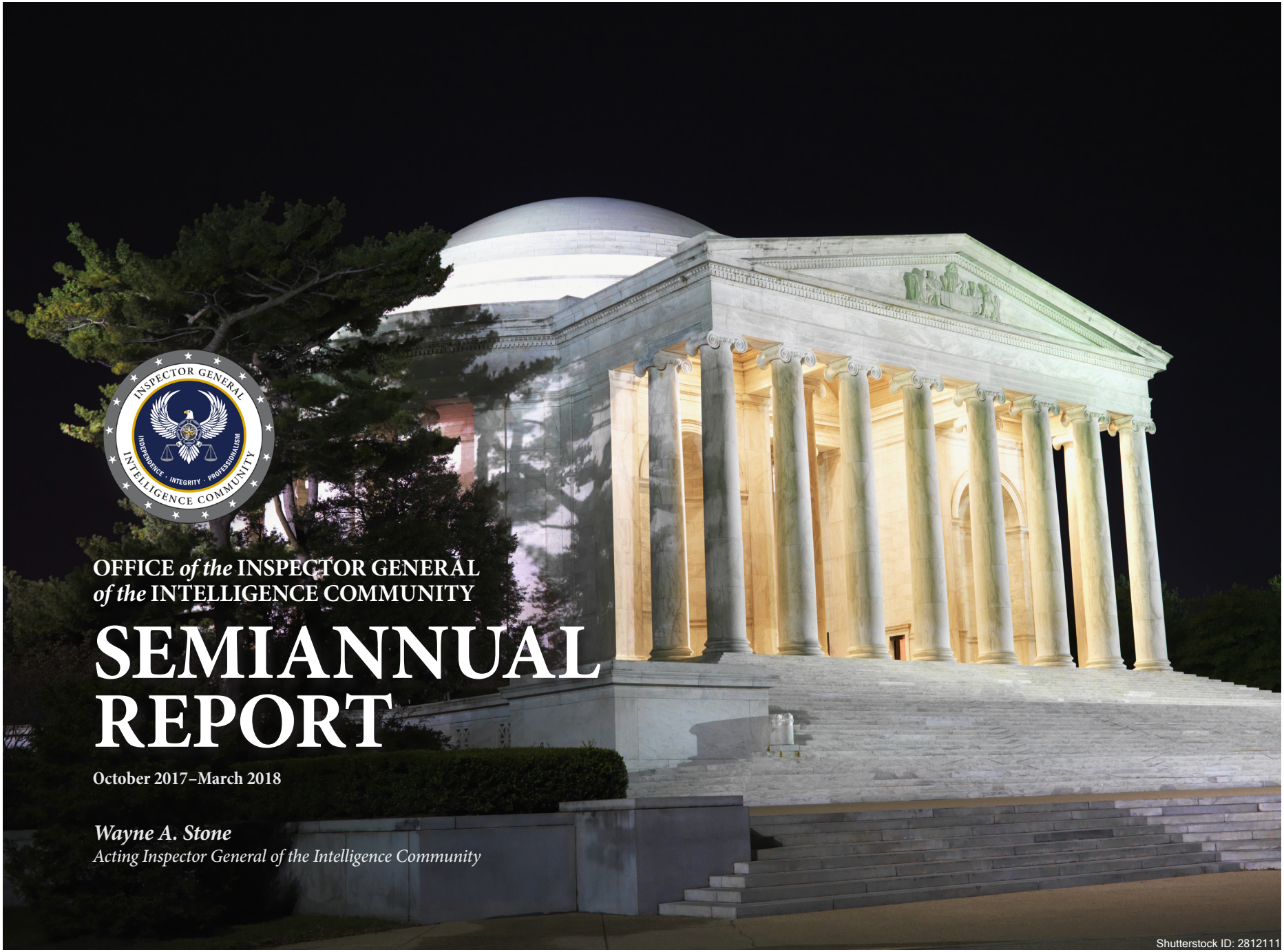


OFFICE *of the* INSPECTOR GENERAL
***of the* INTELLIGENCE COMMUNITY**

SEMIANNUAL REPORT

October 2017–March 2018

Wayne A. Stone
Acting Inspector General of the Intelligence Community

Table *of* Contents

FORUM | RECOMMENDATIONS | AUDIT | INSPECTIONS | INVESTIGATIONS | IC WHISTLEBLOWING | COUNSEL

Questions may be directed to the IC IG at 571-204-8149 or through e-mail at IC_IG_PAO@dni.gov.

INTEGRITY AND ACCOUNTABILITY ARE THE BUILDING BLOCKS OF A STRONG AND EFFECTIVE INTELLIGENCE COMMUNITY.

Statutory Reporting Requirements in 50 U.S. Code §3033 - Inspector General of the Intelligence Community

All Office of the Inspector General of the Intelligence Community (IC IG) inspection and investigation activities conform to standards adopted by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). All audit activities are conducted in accordance with generally accepted government auditing standards.

- We had full and direct access to all information relevant to perform our duties.
- The IC IG issued no subpoenas this reporting period.
- A list of open and closed recommendations for this reporting period can be found on page **12**. Corresponding corrective actions are listed in the classified annex.
- All ongoing and completed audits, inspections, and reviews begin on page **14**.
- Select completed investigations begin on page **21**.
- The updates on whistleblower matters begin on page **23**.

Conference Reporting

Section 739 of the Consolidated Appropriations Act of 2018 requires the Director of National Intelligence (DNI) to annually notify the IC IG of conferences funded at costs between $20,000-$100,000 within 15 days of the conference date. Between October 1, 2017 and March 31, 2018, the DNI notified the IC IG of **50** such conferences.

By the same provision, the DNI is required to annually submit a report to the IC IG for each conference funded at a cost exceeding $100,000. The DNI reported **no** such conferences during the same period.

Additional details are in the classified annex of this report.

OUR

OVERSIGHT

PROVIDES

INSIGHT *AND*

HELPS GUIDE DECISION-MAKING

WE VALUE AND EXHIBIT ACCOUNTABILITY, DIVERSITY, INDEPENDENCE, INTEGRATION, INTEGRITY, OBJECTIVITY, AND PROFESSIONALISM.

Organization

The Intelligence Authorization Act for Fiscal Year (FY) 2010 established the Inspector General of the Intelligence Community. IC IG has authority to initiate and conduct independent audits, inspections, investigations, and reviews of programs and activities within the Director of National Intelligence's responsibility and authority.

Our organization's senior management team includes the Inspector General (IG), a Principal Deputy IG, a Deputy IG, a General Counsel, four Assistant Inspectors General (AIG), and one program Executive Director.

The principal operational divisions are Audit, Inspections & Evaluations, and Investigations. The Management & Administration Division and the General Counsel's Office support the operational divisions and the IC IG Executive Office. The Executive Director for Intelligence Community Whistleblowing & Source Protection (ICWSP) provides support to IC IG Forum Members on whistleblowing matters.

Outreach

The IC IG is committed to promoting transparency in our intelligence oversight mission. The IC IG has dedicated officers to work with key stakeholders and support the operations divisions.

- **Legislative Affairs:** Melissa Wright is the IC IG's Legislative Counsel and Congressional Liaison.
- **Media Affairs:** Monica Tullos is the IC IG's Public Affairs Officer.

They can be reached at 571-204-8149 or IC_IG_PAO@dni.gov to assist with outreach efforts.

Mission

We conduct independent and objective audits, inspections, investigations, and reviews to promote economy, efficiency, effectiveness, and integration across the Intelligence Community.

Vision

Speak truth; enable excellence in management and accountability.

Core Values

Integrity

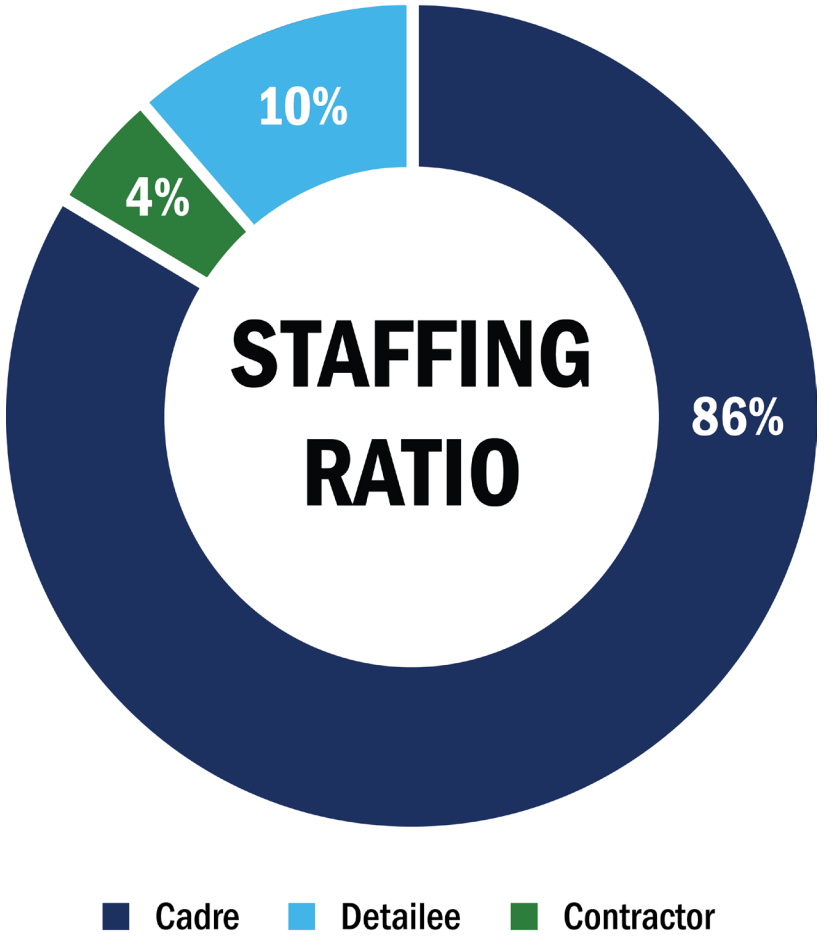
We are honest, trustworthy, accountable for our actions, and committed to fulfilling our mission.

Professionalism

We hold ourselves to the highest standards of technical proficiency and treat others with courtesy and respect.

Independence

We conduct our mission free of external influence and provide objective assessments, advice, and conclusions, regardless of political or personal consequence.



Resources

Funding

The Office of the Director of National Intelligence (ODNI) provided adequate funding to fulfill the IC IG's mission during this reporting period. The budget covered personnel services and general support, including travel, training, equipment, supplies, Information Technology (IT) support, and office automation requirements.

Personnel

The IC IG has a diverse group of talented and highly skilled employees who provide subject matter expertise; and includes cadre (permanent employees), joint duty detailees (employees from other IC organizations), and contractors.

Additional personnel details are listed in the classified annex of this report.


IC IG FORUM

THE IC IG FORUM IS COMPOSED OF INSPECTORS GENERAL WHO HAVE OVERSIGHT RESPONSIBILITIES FOR INTELLIGENCE COMMUNITY ELEMENTS.

The FY 2010 Intelligence Authorization Act established the IC IG Forum. The IC Inspector General chairs the Forum, which includes IGs from the:

- Central Intelligence Agency (CIA)
- Defense Intelligence Agency (DIA)
- Department of Defense (DoD)
- Department of Energy (DOE)
- Department of Homeland Security (DHS)
- Department of Justice (DOJ)
- Department of State (DOS)
- Department of the Treasury (DOT)
- National Geospatial-Intelligence Agency (NGA)
- National Reconnaissance Office (NRO)
- National Security Agency (NSA)

The IC IG collaborates with Forum members to identify and prioritize IC-wide projects, to seek key IG stakeholder buy-in, and to develop strategies on how to best leverage the limited IG resources across the community.

The IC IG's Deputy IG, General Counsel, and Assistant Inspectors General each chair Forum committees to further collaboration, address common issues affecting IG equities, implement joint projects, and support IG training and best practices. The committees endeavor to meet quarterly.

In February, IC IG hosted an IC IG Forum meeting. The Forum welcomed the newly confirmed IGs for NSA and NGA. In discussing the new statutory whistleblowing protections for IC contractors and whistleblower training, the Forum agreed to establish a Whistleblower working group. The Forum also agreed to participate in CIGIE's 40th Anniversary Celebration of the IG Act of 1978. Finally, the Forum agreed to address several human capital initiatives, including training, IG succession planning, and joint duty opportunities for OIG staff over the next quarter.

Committee Updates

Deputy Inspectors General Committee

The Deputy Inspectors General (DIG) continued supporting the IG's priority initiatives this reporting period. In furtherance of key whistleblower priorities, the DIG committee engaged with the IC IG to ensure that all IG's whistleblower programs were showcased at the Senate Whistleblower Caucus held in November 2017. This collaboration afforded each IC IG office the ability to represent their programs and provide insights and highlights to interested congressional stakeholders.

In addition, the DIG committee was extremely supportive of the IC IG Data Analytics Collaboration Initiative. The initiative is a grassroots effort for benchmarking the IC on data analytics initiatives. Thus far, this group of dedicated IG auditors, inspectors, and investigators identified common interests and concerns among IG professionals on how best to use data to identify trends, patterns, anomalies, and exceptions to data. Participants meet on a quarterly basis to share ideas on data collection and analysis, including how to use data to identify potential fraud, waste, and abuse; enhance insights into trends and risks; and improve operations.

Finally, the DIGs led topic development for the Annual IC IG Conference break-out sessions, which included discussions on data analytics, the IC whistleblowing outreach tool, and investigation case studies. The breakout sessions were well-attended and provided an opportunity for Department and Agency OIGs to share some of their work and best practices with IG colleagues. The IC Threat Management & Information Sharing session, co-sponsored by DHS, DOJ, and IC IG, recorded the highest number of registrants with nearly 200 persons selecting this option.

Counsels Committee

The IC IG Counsels Committee meets regularly to discuss common issues and interests, and to promote consistent interpretation of laws, policies, and executive orders. This reporting period, the Counsels collaborated on key initiatives, including the interpretation of the new IC whistleblower protections in the FISA Reauthorization Act of 2017; providing legal support to the newly established IC IG Forum Whistleblower Working Group; and the potential creation of a working group with the Council of the Inspectors General on Integrity and Efficiency Integrity Committee to discuss issues associated with IC OIG complaints.

The Counsels Committee also developed and proposed "Policy Guidance for Independent Inspectors General" as requested in the Intelligence Authorization Act (IAA) for FY 2017. This Act required that certain IC OIGs develop policy guidance for rotational personnel assignments affecting IG personnel. Covered IGs certified their respective agencies' policies are in keeping with the guidance proposed by the Counsels Committee and approved by IC IG Forum members. This guidance preserves the tenets of IG independence while supporting joint duty assignments that broaden career experiences for OIG employees.

Finally, the IC IG Counsels reviewed several provisions within the respective House and Senate IAA bills for FY 2018 and provided technical drafting assistance on certain proposals to ensure consistency with other provisions of the National Security Act of 1947, as amended, and the Inspector General Act of 1978, as amended.

Management & Administration Committee

The Management and Administration Committee continues to support community-wide activities and initiatives. The committee is currently restructuring to address emerging IC IG Forum requirements. During the February IC IG Forum meeting, members requested a community focus on human capital issues such as joint duty assignments and training. The IC IG AIG for Management & Administration (M&A) is exploring expansion of the M&A Committee structure to include two subcommittees, one focused on human capital and the other on information technology. The human capital subcommittee is presently in the nascent stage.

The IT subcommittee is operational and hosted its quarterly meeting in Arlington, Virginia, this reporting period. Members received an overview from the new IC IG Forum Executive Director on his roles and responsibilities, further discussed future IT subommittee activities, and presented their top three OIG IT challenges. Additionally, the group achieved a significant milestone toward future interoperability by initiating collaboration on specific IT solutions to improve efficiency, reduce costs, and share resources across the IC OIG community. Members agreed to participate in commercial off the shelf application testing in the IC OIG cloud environment to chart a path for future integration possibilities.

Audit Committee

In November 2017, the Audit Committee hosted a meeting to discuss the ODNI Intragovernmental Transactions (IGT) invoice working group's proposed guidance. A lack of supporting documentation for IGT resulted in financial statement auditability challenges across the IC. Consequently, the working group developed a proposal that outlines standard invoice elements it believes will meet auditability requirements. The working group asked IC agencies' Chief Financial Offices to provide their respective OIGs with the proposal for review and feedback. OIG representatives met to discuss the proposal and outline a joint response.

In February 2018, the Audit Committee and Cybersecurity subcommittee hosted a meeting to discuss FY 2018 Federal Information Security Modernization Act (FISMA) guidance. Guest speakers from the Audit Executive Council Information Technology Committee provided a briefing on the draft 2018 FISMA metrics and corresponding guidance, which will provide methodology and criteria for performing OIG FISMA audits and evaluations. After DHS issued the Draft FY 2018 FISMA metrics, Audit Committee and Cybersecurity subcommittee attendees met to discuss applicability to the IC, type of engagement for each IC element, standards used by each IC element, and the plan for the 2018 FISMA Capstone report.

Inspections Committee

The Inspections Committee hosted an IC IG's Legislative Counsel Update to learn about proposed FY 2018 legislation and its relevance to IC OIGs for I&E work and contingency planning. Members exchanged views on when they consider an open inspection recommendation to be past due. They also shared strategies and best practices for timely and efficient closure methodologies to achieve desired outcomes.

NGA provided an update on consistency among each member agency's implementation of the CIGIE Guide for Conducting Peer Reviews of

I&E programs. To date, CIA, DIA, IC IG, NGA, and NRO have undergone peer reviews under the new CIGIE I&E peer review guidelines. During the second quarter, a CIA auditor and an IC IG inspector led a discussion on best practices when conducting oversight of compartmented/sensitive programs. The discussion focused on practical and process considerations for pre-inspection planning, logistics requirements, data gathering and analysis, reporting, document management, and recommendations follow-up.

The I&E Committee also shared experiences on the ways our respective programs strive to fully comply with the intent of the Blue Book standard of 'Independence' and in our day-to-day operations. Examples of compliance included requiring all inspection product reviewers sign an independence statement that obligates all OIG staff to complete the financial disclosure form OGE-450 annually. In addition, OIG Counsel could provide annual refresher training to OIG staff on the meaning of independence as an oversight professional standard along with a range of real and perceived conflicts of interests to avoid. Pursuant to the 2017 *CIGIE Guide for Conducting Peer Reviews of I&E Organizations of Federal Offices of Inspector General*, independence is one of seven Blue Book standards that, for the time being, is optional in Inspection peer reviews. CIGIE will eventually make all 14 Blue Book standards mandatory for Inspection peer reviews.

Investigations Committee

In February 2018, NGA hosted the Investigations Committee quarterly meeting and discussed forensic analytic capabilities, whistleblower reprisal investigations, and policies related to IC efforts to deter, detect, report, and investigate unauthorized disclosures of classified national security information.

Intelligence Community Inspectors General Conference

IC IG hosted the Annual IC Inspectors General Conference March 1, 2018. This unclassified conference boasted 504 registered attendees from 13 IC elements and 5 non-IC entities. The Honorable Michael Horowitz, chair of the Council of the Inspectors General on Integrity and Efficiency and Inspector General of the Department of Justice, delivered the keynote address.

Inspectors General from DHS, DoD, NRO, and NSA served on the IG panel, discussing matters of common interest through home agency and department experiences. Conference breakout session topics included the Data Analytic Evolution; Better Statistics, Better Decisions; Exploiting Social Media and Digital Exhaust for Investigations; CIGIE Audit Peer Review ; IC Threat Management and Information Sharing Programs; Data Analytics Utilizing Supervised and Unsupervised Models; Whistleblowing; and Sailing the 7 Cs. Exhibit hall displays were available showcasing various programs, including IC IG career opportunities and IC OIG-dedicated training. CIGIE and the Federal Law Enforcement Training Center promoted federal-wide IG training programs.

Five Eyes Intelligence Oversight and Review Council

The IC IG Forum members participated in the Five Eyes Intelligence Oversight and Review Council (FIORC) Conference in Ottawa, Ontario, Canada, on October 2-3, 2017. Intelligence oversight agency representatives from Australia, the United Kingdom, Canada, New Zealand, and the United States signed the FIORC Charter, officially establishing the Council. The Council compared best practices in review and oversight methodology, explored areas of cooperation on reviews and the sharing of results, and encouraged transparency to the broadest extent possible to enhance public trust.

The Australia contingent will host the 2018 council meeting in Fall 2018.

Pictured above: DOJ IG delivers the IC IG Annual Conference keynote address at the NGA facility in Springfield, VA.

RECOMMENDATIONS

Recommendations Summary

Report Name	Date Issued	Total Issued	New This Period	Open	Closed This Period
2018					
Inspection: Assessment of a Controlled Access Program Information System Deterrence, Detection, and Mitigation of Insider Threats	March	16	16	15	1
Inspection: Assessment of IC Information System Deterrence, Detection, and Mitigation of Insider Threats	March	4	4	4	0
Inspection: Multi-Sector Workforce: Determining the Accuracy of Numbers and Cost of the Civilian and Contractor Workforce	March	2	2	2	0
2017					
Audit: FY 2016 Independent Evaluation of ODNI Compliance with FISMA	September	1	0	1	0
Inspection: ODNI Information System Deterrence, Detection, and Mitigation of Insider Threats	September	19	0	8	11
Inspection: ODNI National Counterterrorism Center/Directorate of Strategic Operational Planning	September	4	0	0	4
Inspection: Joint Review of Domestic Sharing of Counterterrorism Information*	March	*6	0	0	2
2013					
Audit: Study: IC Electronic Waste Disposal Practices	May	5	0	1	0
2012					
Audit: IC Security Clearance Reciprocity	December	2	0	2	0
	Totals	59	22	33	18

* 23 recommendations were issued, but only 6 involve ODNI, which are tracked by IC IG.

AUDIT

THE AUDIT DIVISION CONDUCTS PERFORMANCE AUDITS AND IC-WIDE PROJECTS RELATED TO INFORMATION TECHNOLOGY, PROCUREMENT, ACQUISITION, INTERNAL CONTROLS, AND FINANCIAL MANAGEMENT.

Completed Audit Projects

AUD-2016-005: FY 2016 Consolidated Federal Information Security Modernization Act of 2014 Capstone Report for Intelligence Community Elements; Inspectors General

This project focused on the FY 2016 FISMA report submissions from the OIGs for the IC elements operating or exercising control of national security systems. We applied the Department of Homeland Security (DHS) FY 2015 OIG FISMA metrics issued in June 2015 to perform this evaluation. We summarized eleven IC elements' information security programs by highlighting the strengths and weaknesses their OIGs identified, and provided a brief summary of recommendations made for IC information security programs.

AUD-2017-002: Risk Assessment of the ODNI FY 2016 Charge Card Program

The Government Charge Card Abuse Prevention Act of 2012 requires that all executive branch agencies issuing and using purchase and travel cards establish and implement safeguards and internal controls to ensure the proper, efficient, and effective use of such cards. Office of Management and Budget (OMB) Memorandum, *"Implementation of the Government Charge Card Abuse Prevention Act of 2012,"* requires OIGs to conduct annual risk assessments of agency purchase cards, combined integrated card programs, and travel card programs to analyze the risk of illegal, improper, and erroneous purchases. The OIGs should use risk assessment results to determine the scope and frequency of audits or reviews of those programs.

We reviewed the FY 2016 ODNI Charge Card Program and assessed the risk as moderate for purchase cards and high for travel cards where illegal, improper, or erroneous purchases and payments may have occurred. Based on our results, we initiated an audit of the ODNI Charge Card Program for FYs 2016 and 2017.

AUD-2017-005: Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015, Section 107

Section 107 of the Cybersecurity Information Sharing Act of 2015 (CISA) directs the Inspectors General of seven organizations (Department of Commerce, Department of Defense, Department of Energy, Department of Homeland Security, Department of Justice, Department of the Treasury, and ODNI) to submit, in consultation with the IC IG and the Council of Inspectors General on Financial Oversight (CIGFO), a joint interagency report to Congress on those agencies' implementation of CISA requirements.

We compiled the responses from the OIGs regarding actions taken during CY 2016 to carry out CISA requirements, specifically, the entities' assessments of:

- The sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government;
- Whether cyber threat indicators or defensive measures have been properly classified and an accounting of the security clearances authorized by the Federal Government for the purpose of sharing with the private sector;
- The actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government;

Pictured: Statue of Thomas Jefferson at Thomas Jefferson Memorial in Washington DC.

- The cyber threat indicators or defensive measures shared with the appropriate Federal Government entities; and
- The sharing of cyber threat indicators or defensive measures within the Federal Government to identify barriers to sharing information.

We briefed the results to CIGFO and submitted the joint report to Congress. This was the first biennial joint report.

Peer Review

During this reporting period, IC IG Audit Division underwent external peer review by the National Security Agency (NSA) OIG. NSA conducted the review under the auspices of the IC IG Forum Peer Review Program and in accordance with *Generally Accepted Government Auditing Standards* (GAGAS) and the Council of the Inspectors General on Integrity and Efficiency *Guide for Conducting Peer Reviews of the Audit Organizations of Federal Offices of Inspector General*. The IC IG Audit Division was last peer reviewed in 2015.

The IC IG Audit Division received an external peer review rating of "pass with deficiencies." The external peer review team found that the IC IG Audit Division made improvements since the last peer review. In addition, the external peer review team determined that Audit Division's suitably designed system of quality control for the period ending March 31, 2017 provided the IC IG Audit Division with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

The review team provided three findings for improvement pertaining to independence, compliance with GAGAS requirements for identifying the type of GAGAS engagement performed, and correct use of the GAGAS compliance statement.

We acknowledged and generally concurred with the "pass with deficiencies" assessment and established corrective actions. We believe we followed proper procedures for executing the projects in accordance with the IC IG Audit Manual and GAGAS. Moreover, we note that there was no impact to our reports despite the identified deficiencies. The next external peer review will occur in 2020.

Ongoing Audit Projects

AUD-2018-001: Review of ODNI FY 2017 Policies and Procedures for Implementing the Federal Information Security Modernization Act of 2014

FISMA requires an annual independent evaluation of federal agencies' information security programs and practices. In October 2017, we initially announced this project as the "*Evaluation of FY 2017 ODNI Compliance with the Federal Information Security Modernization Act of 2017*." We changed the title from Evaluation of Compliance to Review of Implementing to reflect the limited scope of the review resulting from the ODNI Office of the Chief Information Officer's relatively recent establishment and the ongoing development of policies and procedures for that new office.

Therefore, this report summarizes ODNI policies and procedures relevant to FISMA. We will incorporate the results of the review in the FY 2017 FISMA Capstone Report. We plan to evaluate the effectiveness of ODNI's information security program using the DHS FY 2018 Inspector General FISMA metrics as part of our *FY 2018 Independent Evaluation of the ODNI Compliance with the Federal Information Security Modernization Act of 2014*.

AUD-2017-003: FY 2017 Federal Information Security Modernization Act of 2014 Capstone of Federal Agencies' Evaluations of Intelligence Community Elements

This project focuses on the FY 2017 FISMA report submissions from the OIGs for the 11 IC elements operating or exercising control of national security systems. We will summarize the results of federal agencies' independent evaluations of their Intelligence Community elements' compliance with the DHS metrics for information security programs. We will also provide a brief summary of the recommendations made for IC information security programs.

AUD-2018-002: Audit of ODNI's FY 2016 and FY 2017 Charge Card Program

The Government Charge Card Abuse Prevention Act of 2012 requires that all executive branch agencies establish and implement safeguards and internal controls to ensure the proper, efficient, and effective use of purchase and travel cards. The audit objective is to determine whether illegal, improper, or erroneous purchases and payments were made through the ODNI Charge Card Program during FYs 2016 and 2017.

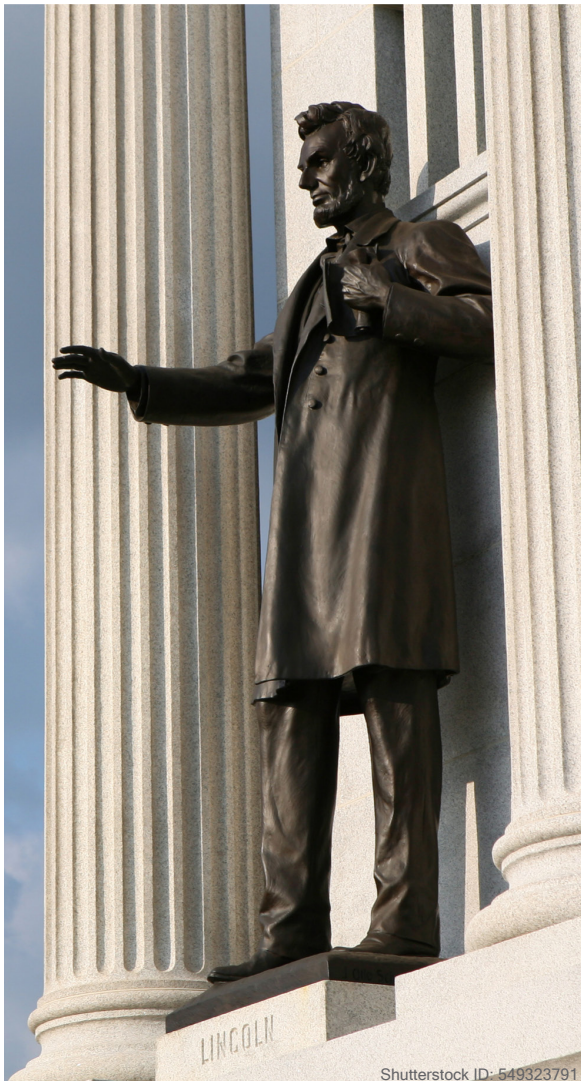
We completed a risk assessment of the FY 2016 ODNI Charge Card Program and assessed the risk as moderate for purchase cards and high for travel cards where illegal, improper, or erroneous purchases and payments may have occurred. Based on our risk assessment results, we initiated an audit of the FY 2016 and FY 2017 ODNI Charge Card Program in December 2017. This will be the first IC IG audit of the ODNI travel card program.

AUD-2018-003: Review of the ODNI's FY 2017 Compliance with the Improper Payments Elimination and Recovery Improvement Act of 2012

The Improper Payments Elimination and Recovery Improvement Act of 2012 requires that each executive agency undergo an annual OIG compliance review to identify any programs or activity payments that may be susceptible to significant improper payments. OIGs are required to submit the review to OMB within180 days after each agency publishes its agency financial report. We initiated our review in January 2018.

Use of Data Analytics Software

In FY 2018, the Audit Division began using data analytic software in its audits and reviews. A significant impact of data analytic software is its ability to query databases and large data files to quickly identify anomalies, errors, and indicators of fraud. The data analytic tool performs rapid testing of entire populations of data, eliminating the need for sample testing. The use of data analytics will increase both the effectiveness and efficiency of our audit fieldwork.



Pictured: Statue of Abraham Lincoln at the Gettysburg National Military Park.

INSPECTIONS & EVALUATIONS

THE INSPECTIONS & EVALUATIONS DIVISION WORKS TO IMPROVE ODNI AND IC-WIDE PERFORMANCE AND INTEGRATION BY EXAMINING INFORMATION ACCESS; COLLABORATION, COLLECTION, AND ANALYSIS; IC PROGRAMS AND ISSUES; AND COMPLIANCE WITH LAWS AND REGULATIONS.

Summary of Completed Reviews

Additional details of these reports are in the classified annex.

INS-2017-001, INS-2017-007, INS-2017-008: Assessments of Intelligence Community Information System Deterrence, Detection, and Mitigation of Insider Threats

We assessed Intelligence Community progress in establishing insider threat programs (ITP), implementing safeguards to protect employee privacy and civil liberties, and developing measures of effectiveness to determine whether the Intelligence Community ITPs detect and deter insider threats. We also assessed community efforts to identify and remediate information system vulnerabilities on classified networks.

INS-2017-005: Report on Reprisals Made Against Covered Contractor Employees Intelligence Authorization Act for Fiscal Year 2017 § 615

I&E completed a report to the Congressional Intelligence Committees on reprisals made against covered contractor employees as defined in Section 615 of the Intelligence Authorization Act of FY 2017. Specifically, for the period from May 5, 2014 to May 4, 2017, the FY 2017 IAA required the IC IG report include:

- Identification of the number of known or claimed reprisals made against covered contractor employees during the three-year period preceding the date of the report and any evaluation of such reprisals;
- Evaluation of the usefulness of establishing a prohibition on reprisals against covered contractor employees as a means of encouraging such contractors to make protected disclosures;
- Description of any challenges associated with establishing such a prohibition, including with respect to the nature of the relationship between the Federal Government, the contractor, and the covered contractor employee; and
- Description of any approaches taken by the Federal Government to account for reprisals against non-Intelligence Community contractors who make protected disclosures, including pursuant to Section 2409 of title 10, United States Code, and sections 4705 and 4712 of title 41, United States Code.

INS-2017-006: Multi-Sector Workforce: Determining the Accuracy of Numbers and Costs of the Civilian and Contractor Workforce

I&E completed an assessment in response to a Congressionally Directed Action in the FY 2017 IAA to determine the accuracy of intelligence community data for the numbers and costs associated with the civilian and contractor workforce in each element of the IC. In accordance with the FY 2017 IAA mandate, the IC IG submitted a written report to Congress of our findings. The IC Chief Human Capital Office assisted I&E with understanding the methodology, scope, and nature of relevant data and documentation that office used to inform our assessment and to comply with Section 306 of the Act.

Summary of Ongoing Reviews

INS-2018-001: Assessment of Intelligence Community Freedom of Information Act Programs

I&E is conducting an assessment of Freedom of Information Act (FOIA) programs within the IC. The review will focus on the effectiveness of (1) each IC element's effort to manage FOIA determinations, (2) each IC elements mechanisms to prevent inconsistent FOIA release determinations, and (3) IC-wide mechanisms to ensure consistent FOIA release determinations across the IC.

Report issuance is targeted for FY 2018.

INS-2018-003: Special Review of the Cyber Threat Intelligence Integration Center

I&E recently launched a routine inspection of the ODNI Cyber Threat Intelligence Integration Center (CTIIC). The inspection will focus on CTIIC management effectiveness, mission performance, resource management, and enterprise oversight, but may also address other issues identified during the course of our review.

Report issuance is targeted for FY 2018.


INVESTIGATIONS

THE INVESTIGATIONS DIVISION INVESTIGATES ALLEGATIONS OF VIOLATIONS OF CRIMINAL, CIVIL, AND ADMINISTRATIVE LAWS ARISING FROM THE CONDUCT OF IC, ODNI, AND CONTRACT EMPLOYEES.

During this reporting period the Investigations Division continued its efforts in cross-IC fraud matters, working jointly with the Federal Bureau of Investigation (FBI), IC OIGs, Defense Criminal Investigative Service, Air Force Office of Special Investigations, and other federal investigative agencies, as well as the DOJ Public Integrity Section and the U.S. Attorney's Office for the Eastern District of Virginia.

Our investigators also spent a significant amount of time on a continuing joint criminal investigation with the FBI, 10 other federal law enforcement organizations, and OIGs. We expect this investigation to continue into the next reporting period.

Select Completed Investigations

INV-2018-0006: Labor Mischarging

IC IG substantiated labor mischarging by a contract employee who submitted false and inaccurate labor hours totaling 181 hours at a rate of $162.50 per hour. The industrial contractor made full restitution of $29,412.50 in improper charges.

INV-2017-0010: Unauthorized Disclosure

IC IG substantiated allegations that an ODNI cadre officer disclosed classified information without authorization, transmitted classified information via unauthorized means, and disclosed classified information to persons not authorized to receive it. During a voluntary interview, the ODNI cadre officer admitted to transmitting classified information over unclassified (internet) email to recipients not authorized to receive classified national security information. The U.S. Attorney's Office for the Eastern District of Virginia declined prosecution. The officer, who was retirement eligible, retired before termination.

INV-2017-0007: Theft of Government Property

The IC IG opened an investigation in response to allegations that an ODNI detailee, and possibly others unknown, allegedly stole over $2 million of computer hardware purchased by the Federal Government. The allegation was unsubstantiated because the computer hardware was successfully deployed, demonstrating the equipment was delivered, received, and subsequently installed.

INV-2017-0008: Assistance to FBI Portland: False Impersonation of an ODNI Officer

IC IG provided investigative assistance to the FBI Portland Field Office by helping determine that Subject, an Iraqi interpreter for the U.S. Armed Forces who was paroled into the United States in 2009, used fraudulent ODNI letterhead to falsely portray himself as a USG employee and directly contact members of the Iraqi Parliament. Subject pleaded guilty to unlawfully using ODNI official insignia and was sentenced to two years of probation.

INV-2017-0004: Assistance to Local Law Enforcement: Child Pornography

IC IG provided investigative assistance to the Fairfax County Police Department regarding an ODNI contractor arrested for engaging in sexually explicit conversations with a minor and viewing pornographic images of the minor on his government computer. The subject's guilty plea to one count of possession of child pornography was rejected and he is awaiting trial.

IC WHISTLEBLOWING & SOURCE PROTECTION

THE IC WHISTLEBLOWING PROGRAM OPERATES IN ACCORDANCE WITH PPD-19, "PROTECTING EMPLOYEES WITH ACCESS TO CLASSIFIED INFORMATION," AND THE DNI'S IMPLEMENTATION OF THAT DIRECTIVE THROUGH ICD 120, "INTELLIGENCE COMMUNITY WHISTLEBLOWER PROTECTION."

IC Whistleblowing

The Intelligence Community employees, contractors, supervisors, and managers detect, collect, and analyze information to develop the most accurate and insightful intelligence possible on external threats. The privileged access of those intelligence professionals carries with it the duty to lawfully disclose information regarding potential wrongdoing, including fraud, waste, abuse, and corruption. IC Whistleblowing is the mechanism to report such wrongdoing and enables transmission of the ***right information*** to the ***right people***, thereby promoting the effectiveness, efficiency, and integrity of the IC and its work product.

IC Whistleblowing Mission-Function Performance

The IC IG established the IC Whistleblower and Source Protection (ICWSP) program in 2013 in response to Presidential Policy Directive 19 (PPD-19) and, subsequently, the DNI's issuance of Intelligence Community Directive 120 (ICD 120). The ICWSP program covers three functional areas: congressional disclosures, external reviews, and outreach and training.

Congressional Disclosures

The ICWSP assists the processing of lawful Intelligence Community Whistleblower Protection Act (ICWPA) disclosures to Congress. The ICWPA established a process to ensure that the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) 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 ICWSP facilitates ICWPA disclosures by coordinating with the IC IG Hotline to prepare disclosure materials for the IC IG General Counsel's Office transmission to the SSCI and HPSCI. ICWSP tracks all disclosures, ensures review of materials for classified information, and coordinates disclosures with other IGs for appropriate review and disposition.

We transmitted nine ICWPA disclosures to the SSCI and HPSCI during this reporting period. Disclosers included current or former IC and federal employees and contractors. Content included allegations ranging from whistleblower reprisal to mishandling of classified information.

Also during this reporting period, the ICWSP program initiated a holistic review of the IC IG ICWPA processing. This review will identify and implement policies and procedures to ensure the effective and efficient intake, processing, tracking, and transmission of ICWPA disclosures.

External Reviews

PPD-19 provides a mechanism for IC employees and contractors to lawfully report wrongdoing and prohibits retaliation against employees and contractors who report such wrongdoing through proper channels. As part of this policy, PPD-19 created an external review process 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 prior to requesting IC IG review. Upon exhaustion of those processes, PPD-19 permits an External Review Panel's (ERP) discretionary review of the agency's determination.

The ICWSP program administers the ERP process by reviewing ERP requests from employees and contractors along with information provided by the employing or contracting agency. After completing the review, the ICWSP makes a recommendation to the IC IG whether to grant the request for an ERP. If granted, the IC IG will convene an ERP consisting of the IC IG and two additional IGs to review the reprisal allegations.

The ICWSP did not receive any new ERP requests during the current reporting period. However, the ICWSP program also briefed summaries and statistics regarding completed ERP reviews to the IC IG Forum members, IC senior leaders, and IC employees, contractors, and stakeholders in an effort to further accountability-focused directives and policies aimed at reducing reprisals.

During this reporting period, the ICWSP program identified the need for a holistic review of ERP processing and procedures. This review will identify the policies, procedures, and tracking mechanisms necessary for efficient and timely processing of ERP requests in accordance with law and policy.

Outreach and Training

ICWSP completed **11** events this reporting period. These events included individualized outreach to various IC OIGs to identify agency-specific and community-wide whistleblower trends, issues, and lessons learned for application across the greater IC OIG community. The ICWSP program also conducted outreach and training activities within ODNI to ensure management stakeholders present a consistent whistleblowing message. As part of this effort, the ODNI Insider Threat Program Manager requested IC IG subject matter expert (SME) support in training their staff on Whistleblower protections. An IC IG representative was available at each of the five training sessions this reporting period; and based on the positive feedback, we will provide SME support in future sessions.

On February 13, 2018, the IC IG Forum members voted unanimously to create an IC Whistleblower Working Group to address whistleblower topics to include critical issues concerning whistleblower protections. This working group is composed of members of all IC OIGs and is intended to address IC-specific whistleblower matters and provide greater opportunities for sharing lessons learned and discussing emergent whistleblower topics, such as implementation of statutory changes

to 50 U.S.C. §§ 3234 and 3341. The IC IG Forum Whistleblower Working Group held its first meeting during this reporting period and will capitalize on this momentum for future collaboration.

In conjunction with other IC IG division, the ICWSP program redesigned and deployed the IC Whistleblowing website for IC stakeholder review. The final version will be available on the IC IG unclassified website in April 2018. The IC specific whistleblower information found on the website will benefit the IC workforce, including supervisors and managers, as well as whistleblowing stakeholders across the legal, academic, corporate, and government communities.

INTELLIGENCE PROFESSIONALS HAVE A DUTY TO LAWFULLY DISCLOSE INFORMATION REGARDING POTENTIAL WRONGDOING, INCLUDING FRAUD, WASTE, ABUSE, AND CORRUPTION.


COUNSEL

IC IG COUNSEL PROVIDES INDEPENDENT, OBJECTIVE, AND CONFIDENTIAL LEGAL ADVICE ON A VARIETY OF LEGAL AND POLICY ISSUES THAT AFFECT THE IC IG MISSION.

The IC IG Office of the General Counsel's primary responsibility is to ensure the IC IG receives independent advice and counsel free of conflicts of interest. We accomplish this by providing:

- Legal and policy advice;
- Operational, administrative, and ethics reviews;
- IC Forum coordination; and
- Serving as the IC IG Congressional Liaison.

Legal and Policy Reviews

OGC continued its outreach to educate IC IG staff, ODNI components, and fellow IG Counsels about legislation and policy impacting IG equities, as well as new statutory and regulatory requirements. OGC also engaged with ODNI legal and policy offices to protect IC IG equities on critical IC-wide policy issues, notably, policy revisions on unauthorized disclosures of classified information – an administration high priority concern.

OGC reviewed these policies and participated in coordination discussions to ensure the revised policies are consistent with IC IG's, and other IGs' ability to conduct independent and objective administrative investigations of alleged unauthorized disclosures.

OGC closely supported the IC Whistleblower and Source Protection program on education and outreach efforts to ensure consistency with evolving legal and policy developments. The ICWSP's public web-based educational tool will provide information on the proper methods for disclosing potential wrongdoing, including fraud, waste, abuse, and corruption within the IC.

The website will also outline IC employee and contractor whistleblower protections, and provide an overview of IG review processes for whistleblower reprisal allegations. OGC assisted with website development by ensuring inclusion of the most recent statutory protections for IC contractor whistleblowers from the Foreign Intelligence Surveillance (FISA) Reauthorization Act of 2017. In March 2018, the ICWSP program provided a well-received demonstration of the website at the 2018 IC IG Annual Conference. We will launch the public website in April 2018.

Operational, Administrative, and Ethics Reviews

The IC IG General Counsel staff provides timely advice to the entire IC IG organization. OGC supports the Investigations Division throughout the investigative process by highlighting and providing guidance on potential legal issues meriting additional, or redirected, investigative efforts. We keep abreast of current legal trends involving individual rights and investigative methods consistent with protecting those rights.

OGC supports the Inspections and Evaluations and Audit Divisions by identifying and interpreting key policy and contract provisions dispositive to its observations, findings, and recommendations as provided in its numerous component and intelligence oversight reviews and audits.

The General Counsel staff also provides day-to-day legal and policy guidance for IC IG administrative efforts such as personnel, training, budgetary, and conference issues.

As part of the ODNI Ethics Program, the IC IG General Counsel reviews Office of Government Ethics (OGE) financial disclosure forms for personal conflicts of interest to protect the credibility and objectivity of the IC IG mission. The General Counsel reviews IC IG personnel independence statements to ensure staff are free from personal impairments that might impugn the work of an auditor, inspector, or investigator under applicable standards.

IC IG Forum Counsel Committee Coordination

The IC IG Counsel Committee fosters discussions on common issues and concerns and promotes consistent authority interpretation. The Committee met numerous times this reporting period to discuss matters and initiatives of mutual interest to IG Forum members.

Legislative Development and Congressional Engagements

The IC IG frequently engaged Congress this reporting period. Counsel provided and arranged for several bipartisan Congressional briefings on recent IC IG activities, submitted nine ICWPA disclosures to the Intelligence Oversight Committees, submitted a legislative proposal for inclusion in the IAA for FY 2019, and provided technical drafting assistance on proposed legislation as requested. For example, we submitted a legislative proposal for consideration in the FY 2019 IAA aimed at enhancing the IC IGs ability to recruit and retain experienced investigators.

The IC OGC also updated the Congressional committees on ICWPA procedures and the IG process for reviewing employee complaints of urgent concern. We continue to engage with OMB, Congressional staff, the ODNI Office of General Counsel, IC IG Forum Counsels, and the CIGIE on congressional mandates and relevant bills.

We continued to review and monitor recently enacted and proposed legislation and regulations potentially impacting IC IG operations specifically, and the broader IG community generally. For example, the Counsel's office closely tracked and commented on the IG Subpoena Authority Act, the Geospatial Data Act of 2017, the Consolidated Appropriations Act of 2018, and the House and Senate Intelligence Authorization Acts of 2018.

At the request of the Senate Whistleblower Caucus, OGC also organized a Whistleblower Caucus event for congressional members and staff with a goal of highlighting the individual IC OIG Whistleblower programs. IG representatives from the DIA, IC IG, NGA, NRO, and NSA briefed their individual programs and the nuances associated with each. The event was well-attended and well-received by many Congressional staff, as well as Senators Grassley and Wyden who serve as the chairman and ranking Member of the caucus, respectively. A summary of congressional activity is depicted in **Figure 1**.

IC IG Confirmation Hearing Support

In November of 2017, President Trump nominated Michael K. Atkinson of Maryland to be the second, Senate-confirmed Inspector General of the Intelligence Community. OGC's Legislative Counsel assisted and supported Atkinson during the confirmation process throughout the duration of this reporting period. Activities associated with the confirmation process included a number of meetings with Members of the Senate Select Committee on Intelligence, as well as several briefings with SSCI and Senate Homeland Security and Governmental Affairs Committee staff. The SSCI held the confirmation hearing for Atkinson on January 17, 2018. A summary of IC IG Confirmation Hearing activity is depicted in **Figure 2**.

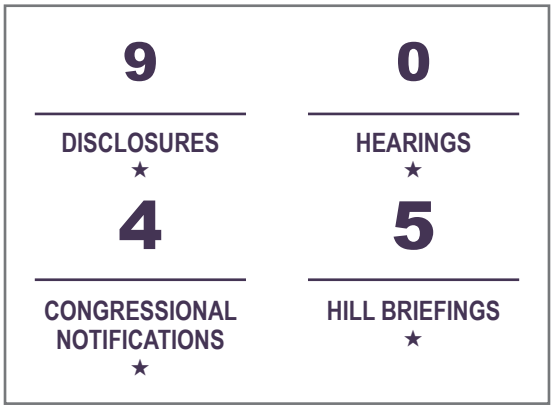


Figure 1: IC IG Congressional Activity, October 2017 - March 2018.

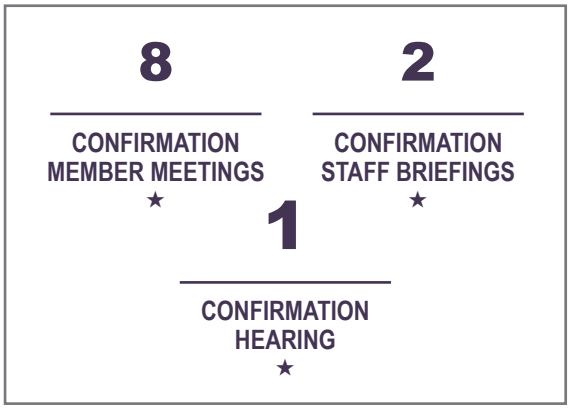


Figure 2: IC IG Confirmation Support, October 2017 - March 2018.

Abbreviations and Acronyms

AIG	Assistant Inspector General
AUD	Audit Division (IC IG)
CDA	Congressionally Directed Action
CIA	Central Intelligence Agency
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of Inspectors General on Integrity and Efficiency
CISA	Cybersecurity Information Sharing Act
CTIIC	Cyber Threat Intelligence Integration Center
DIG	Deputy Inspector General
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DOT	Department of the Treasury
ERP	External Review Panel
FBI	Federal Bureau of Investigation
FIORC	Five Eyes Intelligence Oversight and Review Council
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GTC	Government Travel Card
HPSCI	House Permanent Select Committee on Intelligence
IAA	Intelligence Authorization Act
I&E	Inspections & Evaluations Division (IC IG)
IC	Intelligence Community
ICD	Intelligence Community Directive
IC IG	Office of the Inspector General of the Intelligence Community
ICWSP	Intelligence Community Whistleblower & Source Protection
ICWPA	Intelligence Community Whistleblower Protection Act
IGs	Inspectors General
INV	Investigations Division (IC IG)
IT	Information Technology
ITP	Insider Threat Program
M&A	Management & Administration (IC IG)
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OGE	Office of Government Ethics
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PPD	Presidential Policy Directive
SME	Subject Matter Expert
SSCI	Senate Select Committee on Intelligence
USG	United States Government

IC IG HOTLINE

BE PART OF THE SOLUTION

YOU JOINED TO MAKE A DIFFERENCE, REPORT FOR THE SAME REASON

The hotline intake process provides a confidential means for IC employees, contractors, and the public to report fraud, waste, and abuse. This process includes email, secure and commercial phone numbers, U.S. mail, anonymous secure web application submissions, and walk-ins.

NEW CONTACTS LOGGED BY IC IG THIS REPORTING PERIOD

199 External

73 Internal

Internal Contacts originate from ODNI, CIA, DIA, NGA, NRO, and NSA.
External Contacts comprise all other complaints.

METHODS OF CONTACT

518 Phone Calls

214 Emails

38 USPS Mail

42 Fax

7 Meetings

16 Online Form

Office of the Inspector General of the Intelligence Community | 571-204-8149 | **Hotline: 855-731-3260** | dni.gov/icig