspector General review of the ICFLP since its inception. It focuses on enterprise management in the areas of governance effectiveness, outcomes against ICFLP strategic objectives, and advocacy for budgetary resources and linking allocations to impacts. The goal of this evaluation is to inform ODNI leadership decisions related to the future of the ICFLP within ODNI's current organizational structure and IC2025 Vision initiatives.

Improper Payments Elimination and Recovery Act

During the reporting period, the ICIG's Audit Division began a review of ODNI's compliance with the Improper Payments Elimination and Recovery Act (IPERA). IPERA requires each federal agency to perform a review of programs and activities to assess whether the risk of improper payment is significant. IPERA also requires each Inspector General to assess and submit a report on whether the agency complied with the requirements of IPERA. This review will evaluate the completeness, accuracy, and validity of ODNI's disclosures on improper payments, as reported in ODNI's Agency Financial Report for FY 2018.

Conference Spending

The ICIG's Audit Division began an audit of ODNI's conference spending in January 2019. The federal government has a responsibility to act as a careful steward of taxpayer dollars, ensuring that federal funds are cost effective, used for appropriate purposes, and important to an agency's core mission. The objective of this audit is to determine whether ODNI-sponsored conferences were appropriately justified, approved, funded, and reported in accordance with applicable federal laws and ODNI's policies and procedures.

ODNI's Charge Card Program

The ICIG's Audit Division is continuing its review of ODNI's charge card program for FY 2016 and 2017. The objective of the audit is to determine whether internal controls are sufficient to prevent and detect illegal, improper, and erroneous use of government travel cards.

ODNI Measures in Substantiating Claims of Postsecondary Education Post Entry-on-Duty

In November 2018, the Inspections and Evaluations Division initiated a review of measures to substantiate ODNI employees' postsecondary education claims made after their Entry-on-Duty as ODNI employees. The review focuses on policies and procedures related to the validation of declarations set forth in official government documentation, potential consequences of weak verification controls, and the magnitude of falsified qualifications of personnel performing national security functions. The review is ongoing.

Labor Mischarging

The Investigations Division completed a number of investigations during the reporting period, including substantiating allegations of fraudulent activity that resulted in significant losses of Government funds. For example, the Investigations Division substantiated labor mischarging by an ODNI contract employee who falsely billed the government for almost 1600 hours that the contractor had not actually worked, resulting in an estimated loss to the Government of over $200,000. The contractor's clearance was terminated and ODNI has initiated collection procedures. In addition, local law enforcement authorities filed criminal charges against the former contractor, and those charges remain pending.

3 Championing Protected Disclosures

Intelligence Community employees and contractors collect and analyze information to develop the most accurate and insightful intelligence possible on external threats. These Intelligence professionals serve in a classified work environment in which information about intelligence programs and activities is not available for public review, which makes their duty to lawfully disclose information – or blow the whistle – regarding potential wrongdoing, including fraud, waste, abuse, and corruption, that much more critical to the oversight process.

Whistleblowing is the lawful disclosure of information a person reasonably believes evidences wrongdoing to an authorized recipient. It is the mechanism to relay the right information to the right people to counter wrongdoing and promote the proper, effective, and efficient performance of the Intelligence Community's mission. Whistleblowing in the IC is extremely important as it ensures that personnel can "say something" when they "see something" through formal reporting procedures without harming national security and without retaliation.

After seeking input from key stakeholders, including Congress, the Intelligence Community Inspectors General Forum, and advocacy groups during the last reporting period, the ICIG designed and established the Center for Protected Disclosures (the Center). The Center covers three functional areas critical for whistleblowers in the Intelligence Community.

First, the Center receives and processes whistleblower complaints through the ICIG's Hotline program. The Hotline program receives whistleblower complaints and concerns through public and secure telephone numbers and website addresses as well as walk-in meetings at the ICIG's main office in Reston, Virginia, and its satellite offices in McLean, Virginia, and Bethesda, Maryland. During the reporting period, the ICIG eliminated its backlog of hotline complaints dating back several years. The Hotline program also receives and processes allegations of "urgent concerns" disclosed pursuant to the Intelligence Community Whistleblower Protection Act (ICWPA). The ICWPA established a process to ensure that the Director of National Intelligence, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence receive disclosures of potential flagrant problems, abuses, violations of law or executive order, or deficiencies relating to the funding, administration, or operation of an intelligence activity. The Center tracks all ICWPA disclosures, ensures review of materials for classified information, and coordinates disclosures with other Inspectors General for appropriate review and disposition. During the reporting period, the ICIG transmitted four ICWPA disclosures to the DNI, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence.

To increase the effectiveness of the ICIG's Hotline program, the ICIG hosted the second Intelligence Community Hotline Working Group to discuss challenges and share best practices with IC Hotline partners. Participants included Hotline managers from the Offices of Inspector General of the Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, and the National Reconnaissance Office. Participants discussed hotline triage practices, trends and metrics, information technology management and collection tools, and classification challenges. The Hotline Working Group intends to meet semiannually to further share procedures and lessons learned. In addition, Hotline staff are working with ICIG Counsel and Management and Administration staff to improve intake forms and make the processes more efficient both for Hotline users and ICIG staff.

Second, the Center provides community outreach and guidance to individuals seeking more information about the options and protections

afforded to individuals who may wish to make a protected disclosure to the ICIG and/or Congress, or who believe they have suffered reprisal because they made a protected disclosure. The ICIG also conducts outreach and training activities within ODNI to ensure management stakeholders present accurate and consistent whistleblowing education.

The ICIG launched redesigned and updated versions of its secure and unclassified websites, which provide visitors with more information and easier site navigation. These site improvements support the ICIG's objectives to increase transparency into the ICIG's oversight activities; raise workforce awareness about duties, processes, and protections associated with reporting fraud, waste, and abuse; and enhance communication, coordination, and collaboration among key stakeholders.

Third, the Center administers requests by employees and contractors in the Intelligence Community for the ICIG to review their allegations of reprisal under Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information* (PPD-19). PPD-19 protects employees serving in the IC or who are eligible for access to classified information by prohibiting reprisal for reporting fraud, waste, and abuse, while protecting classified national security information. The ICIG has unique and important responsibilities under PPD-19, including the administration of external review processes to examine allegations of whistleblower reprisal. Under PPD-19, an individual who believes they suffered reprisal for making a protected disclosure is required to exhaust their agency's applicable review process for whistleblower reprisal allegations before requesting an ICIG external review. Upon exhaustion of those processes and a request for review, PPD-19 permits the ICIG to exercise its discretion to convene an External Review Panel (ERP) to conduct a review of the agency's determination.

During this reporting period, three ERP requests received during the last reporting period were denied and closed following initial assessment and review of materials submitted by both the complainants and their employing agencies. The ICIG received five new ERP requests during the current reporting period, one of which was denied and closed following initial assessment and review of materials submitted by both the complainant and the complainant's employing agency. The ICIG is conducting initial assessments of the remaining four new ERP requests.

Building on work begun during the previous reporting period, the ICIG's Office of the General Counsel reviewed and evaluated historical ERP files. As a result of those reviews and evaluations, the ICIG substantially reduced its backlog of pending cases while continuing to improve and streamline ERP processes to identify the policies, procedures, and tracking mechanisms necessary for efficient and timely processing of new cases. Three historical cases remain under review. In further support of the Center, the ICIG's Office of the General Counsel also undertook an evaluation and revision to the procedures governing ERPs, including the development of standards of review.

Congressional Notifications

In November 2018, in response to a letter from former Senate Judiciary Committee Chairman Senator Charles Grassley, the ICIG delivered to the Senate Judiciary Committee, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence, two declassified Congressional Notifications on whistleblower communications prepared by the ICIG in 2014. Now unclassified and re-marked for public release, the Congressional Notifications alerted the Director of National Intelligence and the Congressional intelligence oversight committees that whistleblower-related communications had been accessed through routine Central Intelligence Agency counterintelligence monitoring.

"Inspector General Atkinson and his office were responsive and engaging on something that appeared intractable if small. I thank him for his work."
– Chairman Charles Grassley

The ICIG earned accolades from Senator Grassley for facilitating the declassification and release of the documents within two weeks of his October 15, 2018 request.

Intelligence Community Directive 701

There is a need to clearly distinguish whistleblowers from individuals who make unauthorized disclosures by taking it upon themselves to decide what classified information should be disclosed to the public. Whistleblowers make use of formal reporting procedures that will provide protection to the classified information and to the whistleblower. Any disclosure of classified information falling outside of these established procedures constitutes an unauthorized disclosure – not protected whistleblowing – and falls into the realm of insider threat behavior. Unauthorized disclosures put sensitive operations and intelligence sources and methods at risk. In addition, failing to effectively address unauthorized disclosures reduces the incentive for the IC's workforce to use formal reporting procedures to make protected disclosures to report allegations of fraud, waste, or abuse involving classified information.

The ICIG's Investigations Division continued to take steps during the review period to confirm appropriate IC implementation of Intelligence Community Directive 701, *Unauthorized Disclosures of Classified National Security Information* (ICD 701). These efforts included numerous outreach and liaison events focused on discussing the status of ICD 701 reporting programs, identifying the responsible components within each agency, formalizing reporting processes to ensure appropriate notifications in a timely fashion, and engaging in benchmarking efforts to identify obstacles to appropriate implementation. Multiple stakeholders, including IC elements and law enforcement agencies, participated in these outreach events to share their expertise and institutional knowledge.

The Investigations Division spearheaded an initiative, via the creation of an ICIG-led task force, to review IC elements' internal investigations, ensuring appropriate protective and corrective actions are taken against individuals who make unauthorized disclosures of classified information, and to ensure those elements' internal investigations are not closed prematurely. Additionally, the ICIG collaborating with ODNI's Policy and Strategy Group to create multiple ICD 701 resources (Fact Sheets, Frequently Asked Questions, and internal workflow graphics), for release to the IC's workforce and the public.

The ICIG has also met with the President's Intelligence Advisory Board to discuss ways to reduce unauthorized disclosures and provide greater protections to the IC's most sensitive information. In December 2018, Inspector General Atkinson along with the Inspectors General from the Department of Defense, Department of Justice, Defense Intelligence Agency, National Security Agency, and the Central Intelligence Agency met with the President's Intelligence Advisory Board to discuss the role of Inspectors General in providing end-to-end accountability for protecting classified information. In addition, in March 2019, Inspector General Atkinson and the Inspector General of the Department of Justice met a second time with the President's Intelligence Advisory Board to discuss, among other things, legislative approaches to reduce unauthorized disclosures, including testimonial subpoena authority for OIGs to compel non-agency individuals to provide testimony in administrative investigations.

Establishment of "Ask the Inspector General" Drop Box

In March 2019, the ICIG stationed drop boxes in common areas across ODNI facilities to provide a convenient way for employees to bring to the ICIG's attention allegations of fraud, waste, abuse, and mismanagement. The drop boxes are an extension of the ICIG's existing Hotline program and intake process and help ICIG auditors, inspectors, and investigators uncover potential problems early and address them before they get worse. Employees and contractors are encouraged to complete and submit intake forms located with the boxes and are also available online. ICIG staff collect submissions on a regular basis.


You joined to make a difference.
Report for the same reason.
ICIG
Report suspected fraud, waste, and abuse.
Office of the Inspector General of the Intelligence Community
It's always the right time to do the right thing.
Be part of the solution.

4 Improving Oversight of Artificial Intelligence

Data is one of the cornerstones of work conducted by OIGs. Whether text dense criteria documents or structured databases of transactional or financial data, OIGs face mounting challenges in finding, sorting, and analyzing vast amounts of data. Artificial Intelligence was selected as an objective for review due to the presence it has played in multiple documents and reports published by ODNI. In the *Augmenting Intelligence using Machines (AIM) Initiative*, Director Coats identified artificial intelligence as a vehicle to increase mission capability and enhance data interpretation throughout the IC.

The ICIG is coordinating Intelligence Community OIGs' efforts to recognize the opportunities and challenges presented by machine learning and artificial intelligence. In light of the DNI's *IC2025 Vision* and *Foundational Priorities' Augmenting Intelligence using Machines (AIM) Initiative*, the ICIG is taking action to build general awareness and common understanding among intelligence oversight authorities.

In early March 2019, ODNI's lead for the AIM initiative presented an overview to the Intelligence Community Inspectors General Forum at its quarterly meeting. Later in the month, as part of the Annual Intelligence Community Inspectors General Conference, over 200 representatives from 25 Executive Branch elements attended a breakout session titled, *Making Better Use of Data: Automation, Analytics, and AI*. In the session, a panel with members from the National Reconnaissance Office and Defense Intelligence Agency Offices of Inspectors General, along with the Intelligence Community's Chief Data Officer, explained the differences between automation, analysis, analytics, and AI; discussed the role of each of these methods as OIGs manage and use data; and identified steps OIGs can take to improve their ability to leverage data to accomplish their oversight missions. The goal of the session was to provide a common point of reference for follow-on discussions within and among IC OIGs.

Future activities include:

- Establishing a community of interest under the auspices of the Intelligence Community Inspectors General Forum to consider how AIM could enable individual, joint, or collective IC OIG's efforts in performing internal functions;
- Exploring how OIGs might enhance their individual and collective understanding of this transformative emerging field and thus their capabilities to audit, investigate, inspect, and evaluate implementation of the AIM initiative within IC elements and across the IC Enterprise;
- Evaluating investments in oversight of AI in terms of personnel, training, and technology;
- Hosting information exchanges and collaboration with the Council of Inspectors General on Integrity and Efficiency's Data Analytics Working Group; and
- Engaging with the Council of Inspectors General on Integrity and Efficiency Training Institute to establish a range of education and training resources to develop OIGs' expertise in addressing data and AI-related issues and topics.

5 Integrating the Intelligence Community

The ICIG identified integrating the Intelligence Community as a programmatic objective because it is fundamental to ODNI's mission and national security. When created by the Intelligence Reform and Terrorism Prevention Act of 2004, ODNI was tasked with improving information sharing and ensuring integration across the IC. Strategic prioritization, coordination, and deconfliction of IC collection, analysis, production, and dissemination of national intelligence are essential to optimizing IC resource management, decision making, and accomplishing ODNI's mission. ODNI's *Integrated Mission Strategy for 2019-2023* and the *National Intelligence Strategy* identified developing collaborative collection and analysis capabilities, as well as sharing and safeguarding information, as enduring challenges.

The Five Eyes Intelligence Oversight and Review Council

One significant way the ICIG works to improve the integration of the IC on an international level is through the Five Eyes Intelligence Oversight and Review Council (FIOR Council). The FIOR Council was created in the spirit of the existing Five Eyes partnership, the intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States. The Council is composed of the following non-political intelligence oversight, review, and security entities of the Five Eyes countries: the Office of the Inspector-General of Intelligence and Security of Australia; the Office of the Communications Security Establishment Commissioner and the Security and Intelligence Review Committee of Canada; the Commissioner of Intelligence Warrants and the Office of the Inspector-General of Intelligence and Security of New Zealand; the Investigatory Powers Commissioner's Office of the United Kingdom; and the Office of the Inspector General of the Intelligence Community of the United States.

FIOR Council members exchange views on subjects of mutual interest and concern; compare best practices in review and oversight methodology; explore areas where cooperation on reviews and the sharing of results is permitted; encourage transparency to the largest extent possible to enhance public trust; and maintain contact with political offices, oversight and review committees, and non-Five Eyes countries as appropriate. The Council meets annually, with the location rotating among the Council participants.

Inspector General of the Intelligence Community Participates in Five Eyes Intelligence Oversight and Review Council Conference in Canberra, Australia

In October 2018, the ICIG led the U.S. delegation to the annual meeting of the FIOR Council in Canberra, Australia, which was hosted by The Honorable Margaret Stone, the Inspector-General of the Office of the Inspector-General of Intelligence and Security of Australia. The annual meeting focused on a theme of independence and keeping up with technology. The U.S. delegation to the 2018 conference included the Inspectors General from the U.S. Department of Justice, National Reconnaissance Office, and National Security Agency.

During the annual meeting, the delegations exchanged information and views on developments in their respective jurisdictions over the past year, the importance of and challenges

associated with maintaining institutional independence, keeping up with technology, and best practices to protect whistleblowers and combat unauthorized disclosures of national security information. The conference included a keynote address from Alexander W. Joel, the Chief of ODNI's Office of Civil Liberties, Privacy and Transparency, to the Council members and senior officials in the Australian and New Zealand intelligence services, concerning the importance of encouraging transparency to the largest extent possible to enhance public trust. The FIOR Council members also continued to explore areas during the conference where they could cooperate on reviews and share results, where appropriate.

At the conclusion of the annual meeting, the Council members agreed that the Investigatory Powers Commissioner's Office of the United Kingdom would host next year's annual conference, which will be held in London in October 2019.

The Inspector General of the Intelligence Community Hosts the Canadian Intelligence Oversight Delegation

In October 2018, the ICIG, along with the IGs from the United States Department of Justice, National Reconnaissance Office, and National Security Agency, hosted an information exchange with their Canadian counterparts from the Security Intelligence Review Committee, a member of the FIOR Council, which is an independent Canadian government agency responsible for reviewing the operations of Canada's security service, the Canadian Intelligence Security Service. The information exchange preceded the annual meeting of the FIOR Council.

European Union-United States Privacy Shield

In October 2018, the Inspector General of the Intelligence Community joined other senior officials from the United States Government to participate in the second annual review of the European Union – United States (EU-U.S.) Privacy Shield framework before the European Commission and European data protection authorities in Brussels, Belgium. Operational since August 1, 2016, the Privacy Shield framework regulates and protects personal data transferred from the European Union to the United States for commercial purposes. The Privacy Shield framework's terms are required to be reviewed every year.

The European Commission recently published its second annual review of the EU-U.S. Privacy Shield framework. On the basis of its factual findings, the Commission acknowledged that the Privacy Shield framework has been "generally a success" and that the United States continues to ensure "an adequate level of protection for personal data" transferred under the Privacy Shield from the EU to organizations in the United States.

Both the published report and the accompanying staff working document highlighted the remarks made by the Inspector General of the Intelligence Community before the European Commission and the European data protection authorities in Brussels. The published report's section on independent oversight highlighted the ICIG's remarks on the important oversight role performed by Inspectors General throughout the United States Government and by the ICIG, in particular, saying it confirmed the findings of the first annual review. The report and the accompanying staff working document also emphasized the ICIG's remarks that any referral from the Privacy Shield Ombudsperson would receive his "*serious, timely, and effective attention*."

In late January 2019, the White House nominated Mr. Keith Krach to be the Undersecretary of State for Economic Growth, Energy, and the Environment. The Undersecretary also serves as the Ombudsman for the EU-U.S. Privacy Shield framework to ensure that complaints concerning access to personal data by U.S. authorities are addressed appropriately.

Management Challenges Facing the ODNI

The Reports Consolidation Act of 2000 requires that the Inspector General of the Intelligence Community identify the most serious management and performance challenges facing the Office of the Director of National Intelligence. In September 2018, the ICIG issued its statement outlining what it considered to be the most significant challenges facing ODNI. These were:

- Enhancing Intelligence Community Coordination, Integration, and Information Sharing;
- Reforming the Security Clearance Process;
- Producing Auditable Financial Statements;
- Strengthening Information Security; and
- Improving Management of ODNI's Workforce.

Additional details are listed in the classified Annex of the ICIG's Semiannual Report.

Management Challenges Facing the Intelligence Community

In order to outline the top challenges facing the IC and make the findings more transparent, the ICIG shared its September 2018 Management Challenges Report with the Inspectors General from the Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency. As required by law, the Inspectors General of those elements identified the most significant challenges for their respective agencies.

This year, for the first time, the ICIG worked together with those IGs to identify the most significant shared challenges, which were aggregated in a single, or Capstone Report. This Report is consistent with the ICIG's mission to keep the DNI and Congressional Intelligence Committees fully informed about the problems and deficiencies related to the administration of activities and programs within the responsibility and authority of the DNI, as well as the necessity for, and progress of, corrective actions.

Among others, the Capstone Report identified challenges related to:

- Strengthening Information System Security and Management;
- Countering Insider Threats;
- Strengthening Acquisition and Contract Management;
- Producing Auditable Financial Statements;
- Improving Workforce Management; and
- Reforming the Security Clearance Process.

Additional details are listed in the classified Annex of the ICIG's Semiannual Report.

Intelligence Information Sharing Working Group

Intelligence Community Directives require each agency to share information to the fullest extent possible. Since September 11, 2001, the President, Congress, independent commissions, and think tanks have all placed greater emphasis on the need for information sharing within the Intelligence Community. The DNI has overall responsibility for providing oversight and financial and program management of Intelligence Community information integration efforts. However, no oversight reviews of information sharing or information integration efforts have been conducted to date. Last year, the Inspections Committee of the Intelligence Community Inspectors General Forum launched an Intelligence Information Sharing working group to evaluate the merits of a proposed joint review. The working group is developing recommendations for the scope, objectives, and

criteria for a joint review of the implementation of the DNI's information sharing authorities and responsibilities.

Inspections and Evaluations Navigator Training Tool

The Inspections and Evaluations Division continued to partner with the Council of Inspectors General on Integrity and Efficiency (CIGIE) to develop content for the Inspections and Evaluations Navigator training tool pilot project. The pilot Inspections and Evaluations Navigator is the cornerstone of the CIGIE Training Institute's initial venture into web-based instruction. When fielded and integrated with CIGIE's new performance-focused training design, leading-edge learning, covering Inspections and Evaluations policy, procedure, and workflow will be accessible to OIG staff anywhere. It will augment and replace the current, formal, in-person classroom delivery model. Over time, CIGIE plans to develop and field similar training and performance-enhancing support systems for the investigation and audit communities.

The ICIG's interest in the project stems from the dual goals of leveraging Inspections and Evaluations Navigator to enhance its own on-boarding training and operations support needs, and serving as the IC's champion for making it available on classified networks to members of the Intelligence Community Inspectors General Forum as a service to address common needs.

Collaboration within the Audit Community

The ICIG Assistant Inspector General for Audit (AIG/Audit) meets bimonthly with the AIGs/Audit of the Central Intelligence Agency, National Reconnaissance Office, National Security Agency, Defense Intelligence Agency, and the National Geospatial-Intelligence Agency. The meetings provide the opportunity for the AIGs/Audit to discuss common challenges, e.g., recruiting top talent, developing auditor promotion criteria and auditor career paths, and balancing public transparency with protection of classified information. The AIGs/Audit exchange ideas and best practices. In January 2019, the AIGs/Audit coordinated on plans to hold a procurement summit and a financial summit to encourage greater integration. The summits will include speakers from across the Intelligence Community to provide insight on emerging issues and discussion sessions to share programs and strategies to improve audit approaches in common topical areas. The summits will also provide opportunities for auditors, both supervisory and non-supervisory, to develop working relationships to encourage greater collaboration. Also at the January meeting, the AIGs/Audit established the external peer review schedule for reviews that need to be conducted during Fiscal Years 2019–2021.

Peer Reviews

Throughout the reporting period, the ICIG's Inspections and Evaluations Division supported IC counterparts by participating in peer reviews. An interagency team of peer inspectors assesses whether an OIG Inspections and Evaluations organization's projects and reports complied with CIGIE's *Quality Standards for Inspection and Evaluation* (Blue Book) and the organization's associated internal policies and procedures. Such reviews provide a level of objectivity and independence in making these determinations. The team issues a final peer review report to the reviewed organization and to CIGIE. The reviewed organization may provide copies of the final report to the head of its agency and appropriate congressional oversight bodies. The organization stands to benefit from constructive feedback and/or validation of its work products and processes. In addition, review team members gain exposure to different approaches to conducting Inspections and Evaluations work that they can share with their organizations.

The ICIG's Inspections and Evaluations Division maintains the peer review schedule for the ICIG, National Security Agency, Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, and the National Reconnaissance Office inspection programs. The composition of a typical four-person peer

review team is flexible, and IC teams tend to be composed of inspectors from multiple OIGs. Qualified inspectors from any OIG inspection program may serve on an IC peer review team as long as they meet the security clearance requirements of the reviewed organization. The Inspections and Evaluations Division provides CIGIE with an updated IC peer review schedule every six to twelve months or as events dictate.

An Inspections and Evaluations Division inspector collaborated with an interagency team from the National Geospatial-Intelligence Agency, Central Intelligence Agency, and Defense Intelligence Agency to conduct an external peer review of the National Security Agency Office of Inspector General inspection program. The results of the peer review will be reported in a future National Security Agency Semiannual Report. Inspections and Evaluations Division personnel also participated in the CIGIE Training Institute's first *Inspections and Evaluations Peer Review Lessons Learned* session. The discussion focused on the peer review process, and the bottom line for most Peer Review Teams was that starting the Memorandum of Understanding early is an important step.

Government Auditing Standards require audit organizations performing audits in accordance with generally accepted government auditing standards to have an independent, external peer review at least once every three years. The Audit Division will obtain an external peer review in Fiscal Year 2020.

Intelligence Community Inspectors General Conference

The ICIG sponsored the Annual Intelligence Community Inspectors General Conference and Awards Program on March 28, 2019. More than 500 professionals from the federal IG community attended the event, making it the largest in the ICIG's seven-year hosting history. Attendees included representatives from all IC elements and other federal agencies. Centered on the theme *Coming Together to Discuss Our Mission and Celebrate Our Successes*, the conference brought together members of the Inspector General community to exchange ideas on topics of common interest and provide training opportunities through educational instruction and collaborative working group sessions.

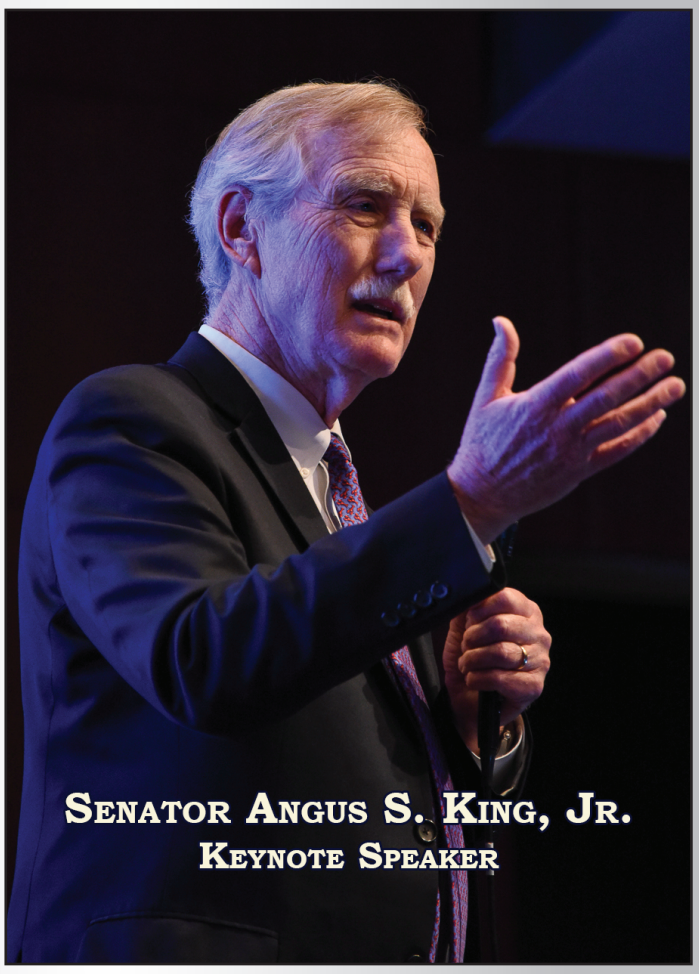
The Honorable Angus S. King, Jr., United States Senator, delivered the keynote address. His remarks at the conference focused on the importance of integrity, independence, and speaking truth to power.

Inspectors General from the Department of State, Department of Defense, Defense Intelligence Agency, National Geospatial-Intelligence Agency, and Central Intelligence Agency participated in an Inspector General panel that discussed matters of common interest through home agency and department experiences. In addition, a panel of former senior leaders in the IC led a dialogue on leadership in the IC.

Conference breakout session topics included: *Unauthorized Disclosures; Whistleblowing; Cryptocurrency; Making Better Use of Data: Automation, Analytics, and Artificial Intelligence;* and *How to Present a Matter to Prosecutors*. Conference participants were also afforded the opportunity to hone their soft skills through a series of presentations led by industry professionals focused on ethics in the workplace, harnessing potential to optimize and sustain performance, and applying influence to create positive change.

This year, for the first time, the ICIG combined the annual conference with the annual Intelligence Community Inspectors General National Intelligence Professional Awards. The Awards recognize individuals in the OIG Intelligence Community who advanced their profession through superior performance and exceptional accomplishments. Eligible candidates and teams were recognized in seven award categories: lifetime achievement; collaboration; leadership; audit; inspections; investigations; and IC-wide mission impact. This year, 39 individuals from 6 different Intelligence Community Inspectors General offices received their awards and recognition for their exceptional accomplishments in front of their families, friends, colleagues, and peers during the conference.

INTELLIGENCE COMMUNITY INSPECTORS GENERAL CONFERENCE



2019 Intelligence Community Inspectors General Conference


Intelligence Community
Inspectors General Conference
Coming Together to
Discuss Our Mission and
Celebrate Our Successes
March 28, 2019


HUR LUNDAHL CONFERENCE CENTER


Mary McCord

One of the most significant ways the ICIG works to improve the integration of the Intelligence Community is through the Intelligence Community Inspectors General Forum (the Forum). By statute, the Forum consists of the twelve statutory or administrative IGs with oversight responsibility for an element of the IC. The Inspector General of the Intelligence Community is the Chair of the Forum.

The Forum serves as a mechanism through which members can learn about the work of individual members that may be of common interest, and discuss questions about jurisdiction or access to information and staff. As Chair, the Inspector General of the Intelligence Community leads the Forum by coordinating efforts to find joint solutions to mutual challenges for improved integration among the Forum members. Forum committees, topic-specific working groups, and subject matter experts generate ideas to address shared concerns and mutual challenges for consideration and decision by the Inspectors General.

The Inspector General of the Intelligence Community chaired two Forum meetings during this reporting period. At the first meeting, held in December 2018, the Forum addressed numerous issues including an agreement for the ICIG to draft an Intelligence Community Management Challenges Capstone report to be vetted through the Forum's Audit and Inspections Committees, prior to submission to ODNI's Chief Financial Officer, to be included in the *Congressional Budget Justification Book*. The ICIG provided a read-out of the Five Eyes Intelligence Oversight and Review Council Conference held in Canberra, Australia, in October 2018, and noted the next conference will be held in the United Kingdom in the fall of 2019. Members of the Forum discussed the Council of the Inspectors General on Integrity and Efficiency's involvement with the Presidential Policy Directive 19 process, and standards governing when Executive Review Panels will be convened. They also discussed unauthorized disclosures.

The second ICIG Forum meeting, held in March 2019, included an Artificial Intelligence and Machine Learning briefing during which members discussed the need to understand various forms of data, how to access the appropriate channels to retrieve said information, and the importance of cultivating working partnerships with those outside the IC. Participants also addressed potential joint projects to encourage cross-IC work and the importance of Forum transparency. The Forum will convene again in June 2019.

Forum Committee Updates

The ICIG's Principal Deputy Inspector General, Assistant Inspectors General, and General Counsel each chair Forum committees to further collaboration, address common issues affecting Inspectors General equities, implement joint projects, support and participate in Inspectors General training, and disseminate information about best practices. These committees and topic-specific working groups meet regularly. Summaries of the Forum committees held during the reporting period are provided below.

Audit Committee

In December 2018, the Audit Division hosted the Audit Committee and Cybersecurity Subcommittee quarterly meetings to discuss multiple topics of community interest. The meeting featured guest speakers from the U.S. Agency for International Development, Office of Inspector General. Their presentation focused on collaborative efforts between OIG auditors and investigators to uncover procurement fraud in a project that involved support to Syria. The presentation was intended to foster ideas for integrating the skillsets of auditors and investigators within an organization and between organizations. The meeting also included a guest speaker from the Department of Transportation OIG, who delivered a presentation on her office's ongoing selection process for automated audit management software. OIGs across the community use automated audit software to document evidence collected for audits and inspections. One software package used by a majority of the IC organizations is moving to a web-based version, which will require significant transition or the selection of another vendor's software package. The presentation was helpful in sharing the challenges and timeline involved in the software selection process.

The Audit Committee highlighted efforts by auditors and investigators in the OIG Community to work jointly to combat procurement fraud.

In February 2019, the Audit Division hosted the Audit Committee quarterly meeting, which featured a guest speaker from the Government Accountability Office who provided a presentation on the updates to Government Auditing Standards that will go into effect in July 2019. The audit standards are the foundation from which all government auditors perform their work. The IC members gained a better understanding of the upcoming changes, along with the decision process for some of the major revisions to audit requirements. The revisions reinforce the principles of transparency and accountability and strengthen the framework for high-quality government audits.

Counsels Committee

The Counsels Committee meets regularly to discuss issues of common interest to the IC, and to promote the consistent interpretation of laws, policies, and Executive Orders. The Counsels Committee operates with the goal of providing legal analysis of, and options relating to, issues of particular importance to the Forum for final decision-making.

During this reporting period, the Counsels discussed and, where appropriate, collaborated on key initiatives, including the following:

At the request of Congress, in February 2018 the Government Accountability Office initiated Engagement 102577 to determine the extent to which IC IGs adhere to their policies and procedures in the area of whistleblower investigations. The review includes whistleblower reprisal investigations and senior leader misconduct investigations conducted by the ICIG, CIA IG, DIA IG, NGA IG, NRO IG, and NSA IG. During this reporting period, the OIGs have been responding to and engaging with the Government Accountability Office in furtherance of this review.

Counsels are collaborating to ensure individuals alleging reprisal receive similar whistleblower protections regardless of whether they submit a complaint against an individual IG or any other person in the Intelligence Community.

The Council of Inspectors General on Integrity and Efficiency (CIGIE) has statutory authority to investigate allegations of wrongdoing by Inspectors General under 5 U.S.C. App. 3 § 11(d)(6). CIGIE's Integrity Committee receives, reviews, and refers for investigation allegations made against Inspectors General and their designated senior staff members. IGs are required by statute to refer allegations of wrongdoing against IGs to CIGIE's Integrity Committee. Forum Counsels continued to discuss the jurisdictional bases and appropriate procedures for addressing complaints submitted to CIGIE's Integrity Committee, and allegations of whistleblower reprisal against Intelligence Community IGs under PPD-19 to ensure that any individual alleging reprisal to the Intelligence Community OIGs receives similar treatment and review regardless of whether they are submitting a complaint against an IG or any other individual.

To standardize and harmonize investigations completed under PPD-19, the Counsels continued to discuss, revise, and enhance the standards for handling External Review Panel (ERP) reviews pursuant to PPD-19, Part C. Counsel

Counsels Committee

discussion and efforts included defining the standards of review that the ICIG would use in defining, first, the standards in its determination to convene an ERP under PPD-19, Part C, and, second, the standards of review the ICIG would use once a decision to accept the request for a review under PPD-19, Part C is rendered. By developing these standards, the Counsels believe the process will be clearer to both the local agency IGs as well as those requesting a review under PPD-19, Part C. Efforts on this initiative are ongoing.

The Counsels discussed how to effectively track and meaningfully discuss potential legislation impacting the Forum members, including the Senate and House versions of the Intelligence Authorization Acts for Fiscal Years 2018 and 2019.

Finally, the Counsels are identifying potential joint legislative priorities to enhance the effectiveness and operations of the Intelligence Community OIGs, and are continuing to identify points of contact within Intelligence Community IG offices and elements to facilitate efficient interagency classification reviews.

The Counsels Committee is identifying potential legislative priorities that will enhance the effectiveness and operations of the Intelligence Community OIGs.

Inspections and Evaluations Committee

The Inspections and Evaluations Division shared with the Inspections Committee the results of a 2018 benchmarking exercise on Intelligence Community OIG policies and practices regarding CIGIE's Quality Standards for Inspection and Evaluation (Blue Book) related to "Independence," one of the fourteen professional standards for Inspection programs. Independence is foundational to Inspection programs in that it ensures that the organization and each individual inspector are free both in fact and appearance from personal, external, and organizational impairments. Benchmarking results can inform members about the comprehensiveness of their respective program's policies and practices on independence in comparison to their peers. The Inspections and Evaluations Division is using the benchmarking results to improve its division manual and standard operating procedures. The results are also being used as a useful check on the completeness of the ICIG's independence-related policies and procedures.

The Inspections and Evaluations Committee collaborated on best practices for "Independence" standards and "Significant" or "High Impact" recommendations.

The Inspections and Evaluations Division also shared the results of a separate benchmarking exercise regarding Intelligence Community Inspection programs that designate inspection-derived recommendations as "Significant" or "High Impact." Though not required by CIGIE, Inspection programs can make such distinctions as a way to highlight for stakeholders recommendations that address a problem, abuse, or deficiency that meets one or more established conditions. These criteria normally involve substantial risk or vulnerabilities to the mission, inadequate stewardship of resources, the integrity of the oversight process or relationship with Congress, or noncompliance with law, Executive Order, or a significant violation of agency regulation or policy. The criteria for a Significant Recommendation may also apply to an OIG's Audit program, and both ICIG's Inspections and Evaluations and Audit Divisions began applying the same Significant Recommendation criteria to reviews initiated in FY 2019.

For its second session, the Committee members discussed their Fiscal Year 2020 work planning, as well as common challenges and projects that could be conducted jointly or concurrently. The Committee also discussed best practices in conducting interviews and collecting data that is unclassified but OIG-sensitive,

Inspections and Evaluations Committee

in non-secure environments. During the execution phase of a review, Intelligence Community OIGs have occasion to collect relevant information from individuals and organizations outside of the Intelligence Community. Recommended practices include working with elements' security offices to use secure locations to the fullest extent possible as well as ensuring the clearance level of interviewees is known in advance; submitting interview questions in advance for classification and pre-publication review; ensuring interviewees know what will be done with their information and whether they will be able to access the final inspection report; and encrypting information shared online.

Committee members discussed Fiscal Year 2020 work planning to identify common challenges and projects that could be conducted jointly or concurrently.

Investigations Committee

The Forum's Investigations Committee met twice during this reporting period. Highlights of the sessions included a parallel meeting with the Audit Committee forum that featured a presentation by guest speakers from the U.S. Agency for International Development, Office of Inspector General, and covered topics of collaborative investigative efforts by both auditors and investigators to identify procurement fraud. In addition, the Investigations Committee led benchmarking efforts regarding investigative strategies and processes, investigative thresholds, and the implementation of Intelligence Community Directive 701 (ICD 701), Unauthorized Disclosure of Classified National Security Information.

In March 2019, the Committee hosted representatives from IC elements and their security components to discuss the threshold and process for reporting unauthorized disclosures, increased transparency, and developing community principles and consensus on the implementation of ICD 701. Participants focused on effective, efficient and appropriate implementation of unauthorized disclosure investigative efforts and requisite reporting.

Finally, attendees discussed resource allocation challenges to effectively investigate time and attendance fraud, and potential solutions to address the on-going threat of fraud, waste, abuse, and mismanagement associated with labor mischarging.

The Investigations Committee coordinated discussions between OIGs and security offices to report, track, and monitor reports of unauthorized disclosures under ICD 701, *Unauthorized Disclosure of Classified National Security Information.*

Management and Administration Committee

During this reporting period, the Management and Administration Committee engaged on the following topics: Information Technology (IT) independence; best practices for data protection when employees depart IG offices; talent management; and workforce training and development. There was robust dialogue on IT independence and consensus that this is a challenge area for IG offices across the IC. The Department of Defense OIG Chief of Staff briefed the members on the Department of Defense's efforts to achieve Information Technology independence, the challenges they faced, how they overcame those challenges, and lessons learned.

The Committee also discussed the potential for cross-community recruitment initiatives to address difficulties associated with recruiting for hard to fill positions, such as auditors, and Information Technology professionals, and how recruitment efforts could be enhanced by leveraging technology currently in development.

The Management and Administration Committee initiated cross-community recruitment discussions to improve recruiting for hard to fill positions, such as auditors and IT professionals.

The Committee initiated discussions on shared training opportunities and how to inform Forum members when space is available in training courses to ensure maximum participation across the community. The Information Technology Subcommittee chair also provided an update on their activities. The Committee will convene again in May 2019.

The Information Technology Subcommittee falls under the purview of the Management and Administration Committee. The Information Technology Subcommittee continued to focus on leveraging enterprise-managed IT systems and resources for efficiency, cloud computing within the IC, and protection of sensitive OIG data when employees depart OIG offices. Representatives from ODNI's Information Services Group briefed the attendees on the basic construct of Cloud Computing and configurations to protect sensitive data. The members also discussed methods for addressing widespread concerns regarding information maintained in email of departed OIG personnel. To address this concern, the group will collaborate with the Intelligence Community Chief Information Office to develop an Intelligence Community Directive that provides clear guidance on OIG data protection.

Community-Wide Outreach Activities

During the reporting period, consistent with its objective of working to improve integration of the Intelligence Community (IC), the ICIG joined with other oversight authorities and mission operators to conduct numerous outreach efforts. The ICIG held outreach events with the workforce of both ODNI and the entire IC as well as other stakeholders, including non-government organizations and advocacy groups.

October 2018

The Inspector General, along with ODNI senior leaders from the Intelligence Community Office of Equal Employment Opportunity & Diversity, Office of Civil Liberties, Privacy and Transparency, Office of General Counsel, and Office of the Ombudsman, provided information to and answered questions from the National Counterterrorism Center workforce about oversight and compliance matters.

November 2018

In conjunction with International Fraud Awareness Week, the Inspector General hosted an event at ODNI's headquarters at Liberty Crossing to promote anti-fraud awareness and education.

November 2018

The Inspector General joined other senior officials from ODNI for a discussion with Howard University Law School students enrolled in a national security law class. The Intelligence Community Office of Equal Employment Opportunity & Diversity sponsored the event with the support and participation of the Office of General Counsel, Office of Civil Liberties, Privacy and Transparency, the National Counterterrorism Center, and the ICIG.

January 2019

The Inspector General joined representatives from ODNI's Office of General Counsel, Civil Liberties, Privacy, and Transparency Office, and the Intelligence Community Analytic Ombudsman at ODNI's Intelligence Community Ombudsman Forum. Participants engaged in a robust discussion about the relationship between IGs in the IC and IC Ombudsmen, and also discussed their shared views on the importance of visitor confidentiality and whistleblower protections.

February 2019

The ICIG redesigned its secure and unclassified websites to provide visitors with more information and easier site navigation. This improvement increased transparency into the ICIG's oversight activities; raised workforce awareness about duties, processes, and protections associated with reporting fraud, waste, and abuse; and enhanced communication, coordination, and collaboration among Inspector General partners. Furthermore, the updated website informs individuals within the IC and other interested persons about whistleblower protections and rights.

March 2019

The Principal Deputy Inspector General participated in a panel discussion hosted by ODNI's Strategy and Engagement Directorate. The panel, consisting of representatives from ODNI oversight offices, provided an organizational overview highlighting their mission resources and complainant reporting channels and processes.

Ongoing

The ICIG makes good use of opportunities to communicate its mission, strategies, and processes. ICIG personnel regularly speak at ODNI onboarding and training seminars to build trust and credibility with the ODNI and IC workforce.

RECOMMENDATIONS SUMMARY

Following publication of an inspection report, the ICIG's Inspections and Evaluations Division interacts with the inspected elements at least quarterly to ensure actions are taken to implement report recommendations. A description of the actions are entered into the ICIG's recommendations tracking database. Inspections and Evaluations leadership has the responsibility for approving closure of a recommendation once it has been demonstrated that responsive actions have met the intent of a recommendation. The Inspections and Evaluations Division may revisit closed recommendations to ensure there is no slippage or back-tracking in their fulfillment or to inform follow-on reviews.

For the ODNI to realize the maximum benefit from ICIG audits, management should ensure that adequate corrective action is taken in a timely manner to address audit recommendations. The Audit Division closely monitors implementation of its recommendations through continuous communication with stakeholder points of contact on progress and actions. The status of open recommendations is periodically conveyed to ODNI senior managers. The Audit Division issues a formal closure of audit memorandum when it determines that all recommendations in a report have been addressed.

Report Name	Date Issued	Total Issued	New This Period	Open	Closed This Period
2019					
Inspection: Cyber Threat Intelligence Integration Center	January	9	9	9	0
Audit: FY 2018 Independent Evaluation of Federal Information Security Modernization Act (FISMA)	February	11	11	11	0
2018					
Inspection: IC Freedom of Information Act (FOIA) Programs	September	10	0	7	3
Audit: Memo to the Chief Operating Officer re: Charge Card Program	August	2	0	2	0
Inspection: Assessment of IC Information System Deterrence, Detection, and Mitigation of Insider Threats	March	4	0	1	3
Assessment of a Controlled Access Program Information System Deterrence, Detection, and Mitigation of Insider Threats	January	16	0	0r	5
2017					
Inspection: Assessment of ODNI Information System Deterrence, Detection, and Mitigation of Insider Threats	September	19	0	4	4
2013					
Audit: Study: IC Electronic Waste Disposal Practices	May	5	0	1	0
2012					
Audit: IC Security Clearance Reciprocity	December	2	0	1	1
	Totals	**78**	**20**	**36**	**16**

ICIG HOTLINE

You joined to make a difference.
Report for the same reason.

ICIG

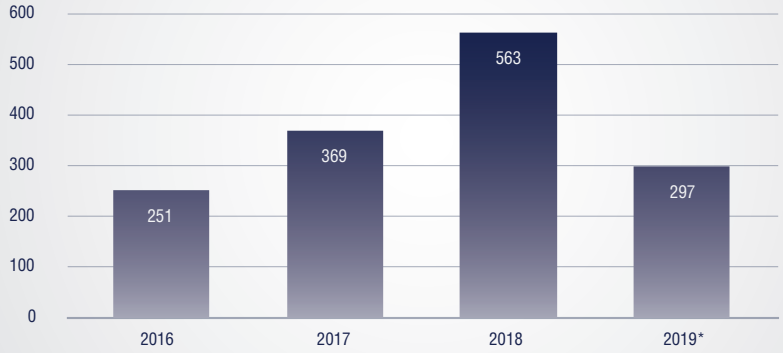
Report suspected fraud, waste, and abuse.

Office of the Inspector General of the Intelligence Community

Unclassified phone: 855-731-3260 |Secure phone: 933-2800
Unclassified fax: 571-204-8088
Unclassified email: ICIGHOTLINE@dni.gov
Secure email: ICIGHOTLINE@dni.ic.gov
https://www.dni.gov/ICIG-Whistleblower
12290 Sunrise Valley Drive, Reston VA 20191

The ICIG Hotline provides a confidential means for Intelligence Community employees and contractors, as well as the public, to report fraud, waste, and abuse. The Hotline can be accessed via classified and unclassified email and phone lines, U.S. mail, secure web submissions, walk-ins, and drop boxes located in select ODNI facilities.

NEW HOTLINE CONTACTS BY FISCAL YEAR



* Includes data for half FY, from October 2018 - March 2019

NEW CONTACTS THIS REPORTING PERIOD

297

METHODS OF CONTACT

including repeat contacts; excluding walk-ins and drop box submissions

839 Phone Calls	**16** USPS Mail
9 Faxes	**209** Email/Web

ABBREVIATIONS AND ACRONYMS

AI ..... Artificial Intelligence
AIG/Audit ..... Assistant Inspector General for Audit
AIM ..... Augmenting Intelligence using Machines
The Center ..... The Center for Protected Disclosures
CIA ..... Central Intelligence Agency
CIGIE ..... Council of Inspectors General on Integrity and Efficiency
CISA ..... Cybersecurity Information Sharing Act of 2015
CTIIC ..... Cyber Threat Intelligence Integration Center
DIA ..... Defense Intelligence Agency
DNI ..... Director of National Intelligence
EO ..... Executive Order
ERP ..... External Review Panel
EU ..... European Union
FIOR Council ..... Five Eyes Intelligence Oversight and Review Council
FISMA ..... Federal Information Security Modernization Act of 2014
FOIA ..... Freedom of Information Act
The Forum ..... Intelligence Community Inspectors General Forum
FY ..... Fiscal Year
GAO ..... Government Accountability Office
IC ..... Intelligence Community
ICD ..... Intelligence Community Directive
ICIG ..... Inspector General of the Intelligence Community
ICFLP ..... Intelligence Community Foreign Language Program
IG ..... Inspector General
IPERA ..... Improper Payments Elimination and Recovery Act
ICWPA ..... Intelligence Community Whistleblower Protection Act
IT ..... Information Technology
OGC ..... Office of the General Counsel (ICIG)
NGA ..... National Geospatial-Intelligence Agency
NRO ..... National Reconnaissance Office
NSA ..... National Security Agency
ODNI ..... Office of the Director of National Intelligence
OIG ..... Office of the Inspector General
PPD ..... Presidential Policy Directive
U.S. ..... United States
U.S.C. ..... United States Code

Office of the Inspector General of the Intelligence Community

571-204-8149 open; 939-9200 secure