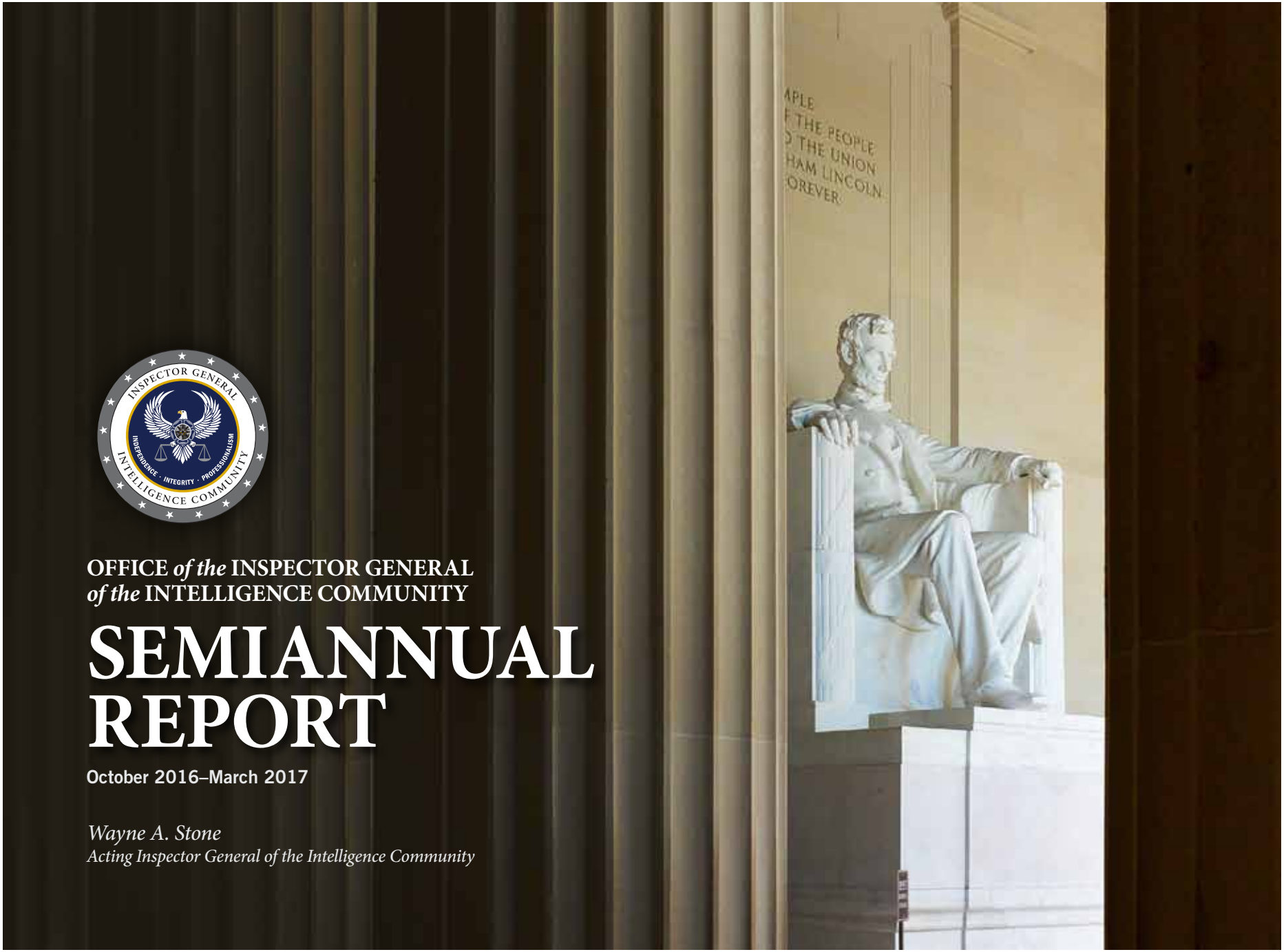


OFFICE *of the* INSPECTOR GENERAL
***of the* INTELLIGENCE COMMUNITY**

SEMIANNUAL REPORT

October 2016–March 2017

Wayne A. Stone
Acting Inspector General of the Intelligence Community

Table *of* Contents

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

DISCLAIMER: Stock photos were purchased through Shutterstock.
Questions may be directed to the IC IG at 571-204-8149.

Pictured above left to right: Mr. Wayne Stone, Acting IC IG; Mr. Joseph Composto, NGA IG; Mr. Michael Horowitz, DOJ IG; and Ms. April Stephenson, DOE Acting IG.

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 carried out in accordance with generally accepted government auditing standards.

- We had full and direct access to all information relevant to perform our duties.
- The Investigations Division did not issue any subpoenas this reporting period.
- Select completed investigations are described on page 19.
- The status of whistleblower issues begins on page 22.
- All ongoing and completed audits, inspections, and reviews begin on page 12.
- A list of open and closed recommendations for this reporting period can be found on page 10. Corresponding corrective actions are listed in the classified annex.
- ODNI held 37 conferences with cost estimates each between $20,000 and $100,000. One conference exceeded $100,000. Details are in the classified annex.

Pictured: Ms. Letitia Long, keynote speaker at the 2017 Inspectors General Conference at NGA, and Mr. Wayne Stone, Acting IC IG.

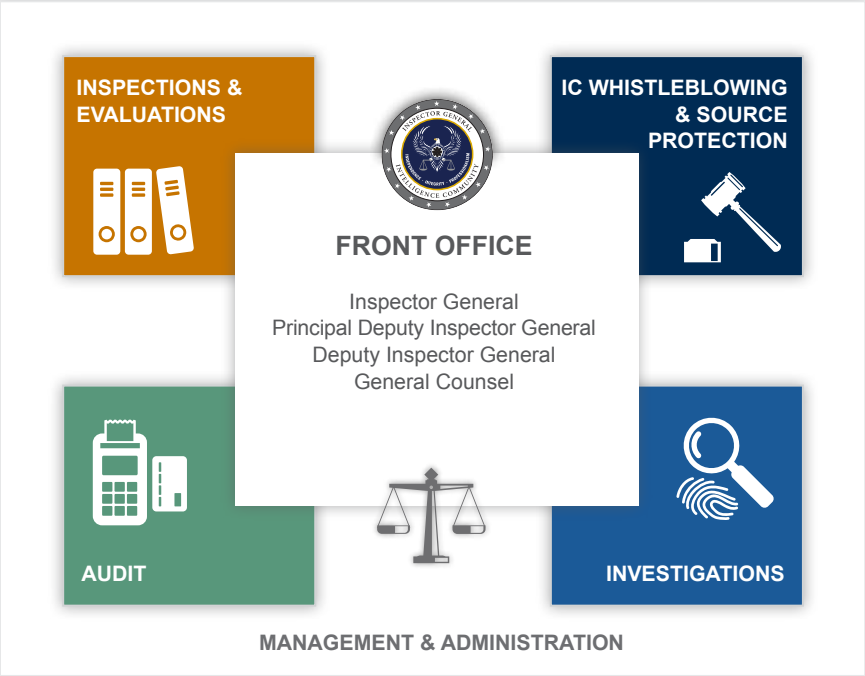
OUR

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

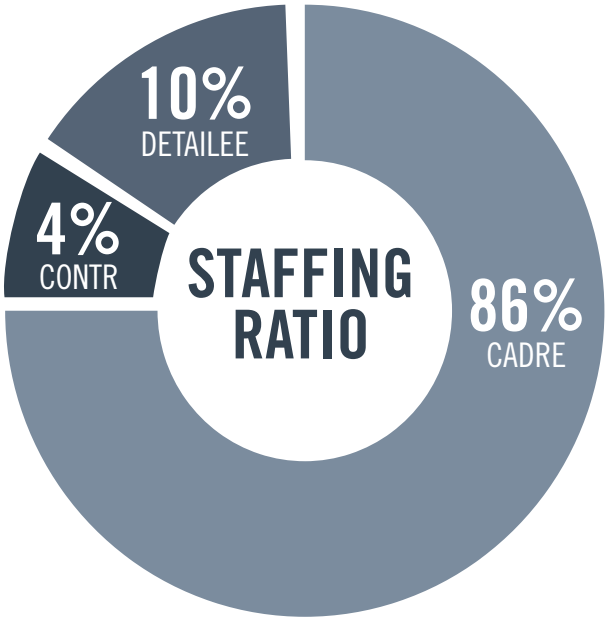
The principal operational divisions are Audit, Inspections & Evaluations, and Investigations. The Management & Administration Division and the General Counsel's Office support the operational divisions and the IC IG Front Office. The Executive Director for Intelligence Community Whistleblowing & Source Protection supports IC-wide Inspector General activities.

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:** Tamara Johnson, AIG for Management & Administration, is serving as the interim POC.

They can be reached at 571-204-8149 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 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, 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 include 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:

- Department of State
- Department of the Treasury
- Department of Defense
- Department of Justice
- Department of Homeland Security
- Department of Energy
- Central Intelligence Agency
- Defense Intelligence Agency
- National Geospatial-Intelligence Agency
- National Security Agency
- National Reconnaissance Office
- Federal Bureau of Investigation

The IC IG collaborates with Forum members to identify and prioritize IC-wide projects; to seek key IG stakeholder project 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 try to meet quarterly.

IC IG Annual Inspectors General Conference

IC IG hosted the Annual IC Inspectors General Conference March 30, 2017. This was IC IG's largest conference to date with 535 registered attendees from 13 IC agencies and 17 non-intel agencies. Ms. Letitia Long, former NGA director, provided the keynote address. The IG panel included CIA, DoD, DOE, DOJ, and NGA. Other sessions covered IC Joint Duty Opportunities, Service Organization Control Reports, Responding to "Off the Record" and Other Interview Challenges, Proactive Fraud Detection, IG Work Product on Appeal, Updating the Yellow Book, FOIA, Criminal Case Review of United States v. S. Darin Kinion, and Strategic Recruitment. There was also an exhibit hall to showcase various programs and opportunities including IC Joint Duty, Whistleblowing, and CIGIE and FLETC promoted federal-wide IG training programs. The conference was held at the unclassified level.

Pictured above left to right: Mr. Wayne Stone, Acting IC IG; Mr. Joseph Composto, NGA IG; Mr. Michael Horowitz, DOJ IG; Ms. April Stephenson, DOE Acting IG; and Mr. Glenn Fine, DoD Acting IG.

Committee Updates

Audit

The Audit Committee continued to build a better understanding of the Intelligence Community Information Technology Enterprise (IC ITE). In December 2016, the committee hosted IC Cloud subject matter experts from CIA and NSA who presented their respective roles and responsibilities as cloud computing service providers. The committee also discussed the importance of clearly defining the service provider and consumer roles because of the effect they have on members' audit responsibilities.

In March 2017, the Audit Committee hosted speakers from the American Institute of Certified Public Accountants, who provided an overview of System & Organization Control (SOC) Reporting. SOC reporting is a risk management framework that allows a service organization to determine its risks and how to mitigate such risks. The presentation

was beneficial as it provided details on how to use SOC reporting, which was a topic at previous committee meetings. Further, committee members were able to see how SOC reporting could be applied to provider and consumer relationships like those within IC ITE.

Counsel

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. For example, the committee discussed how the IG Empowerment Act's transparency provisions affect oversight of an IC element's classified mission. Committee members also discussed unique Vacancy Act requirements for current and upcoming vacant IG positions.

Information Technology

The IC IG Forum IT Committee hosted its second quarterly meeting welcoming speakers from the CIGIE and the Department of Homeland Security (DHS) OIG. CIGIE's CIO Subcommittee Chair provided an overview of the non-Title 50 OIG IT trends, best practices, and ongoing initiatives. The DHS OIG CIO led a discussion on lessons learned from efforts to deploy TeamMate in a classified environment. Several IC OIGs use this software to bring efficiency and consistency to the audit and inspection oversight process. Members also discussed plans to continue updating the IT application survey and future efforts to broaden the tool to enhance organizational insight and to seek opportunities focused on unifying efforts for related applications.

Inspections Committee

The Inspections Committee hosted the ODNI Chief of the Office of Civil Liberties, Privacy, and Transparency (CLPT) to discuss how increased transparency in the Intelligence Community can help build public trust and counter inaccurate information. OIGs can further build trust by making our products public. CLPT advocates preparing OIG products that group unclassified information in the report body and presenting classified information in footnotes, which OIG officials can easily redact or remove, thus maintaining the readability of the public product.

The Department of State OIG's Compliance Division provided the committee with an update on the processes, procedures, and tools they employ to assess and evaluate embassy operations worldwide. Members compared templates, routines, repeatable actions, and shared lessons learned from those that have garnered efficiencies and improved accuracy in tracking activities responsive to IG recommendations.

Members also received an overview on the ODNI Systems and Resources Analyses (SRA) office, which conducts analyses of IC program costs and performance. SRA activities that may serve as useful points of reference for OIG Inspection programs include processes for determining how prior resource investments performed; how the IC is postured on certain issues; and what investments the IC may pursue.

Finally, committee members discussed a framework proposed by IC IG for conducting joint reviews and resolving a number of coordination challenges that have historically lengthened the time it took to conduct and issue joint reports. The approach will be raised to the IC IG Forum for consideration.

Five Eyes Intelligence Oversight and Review Council

In the previous Semiannual Report, we reported hosting a modified version of the International Intelligence Review Agencies Conference. That meeting included representatives from intelligence oversight agencies in each of the "Five Eyes" countries. Representatives from Australia, the United Kingdom, Canada, New Zealand, and the United States had a successful meeting resulting in participants agreeing to form the new Five Eyes Intelligence Oversight and Review Council. The group construct closely mirrors other IC international groups, and will assist the IC IG in collaboration on international intelligence oversight issues.

Member enthusiasm for the Council has grown considerably. The IC IG now serves as the Executive Secretariat and we plan to organize meetings each calendar quarter. This quarter we exchanged information about founding authorities and the oversight responsibilities of each member. We will soon start coordinating plans for our next annual conference in Canada this Fall.

Recommendations Summary

Report Name	Issued	Total	Open	Closed this period
2017				
Inspection: ODNI Office of General Counsel	March	4	4	0
Inspection: Joint Review of Domestic Sharing of Counterterrorism Information*	March	*6	6	0
Audit: Transition to the Intelligence Community Cloud	January	0	0	0
Audit: Letter to OMB re Status of Audit Recommendations in regard to ODNI's FY 2016 Charge Card Program	January	0	0	0
Audit: Evaluation of Section 406(b) Federal Computer Security	December	0	0	0
2016				
Inspection: ODNI Mission Support Division	September	10	0	9
Inspection: Intelligence Community Campus-Bethesda	September	5	0	3
Inspection: Program Manager-Information Sharing Environment	February	11	0	4
Inspection: Public Affairs Office	March	3	0	3
2014				
FY 2014 Independent Evaluation of ODNI Compliance with FISMA	November	2	1	0
2013				
Study: IC Electronic Waste Disposal Practices	May	5	1	0
2012				
FY 2012 Independent Evaluation of ODNI Compliance with FISMA	December	12	1	0
Audit: IC Security Clearance Reciprocity	December	2	2	0
	Totals	**60**	**15**	**19**

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

The list detailing the status of recommendations for this reporting period is in the classified annex.

AUDIT

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

Completed Audits

AUD-2017-001: Letter to OMB re Status of Audit Recommendations in regard to ODNI's FY 2016 Charge Card Program

The Government Charge Card Abuse Prevention Act of 2012 and the guidance in OMB Memo 13-21, *Implementation of the Government Charge Card Abuse Prevention Act of 2012*, requires Offices of Inspectors General to annually provide the status of outstanding recommendations pertaining to government purchase card or government travel card programs to the Office of Management and Budget (OMB). The IC IG accordingly reported on January 19, 2017 to the OMB Director that there were no outstanding charge card recommendations for the Office of the Director of National Intelligence.

AUD-2016-003: Evaluation of Section 406(b) Federal Computer Security

The Cybersecurity Act of 2015 requires federal Offices of Inspectors General to report to Congress information related to covered computer systems. Our classified report dated December 14, 2016 did not contain any findings or recommendations, but did include a description of ODNI:

- logical access policies and practices;
- logical access controls for privileged users;
- multifactor authentication for privileged users;
- information security management practices; and
- policies and procedures used to ensure personnel implement the information security management practices.

AUD-2015-006: Transition to the Intelligence Community Cloud

In 2012, the Director of National Intelligence and leaders across the IC agreed to transition to a common enterprise architecture, the Intelligence Community Information Technology Enterprise (IC ITE), with three primary goals: increase intelligence integration, enhance information technology safeguards, and increase efficiencies. IC ITE will give our mission partners, warfighters, and decision-makers the most accurate and timely information necessary to keep the nation secure.

The IC elements' transition to IC ITE's cloud environment is a key enabler for achieving the initiative's overarching goals. As such, IC ITE's success depends in part on not only the elements transitioning their information system resources and tools (generically referred to as "systems") to the cloud, but also enabling authorized users from the other IC elements to access these items. However, interoperability in a cloud environment and information sharing across IC ITE also creates security concerns. In particular, the information system security risks or vulnerabilities of any system operating on IC ITE may result in a risk to all IC elements.

We conducted our performance audit of the transition to the IC Cloud from February 2016 through January 2017. We did not issue findings or recommendations. The objectives for the audit were to:

1. Assess how the IC elements are planning to transition to the IC Cloud environment;
2. Determine the IC elements'progress in implementing IC Cloud transition plans; and
3. Compare how the IC elements apply the Risk Management Framework (RMF) to obtain authorization to operate on the IC Cloud.

Our March 2017 audit informed the Intelligence Community Chief Information Officer that the IC elements reported they are making progress in transitioning systems, applications, and data to the IC Cloud, or are considering whether to transition to the IC Cloud. Specifically:

- Eleven of the 17 IC elements prepared plans to address transitioning to the IC Cloud and are implementing their plans;
- Fourteen of the 17 IC elements are using systems, applications, and data transitioned to the IC Cloud by other IC elements; and
- Nine IC elements currently transitioning systems to the IC Cloud stated they plan to apply the Risk Management Framework to the systems transitioning.

Some IC elements stated they have realized cost savings as a result of transitioning to the IC Cloud. However, they face challenges, most notably a lack of resources (funding and trained personnel).

Ongoing Audit Projects:

AUD-2016-004: FY 2016 ODNI Compliance with the Federal Information Security Modernization Act of 2014 Evaluation

The Federal Information Security Modernization Act (FISMA) requires an annual independent evaluation of federal agencies' information security program and practices. The IC IG evaluates ODNI by assessing its program's effectiveness and status for ODNI's internal operations using the Department of Homeland Security's FY 2015 Inspector General FISMA metrics issued in June 2015. We will also follow up on two open FISMA recommendations. The report is scheduled to be completed during FY 2017.

Additional details of this report are in the classified annex.

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

This project will focus on the FY 2016 FISMA report submissions from the OIGs for the IC elements operating or exercising control of national security systems. We will summarize 11 IC elements' information security programs by highlighting the strengths and weaknesses their OIGs identified, and provide a brief summary of the recommendations made for IC information security programs.

To perform this evaluation, we will apply the DHS's FY 2015 Inspector General FISMA metrics issued in June 2015. The report is scheduled to be completed during FY 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* (CISA) of 2015 directs the Inspectors General for seven organizations (Department of Commerce, Department of Defense, Department of Energy, Department of Homeland Security, Department of Justice, Department of the Treasury, and Office of the Director of National Intelligence) to submit a joint interagency report to Congress on those agencies' implementation of new requirements as set forth in this Act.

Specifically, the legislation provides that "the inspectors general of the appropriate Federal entities, in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress an interagency report on the action of the executive branch of the Federal Government to carry out this title during the most recent 2-year period." The Act also sets forth the content requirements of the report.

We will jointly report on actions taken during the calendar year 2016 to carry out CISA requirements. Specifically, the report will include:

- An assessment of the sufficiency of policies and procedures related to sharing cyber threat indicators within the Federal Government;
- An assessment of whether cyber threat indicators and defensive measures have been properly classified and an accounting of the security clearances authorized for the purpose of sharing cyber threat indicators and defensive measures with the private sector;
- A review of actions taken to use and disseminate cyber threat indicators and defensive measures shared with the Federal Government;
- An assessment of the cyber threat indicators and defensive measures shared with the appropriate Federal entities; and
- An assessment of the sharing of cyber threat indicators and defensive measures within the Federal Government to identify barriers to sharing information.

The first biennial report is due in December 2017. We are conducting an ODNI-specific audit (AUD-2017-004) to obtain the information needed for our portion of the joint report.

Audit Projects Planned, Not Initiated

Assessment of the ODNI FY 2016 Charge Card Program

The Government Charge Card Abuse Prevention Act of 2012 requires executive agency IGs to conduct periodic risk assessments of agency purchase card or convenience check programs to identify and analyze the risks of illegal, improper, or erroneous purchases and payments. IGs are to use the results of the assessments to determine the scope, frequency, and number of periodic audits of these programs. Due to the availability of audit personnel, we have not initiated the FY 2016 ODNI Charge Card risk assessment. When additional personnel become available, we will conduct the assessment.

Evaluation of the Office of the Director of National Intelligence Fiscal Year 2016 Compliance with the Improper Payments Elimination and Recovery Improvement Act of 2012

The Improper Payments Elimination and Recovery Improvement Act (IPERIA) requires that each executive agency undergo an annual IG compliance review. Offices of Inspectors General are required to submit the review 180 days after the agency publishes its agency financial report (AFR). The ODNI published its AFR in November 2016, making the review due mid-May 2017. Due to the availability of audit personnel, we have not initiated the FY 2016 IPERIA risk assessment. When additional personnel become available, we will conduct the assessment.

INSPECTIONS & EVALUATIONS

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

Completed Reviews

INS-2015-005: Joint Review of Domestic Sharing of Counterterrorism Information

Together with OIG partners at the Departments of Homeland Security and Justice, IC IG evaluated federally supported entities engaged in field-based domestic counterterrorism; homeland security; and information sharing activities in conjunction with state, tribal, and local law enforcement agencies. The review was in response to a request from the Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee.

The objectives of this review were to:

- Identify and examine the federally supported field-based intelligence entities engaged in counterterrorism information sharing to determine the overall missions, specific functions, capabilities, funding, and personnel and facility costs;
- Determine if counterterrorism information is being adequately and appropriately shared with all participating agencies; and
- Identify any gaps or duplication of effort among these entities.

The OIGs concluded that the partners in the terrorism-related Information Sharing Environment – components of the ODNI, DHS, DOJ, and their state and local partners – are committed to sharing counterterrorism information. Actions taken before, during, and following terrorism-related incidents, as well as programs and initiatives designed to improve sharing of counterterrorism information illustrate the partners' commitment to protecting the nation.

The OIG's joint review also identified several areas for improvement that resulted in them making 23 recommendations for enhancing counterterrorism information sharing, and ultimately, the nation's ability to prevent terrorist attacks.

Four recommendations are ODNI-centric. Of these, three recommend that the DNI, in coordination with the FBI:

- Evaluate the existing Domestic DNI Representative (DDNIR) program regional structure, in consultation with the Office of Intelligence and Analysis (I&A), to ensure that regions are appropriately sized and defined to provide common areas of interest and geographic coordination among participating partners.
- Develop and disseminate to IC member partners additional guidance and a strategy for ensuring the DDNIR program is implemented consistently across regions and update the 2011 Memorandum of Agreement to more accurately reflect the current state of the program.
- Evaluate the feasibility of incorporating non-IC members into the DDNIR program in an appropriate fashion.
- Another recommendation emphasizes that the Director of the ODNI National Counterterrorism Center (NCTC) consider assigning additional NCTC representatives to the field and/or revising the existing territorial regions, potentially to align with the DNI domestic regions, to ensure effective NCTC representation within the domestic field.

Two other recommendations are directed at ODNI, DHS, and DOJ, namely:

- All three agencies should review the 2003 interagency Memorandum of Understanding on information sharing and determine what actions are necessary to update intelligence information sharing standards and processes among the departments.
- All three agencies should codify an overarching engagement and coordination body for the terrorism-related Information Sharing Environment.

The remaining 17 recommendations are assigned to DHS and DOJ.

INS-2016-003: Assessment of Foreign Intelligence Surveillance Act Title V Information

In accordance with Section 108 of the *USA FREEDOM Act of 2015*, the IC IG completed an assessment of information acquired under Title V of the *Foreign Intelligence Surveillance Act* (FISA) (50 U.S.C. § 1861 et seq.) during calendar years 2012 through 2014. Accordingly, the IC IG assessed:

- The importance of information acquired under Title V of FISA to the activities of the IC;
- The manner in which business record information was collected, retained, analyzed, and disseminated by the IC under Title V;
- Minimization procedures used by IC elements under Title V, and whether the minimization procedures adequately protect the constitutional rights of United States persons; and
- Minimization procedures proposed by an IC element under Title V that were modified or denied by the Foreign Intelligence Surveillance Court (FISC).

Additional details of this report are in the classified annex.

INS-2017-003: Inspection: ODNI Office of the General Counsel

The mission of the ODNI Office of the General Counsel (OGC) is to provide accurate and timely legal guidance and counsel to the DNI and to the ODNI to ensure all employees and contractors assigned to the ODNI comply with U.S. law and any other applicable regulations and directives. This mission also includes supporting the DNI in carrying out statutory responsibilities that ensure compliance with the Constitution and laws of the United States by IC elements that are part of the National Intelligence Program. To this end, OGC works closely with legal officers across the IC to coordinate the development of legal mechanisms to facilitate the implementation of DNI policies and to ensure compliance with applicable law.

Additional details of this report are in the classified annex.

Ongoing Reviews

INS-2017-001: Assessment of IC Information System Deterrence, Detection, and Mitigation of Insider Threats

The Inspections and Evaluations Division (I&E) is assessing the insider threat programs of CIA, DIA, FBI, NGA, NRO, NSA, ODNI, and the Special Reconnaissance Program, and is limited to classified systems. Our review focuses on IC efforts to:

- Establish risk-based insider threat programs to protect classified information and systems and reduce the impact of unauthorized disclosures;
- Identify and remediate information security vulnerabilities of classified networks and share insider threat information with partners;
- Measure the effectiveness of information security controls to detect and deter insider threats; and
- Implement safeguards to protect employee privacy and civil liberties.

We will issue this report during FY 2018.

INS-2017-004: Inspection: National Counterterrorism Center, Directorate of Strategic Operational Planning

I&E recently launched an inspection of NCTC's Directorate of Strategic Operational Planning (DSOP). By law, one of NCTC's missions is to conduct strategic operational planning for counterterrorism (CT) activities across the U.S. Government. DSOP fulfills this responsibility by integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement, to ensure unity of effort. DSOP coordination officers and assessment officers work with the National Security Council staff and all USG departments and agencies to develop strategies, action plans, and assessments integrating and evaluating all USG CT capabilities. I&E last inspected NCTC in 2012.

We will issue this report during FY 2017.


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 FBI, IC Offices of Inspectors General, 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 and ten other federal law enforcement organizations and Offices of Inspectors General. We expect this investigation to continue into the next reporting period.
We continued to make significant investments in employee training. Another IC IG investigator completed the Federal Law Enforcement Training Center's (FLETC) Criminal Investigator Training Program. Having our officers FLETC-trained ensures they are employing the highest professional standards on each investigation.

Select Completed Investigations

INV-2014 -0012: Fraud - Update

As reported in the last semiannual report, a criminal fraud investigation substantiated that a Lawrence Livermore National Lab physicist and research scientist conducted fraudulent work on behalf of Intelligence Advanced Research Projects Activity, resulting in a $3.5 million loss to the government. The Department of Energy debarred the researcher for ten years and he is now in the GSA's Excluded Parties List System. The researcher pleaded guilty in federal court to one count of mail fraud and was sentenced to 18 months imprisonment. In addition to the prison term, he was ordered to serve three years of supervised release and to pay restitution to the government.

INV-2015-0003: Potential Time and Attendance Abuse

IC IG initiated a joint investigation with DOJ OIG after receiving an allegation of an FBI employee detailed to ODNI submitting falsified time and attendance reports. The investigation identified significant discrepancies in labor hours charged by the employee. DOJ declined prosecution in lieu of administrative action by the FBI. The matter was referred to the FBI's Office of Professional Responsibility.

INV-2015-0006: Potential Time and Attendance Abuse

IC IG initiated an investigation after receiving an allegation of an ODNI officer submitting falsified time and attendance reports. The investigation identified significant discrepancies in labor hours charged by the officer. DOJ declined prosecution in lieu of administrative action by the ODNI. IC IG referred this matter to the responsible ODNI component for appropriate action.

INV-2016-0008: Alleged Violation of Executive Order 12333

IC IG opened an investigation after receiving allegations of an ODNI officer inappropriately using social media to collect non-U.S. person and U.S. person data potentially in violation of Executive Order 12333. While the allegations were unsubstantiated, IC IG's investigation identified concerns about the officer's security practices and suitability for continued access to classified information. IC IG briefed ODNI management and referred the concerns to the appropriate ODNI components.

Conference Reporting

Section 535 of the *Consolidated Appropriations Act of 2016* (PL 114-113) requires the DNI to annually notify the IC IG of conferences it funds where the cost to the U.S. Government is between $20,000-$100,000 within 15 days of the date of the conference. Between October 1, 2016 and March 31, 2017, the DNI notified the IC IG of 37 such conferences.

By the same provision, the DNI is required to annually submit a report to the IC IG for each conference it funds that cost the U.S. Government more than $100,000. The DNI reported one such conference during the same period.

Additional details are in the classified annex of this report.

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."

The National Security Mission

In the IC, intelligence officer's day-to-day role involves detecting, collecting, and analyzing information to produce the most insightful intelligence possible on external threats.

Intelligence officers also have a duty to lawfully disclose information regarding potential wrongdoing related to fraud, waste, abuse, and corruption. They expose those internal threats undermining the integrity of the IC. Collectively, these efforts mitigate national security threats.

Overview

The IC IG established the IC Whistleblowing 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 Executive Director for Intelligence Community Whistleblowing and Source Protection (ICW&SP) is the program manager for the IC Whistleblowing program.

ICW&SP executes the directives governing IC Whistleblowing through focused activities in four primary functional areas:

Congressional Disclosures

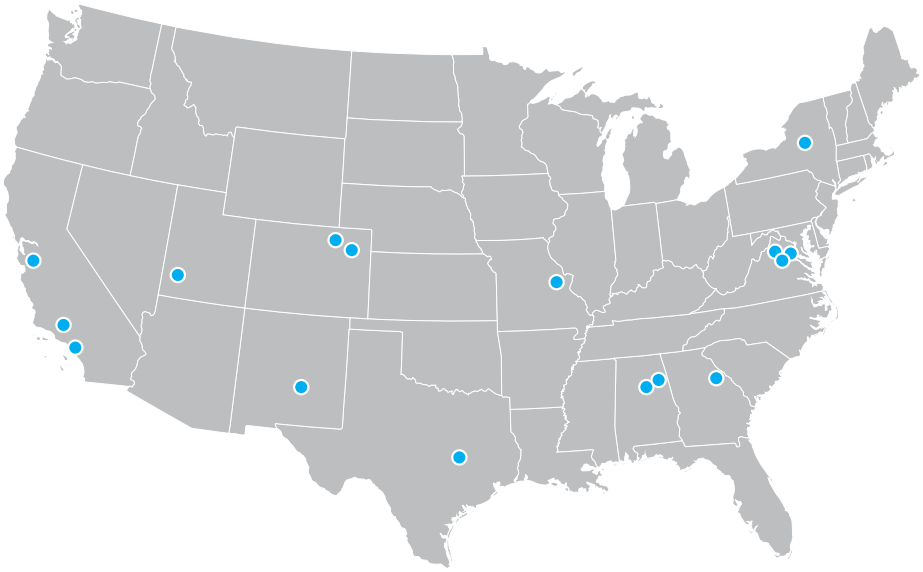
The ICW&SP promotes and facilitates lawful Intelligence Community Whistleblower Protection Act (ICWPA) disclosures to Congress. ICW&SP prepares disclosure materials in coordination with the IC IG Legislative Counsel for secure transmission through the DNI to the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).

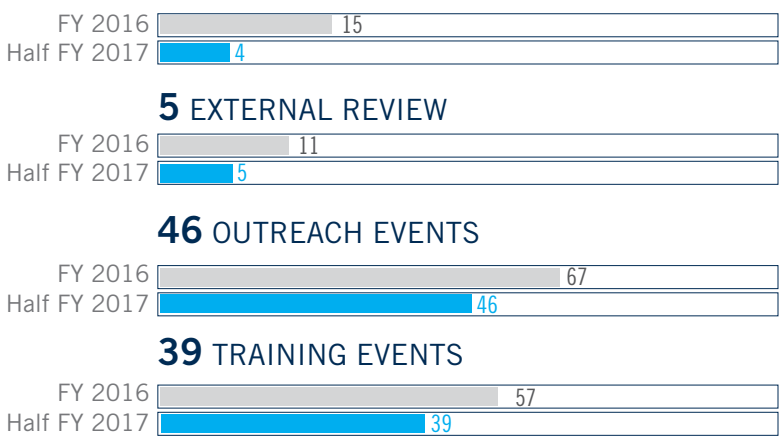
In the first half of FY 2017, ICW&SP processed four Congressional disclosures. These disclosures included employees from the Department of Health and Human Services, the Department of Defense, the IC IG, and the National Geospatial-Intelligence Agency. Content included allegations ranging from failure of personnel security programs to contract procurement irregularities.

The IC IG typically does not investigate every allegation, but forwards them to the SSCI and HPSCI for their review and disposition.

External Reviews

PPD-19 not only ensures a protected path for IC employees and contractors to lawfully report wrongdoing, it also prohibits retaliation against employees and contractors for reporting wrongdoing. As part of this policy, PPD-19 provides an external IG review process for an employee who has exhausted the applicable review process of their respective agency. ICW&SP manages the External Review Panel





(ERP) process on behalf of employees and contractors who request a review of local agency whistleblowing reprisal reviews. In these reviews the employee alleges whistleblower retaliation through adverse actions and/or decisions affecting eligibility for access to classified information. ICW&SP reviews available information for each request and provides a recommendation to the IC IG as to whether a specific case warrants convening the three-member PPD-19 ERP. ICW&SP briefs the IC IG Forum members, IC senior leaders, and IC employees, contractors, and stakeholders on the results of completed reprisal investigations in an effort to further accountability-focused directives and policies aimed at reducing reprisals.

In the first half of FY 2017, ICW&SP received five new external review requests, indicated above, and continues to process cases carried over from FY 2015 and FY 2016.

Outreach

ICW&SP's outreach goal is to use all communication media available to advance an IC professional culture respecting whistleblowing as a Federal mission. This involves promoting awareness of IC whistleblowing policies, procedures, and protections; why whistleblowing is important; how the process works; and how the workforce will be supported when coming forward with a disclosure of wrongdoing.

The outreach audience includes IC element employees and federal contractors as potential whistleblowers, as well as opinion leaders and enablers who either inform or assist potential whistleblowers.

To further extend outreach, ICW&SP is developing an IC Whistleblowing Outreach Web Tool targeted for launch on the ODNI's unclassified network in the late Spring of 2017. A classified application is planned to follow soon thereafter. The IC Whistleblowing Outreach Web Tool will be available to the IC workforce, including supervisors and managers, as well as whistleblowing stakeholders across the legal, academic, corporate, and government communities.

During the first half of FY 2017, ICW&SP conducted 46 outreach events and continued quarterly field visits to employees and contractors in Colorado and New Mexico. These trips included visits to two Department of Energy national laboratories (Sandia and Los Alamos), as well as the New Mexico All- Source Intelligence Center. Locally, outreach included the National Intelligence University, the University of the District of Columbia's David A. Clark School of Law, and the Georgetown Government Affairs Institute.

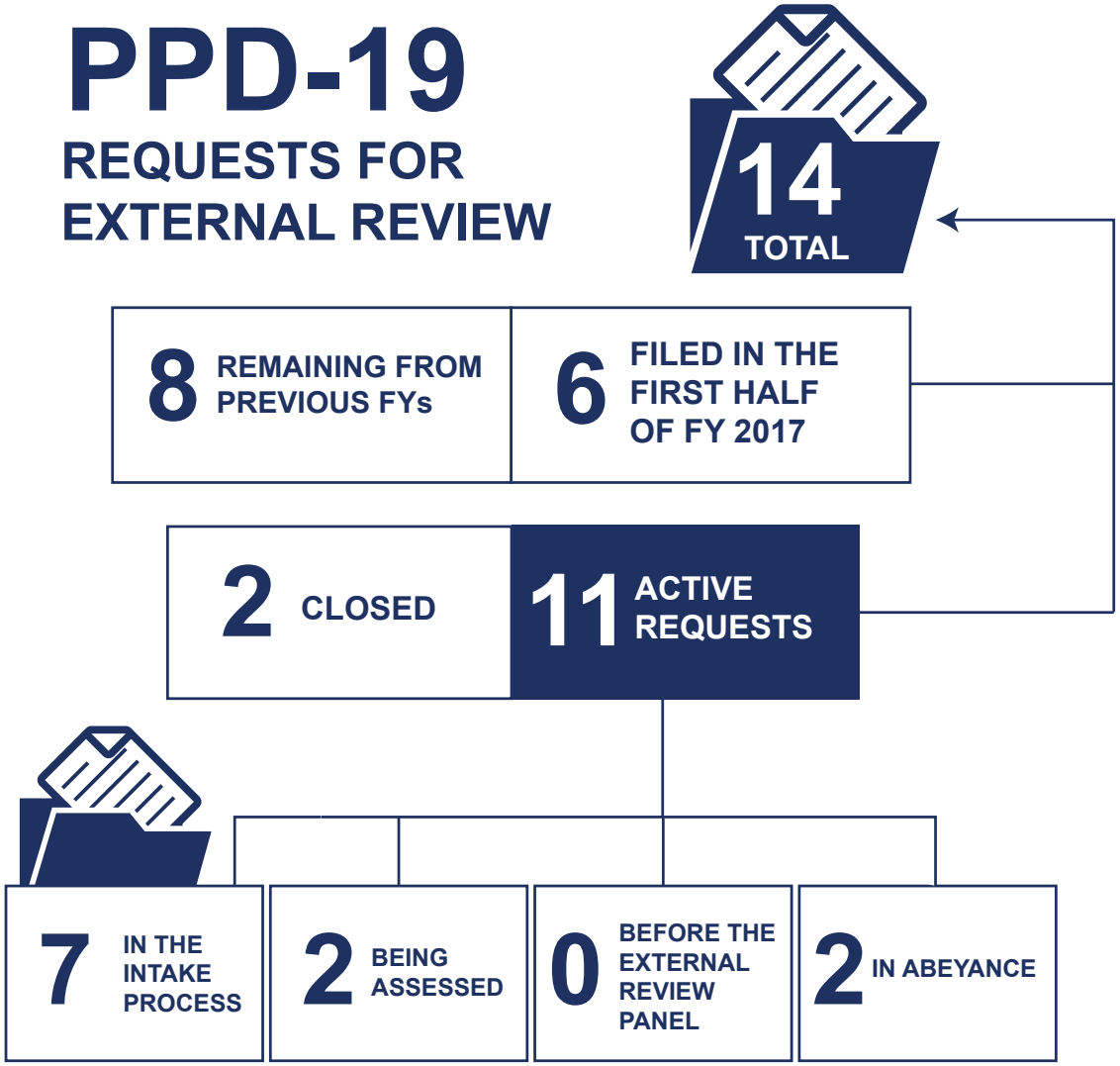
Training

ICW&SP conducts training – distinct from outreach – for IG personnel executing PPD-19 and ICD 120. ICW&SP does not conduct agency workforce training, but rather trains IG personnel enabling the IC whistleblowing mission.

In addition, ICW&SP prepares tailored training materials for the IG supervisors and managers as they provide specialized instruction to their workforce on implementing PPD-19. These activities give participants an opportunity to share concerns and experiences with one another.

In the first half of FY 2017, ICW&SP conducted 39 training events (76 percent of the 51 events conducted in FY 2016), including the following:

- National Security Agency investigators and leadership
- Department of Energy Office of the IG
- Department of Labor Annual Employment Retaliation Law Conference
- Council of Inspectors General on Integrity and Efficiency (CIGIE) leadership
- Whistleblower Protection Ombuds Working Group
- IC IG Annual Conference




COUNSEL

IC IG COUNSEL PROVIDES INDEPENDENT, OBJECTIVE, AND CONFIDENTIAL LEGAL ADVICE ON A VARIETY OF LEGAL AND POLICY ISSUES THAT EFFECT THE IC IG MISSION. COUNSEL MANAGES FOUR MAIN PORTFOLIOS: LEGAL AND POLICY REVIEWS, LEGISLATIVE REVIEWS, ETHICS REVIEWS, AND CONGRESSIONAL ENGAGEMENTS.

The IC IG Office of the General Counsel's primary responsibility is to ensure the IC IG receives independent advice and counsel that is 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 for legislative and congressional engagements.

Legal and Policy Advice

During this reporting period, we continued outreach to IC IG staff, ODNI components, and fellow IC Counsels to ensure incorporation of IG equities and statutory requirements into policy guidance. We also reviewed and provided appropriate feedback on proposed ODNI and IC authorities to advocate for, and ensure the preservation of IG equities.

We worked closely with the Executive Director for IC Whistleblowing on education and outreach efforts to ensure consistency with evolving legal and policy developments. The Executive Director is developing a public, web-based educational tool that provides information on the proper method for disclosing concerns within the IC; IC employee and contractor whistleblowing protections; and the IG whistleblower reprisal allegation review processes. The legal reviews conducted by the IC IG Forum Counsel committee will assist in meeting the website's target launch date at the end of this fiscal year.

In addition, the IC IG General Counsel has engaged with ODNI legal and policy offices to protect IC IG equities on several critical IC-wide policy issues. For example, the IC is undertaking an initiative to revise policies related to unauthorized disclosures of classified information. We have reviewed these policies and participated in coordination discussions to ensure that the revised policies do not infringe upon the IC IG's, and other IGs' ability to conduct independent and objective administrative investigations into unauthorized disclosures.

Operational, Administrative, and Ethics Reviews

The IC IG General Counsel staff provides timely advice to the entire IC IG organization. For example, we routinely work with investigators during the course of an investigation to identify potential legal issues. This collaboration presents opportunities for counsel to identify areas requiring further examination and provide effective legal guidance throughout the investigative process.

During this reporting period, we identified key policy aspects for the IC IG inspectors conducting component and intelligence oversight reviews. The General Counsel staff also provided legal and policy guidance for IC IG administrative efforts such as personnel, training, budgetary, and conference issues.

IC IG General Counsel also reviewed IC IG staff Office of Government Ethics (OGE) mandatory financial disclosures, a part of the ODNI Ethics Program. The General Counsel reviewed OGE financial disclosure forms for personal conflicts of interest to protect the credibility and objectivity of the IC IG mission. We reviewed IC IG personnel independence statements to ensure there were no personal impairments that may impugn the work of an auditor, inspector, or investigator under these functional area related standards. With the presidential election occurring this reporting period, we highlighted the importance of IC IG

personnel complying with the *Hatch Act's* partisan political activity restrictions.

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 various issues and initiatives of mutual interest to IG Forum members. For example, the committee discussed how the *IG Empowerment Act's* transparency provisions affect oversight of an IC element's classified mission. We also discussed unique *Vacancy Act* requirements for current and upcoming vacant IG positions.

Performing and Supporting Legislative Development and Congressional Engagements.

The IC IG frequently engaged Congress this reporting period. We provided seven bipartisan Congressional briefings on recent IC IG reports and the fiscal year 2017 work plan, submitted three *IC Whistleblower and Protection Act* disclosures to the Intelligence Oversight Committees, and provided technical assistance on proposed legislation. IC IG received its first Congressional request to brief committee staff on IG oversight processes and practices during this reporting period.

On January 4, 2017 - at the beginning of the 115th Congress - IC IG Audits, Inspections and Evaluations, and Investigations leadership briefed the House Permanent Select Committee on Intelligence (HPSCI) bipartisan staff on IG authorities, standards, and intra-IC OIG organizational distinctions. We also covered core mission objectives, standards, procedures, and functions associated with IG audits, inspections, investigations, and intelligence oversight. IC IG presenters described the full lifecycle of an IG review from project initiation through recommendation tracking. HPSCI staff provided positive feedback on the briefing, which provided better insight on how IG's conduct oversight.

The Senate Select Committee on Intelligence (SSCI) staff requested a briefing on *Reducing Over-Classification Act* (ROCA) review findings. The IC IG led a joint presentation with CIA, DIA, NRO, NGA, and NSA IG professionals on their respective ROCA review findings. This coordinated briefing gave SSCI staff an opportunity to hear and ask questions about each agency's report and findings in a single session.

In addition, we updated the Congressional committees on the *Intelligence Community Whistleblower Protection Act* procedures and the IG process for reviewing employee complaints of Urgent Concern. We continued to engage with OMB, Congressional staff, the ODNI Office of General Counsel, IC IG Forum Counsels, and the Counsel of the Inspectors General on Integrity and Efficiency (CIGIE) on congressional mandates and relevant bills. During this reporting period, we submitted several legislative proposals for inclusion in the *Intelligence Authorization Act of Fiscal Year 2018*, and provided legislative technical drafting assistance.

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 General Counsel's office closely tracked and commented on the *Inspector General Empowerment Act of 2016*, the *Administrative Leave Act of 2016*, the House and the Senate *Intelligence Authorization Acts for Fiscal Year 2017*, and the *Consolidated Appropriations Act of 2016 and 2017.*

3
DISCLOSURES ★

0
HEARING ★

0
CONGRESSIONAL NOTIFICATIONS ★

9
HILL BRIEFINGS ★

These numbers reflect this reporting period.

Abbreviations and Acronyms

AFR	Agency Financial Report
AUD	Audit Division (IC IG)
CFO	Chief Financial Officer (ODNI)
CIA	Central Intelligence Agency
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer (ODNI)
CISA	Cybersecurity Information Sharing System
CLPT	Civil Liberties, Privacy and Transparency
CMO	Chief Management Officer (ODNI)
CT	Counterterrorism
DDNIR	Domestic DNI Representative
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
DSOP	Directorate of Strategic Operational Planning
EO	Executive Order
ERP	External Review Panel
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Modernization Act
FISC	Foreign Intelligence Surveillance Court
FLETC	Federal Law Enforcement Training Center
FOIA	Freedom of Information Act
FY	Fiscal Year
GC	General Counsel (IC IG)
GSA	General Services Administration
HOGR	House Oversight and Governmental Reform Committee
HOGR	House Oversight and Government Reform Committee
HPSCI	House Permanent Select Committee on Intelligence
I&A	Office of Intelligence and Analysis (DHS)
I&E	Inspections & Evaluations Division (IC IG)
IARPA	Intelligence Advanced Research Project Activity (ODNI)
IC	Intelligence Community
IC IG	Office of the Inspector General of the Intelligence Community
IC ITE	Intelligence Community Information Technology Enterprise
ICW&SP	Intelligence Community Whistleblower & Source Protection Office
ICWPA	Intelligence Community Whistleblower Protection Act
IG	Inspector General
IMD	Information Management Division (ODNI)
INS	Inspection (IC IG)
INV	Investigations Division (IC IG)
IPERIA	Improper Payments Elimination and Recovery Improvement Act
IT	Information Technology
M&A	Management & Administration (IC IG)
MSD	Mission Support Division (ODNI)
NCTC	National Counterterrorism Center
NGA	National Geospatial-Intelligence Agency

Abbreviations and Full Name

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
OSC	Office of Special Counsel
PPD	Presidential Policy Directive
RMF	Risk Management Framework
ROCA	Reducing Over-Classification Act
SOC	System & Organization Control
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 and intake processes provide 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.

THE IC IG LOGGED

132 CONTACTS

THIS REPORTING PERIOD

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