OFFICE *of the* INSPECTOR GENERAL
of the INTELLIGENCE COMMUNITY

SEMIANNUAL REPORT

April 2017–September 2017

Wayne A. Stone
Acting Inspector General of the Intelligence Community

Table *of* Contents

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

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 IC IG issued no subpoenas this reporting period.
- Select completed investigations begin on page 19.
- The updates on whistleblower matters begin 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 11. Corresponding corrective actions are listed in the classified annex.

Conference Reporting

Section 305 of the Consolidated Appropriations Act of 2016 (PL 114-113) requires the Director of National Intelligence (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 April 1, 2017 and September 31, 2017, the DNI notified the IC IG of **56** 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 costs the U.S. Government more than $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.

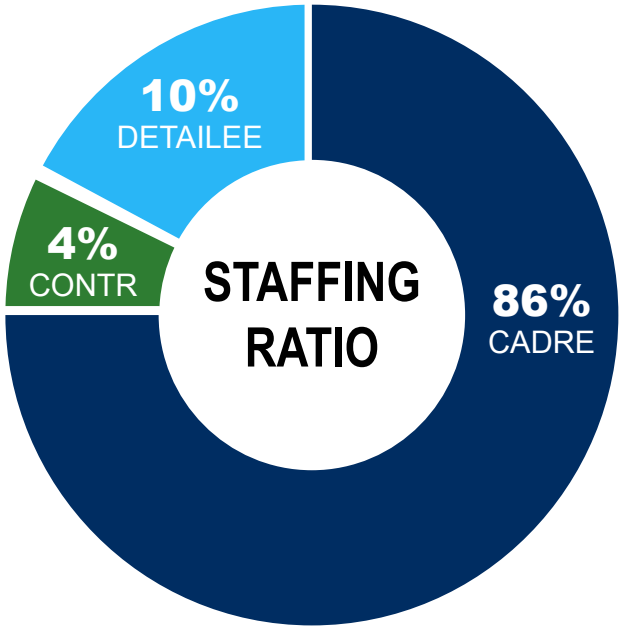
The principal operational divisions are Audit, Inspections & Evaluations, and Investigations. The Management & Administration Division and the General Counsel's Office support the operational divisions and the IC IG Front Office. The Executive Director for Intelligence Community Whistleblowing & Source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

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 point of contact.

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 Office of the Director of National Intelligence (ODNI) provided funding that was adequate 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:

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

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.

Committee Updates

Deputy Inspectors General

The Deputy Inspectors General met this reporting period on several key initiatives to support IC IG Forum activities. For example, the Deputies developed a new IC IG Award category to recognize IG professionals whose work impacted the IC beyond their own agency. The IGs approved this new award category for inclusion in the 2018 award season.

Audit

In June 2017, the IC IG Audit AIG led a discussion on the April 2017 IC Cloud Transition Report and the systemic challenges and efficiencies associated with IC elements transitioning to the IC Cloud. The Committee also discussed the joint report on the IC implementation of Section 107 of the *Cybersecurity Information Sharing Act of 2015*. Additionally, Government Accountability Office representatives briefed the committee on how to determine the potential monetary benefits from OIG recommendations.

In September 2017, the Audit Committee hosted the ODNI Assistant Director, Supply Chain Directorate, National Counterintelligence Security Center, who discussed information technology Supply Chain Risk Management implications to the IC. She provided an overview of service offerings and emphasized the importance of seeking guidance in the early planning stages of IT acquisitions to mitigate potential CI risks. The Committee also discussed FY 2017 *Federal Information Security Modernization Act* (FISMA) report submissions and FY 2018 OIG work plans.

Also in September, an IC IG auditor briefed the Council of Inspectors General on Financial Oversight (CIGFO) on the *Cybersecurity Information Sharing Act of 2015* joint report. The *Cybersecurity Information Sharing Act (*CISA) Section 107(b) requires the IGs of the ODNI and the DoD, DOE, DHS, DOJ, DOT, and the Department of Commerce, in consultation with CIGFO, to submit a joint interagency report to Congress on the executive branch of the Federal Government's actions to implement CISA. The auditor provided CIGFO the status, timing, and process of the joint report. CIGFO members will review the draft report before it is issued in December 2017.

Counsel

The IC IG Counsel Committee discusses common issues and interests and promotes consistent authority interpretation. The Counsels collaborated on key initiatives including a policy review of their respective agency personnel rotational policies. This review will enable IC IG Forum Members to address agency personnel rotational policies while fiercely protecting IG independence and preserving career options for IG personnel seeking career enhancing

opportunities outside of the IG arena. In addition, the IC IG Counsels reviewed several provisions within the respective House and Senate Intelligence Authorization Bills for FY 2018. The counsels 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.

Information Technology

The IC IG Forum IT Committee held two meetings this reporting period. In May, the National Aeronautics and Space Administration (NASA) Office of Inspector General (OIG) hosted IT Committee Members at NASA Headquarters. Members were briefed on the capabilities of the NASA Advanced Data Analytics Program, as well as techniques to leverage current technology to improve efficiency and effectiveness.

NGA OIG hosted the September quarterly meeting where members received a detailed overview of NGA OIG data analytics processes, including tips on OIGs developing their own internal data analytics capabilities. The presentation provided timely and useful information that four OIGs plan to leverage in the near term. Members also discussed plans to continue updating the IT application survey and future efforts to broaden the survey tool to enhance organizational insight and to seek possible opportunities focused on unifying efforts for related applications.

Inspections Committee

The Inspections and Evaluations (I&E) Committee hosted CIGIE's Director of the Leadership & Mission Support Academy for a presentation on current and planned professional development opportunities. Members heard about the Audit, Inspections & Evaluation Academy and on leadership training corresponding to the full career span of an IG professional with training for emerging, new, and experienced leaders currently available.

The head of NASA OIG's Advanced Data Analytics Program briefed the Committee on how data analytic tools can enable the identification of emerging risk, make oversight processes more efficient and effective, and complement the more traditional all-source analytic techniques. Federal Government use of data analytics is increasingly the norm. Members giving consideration to adding or expanding a data analytics capability have visited NASA OIG for an up-close look at their program operations and how data analytics are being applied to oversight reviews.

During the fourth quarter, the I&E Committee discussed external peer reviews that will soon be mandatory under CIGIE for all OIG Inspection programs. These have been underway since 2014 by CIA, DIA, NGA, NRO, NSA and IC IG under the auspices of the IC IG Forum.

A CIGIE I&E Committee representative updated members on status and future plans for implementing government-wide peer reviews, including incorporating additional mandatory standards. Currently, seven of the fourteen CIGIE quality standards must be included in Inspections program peer reviews. After this presentation, Committee members discussed the need for consistent implementation of the CIGIE Peer Review Guide for Conducting I&E Peer Reviews. NGA will lead a follow-on discussion at the December 2017 committee meeting.

Finally, the DoD AIG for Administrative Investigations shared his perspectives on using recording devices for I&E interviews. The AIG identified practical and process considerations before introducing the use of recording devices in an Inspections program.

Five Eyes Intelligence Oversight and Review Council

The IC IG Forum members continued to prepare for the upcoming Five Eyes Intelligence Oversight and Review Council (FIORC) Conference. Intelligence oversight agency representatives from Australia, the United Kingdom, Canada, New Zealand, and the United States agreed to focus this year's conference on signals intelligence oversight and transparency. Signals intelligence is of paramount concern to IC IG Forum members, and IGs throughout the Intelligence Community, particularly the DoD, DOJ, and NSA.

The FIORC conference's focus on signals intelligence will provide opportunities to share insights, best practices, lessons learned, perspectives, and creative ways to collaborate on oversight methodologies that enhance IG efficiency and Five Eyes Collaboration. The FIORC Conference will be held in Ottawa, Canada October 2-3, 2017.

RECOMMENDATIONS

Recommendations Summary

Report Name	Issued	Total	Open	Closed this period
2017				
Audit: FY 2016 Independent Evaluation of ODNI Compliance with FISMA	September	1	1	0
Inspection: ODNI Information System Deterrence, Detection, and Mitigation of Insider Threats	September	19	19	0
Inspection: ODNI National Counterterrorism Center/Directorate of Strategic Operational Planning	September	4	4	0
Inspection: ODNI Office of General Counsel	March	4	0	4
Inspection: Joint Review of Domestic Sharing of Counterterrorism Information*	March	*6	2	4
2014				
Audit: FY 2014 Independent Evaluation of ODNI Compliance with FISMA	November	2	0	1
2013				
Audit: Study: IC Electronic Waste Disposal Practices	May	5	1	0
2012				
Audit: FY 2012 Independent Evaluation of ODNI Compliance with FISMA	December	12	0	1
Audit: IC Security Clearance Reciprocity	December	2	2	0
	Totals	55	29	10

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

A detailed list of 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 Audit Projects

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

FISMA requires an annual independent evaluation of federal agencies' information security (IS) programs and practices. The IC IG assessed the ODNI program's effectiveness and status for ODNI's internal operations using the June 2015 Department of Homeland Security FY 2015 Inspector General FISMA metrics. We reported that for FY 2016, the ODNI IS program did not meet DHS metrics for the following six program areas:

- Continuous Monitoring Management
- Configuration Management
- Incident Response and Reporting
- Risk Management
- Plan of Action and Milestones
- Remote Access Management

For the remaining four program areas, ODNI Chief Information Office officials did not provide sufficient information to indicate whether the program met the following DHS metrics:

- Identity and Access Management
- Security Training
- Contingecy Planning
- Contractor System

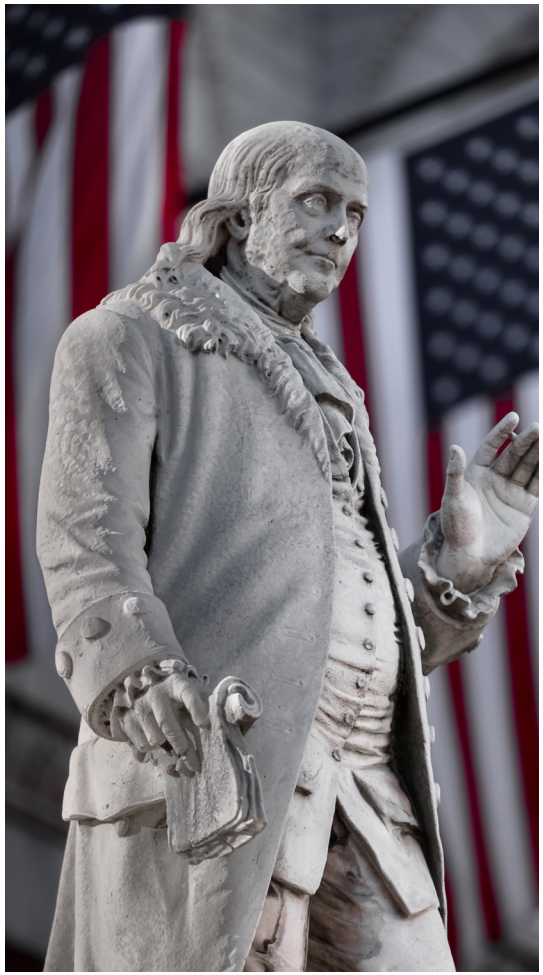
The information in our September 27, 2017 report will be included in an IC FISMA capstone report to be issued during the next fiscal quarter.

AUD-2017-004: ODNI Implementation of the Cybersecurity Information Sharing Act of 2015, Section 107, Oversight of Government Activities

The IC IG reviewed and summarized ODNI's reported actions in calendar year 2016 to comply with requirements defined in Section 107 of the 2015 *Cybersecurity Information Sharing Act*. The objective of this project was to summarize ODNI's assessment of actions taken during CY 2016 to carry out the CISA's requirements, which included:

- 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;
- 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 will include the findings of this August 23, 2017 report in the joint IG report to Congress that we will issue on or before December 18, 2017.



Pictured: Statue of Benjamin Franklin at Old Post Office building, Washington DC

Ongoing 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 focuses 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 eleven IC elements' information security programs by highlighting the strengths and weaknesses their OIGs identified, and provide a brief summary of recommendations made for IC information security programs. We will apply the DHS's FY 2015 Inspector General FISMA metrics issued in June 2015 to perform this evaluation.

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 directs the Inspectors General of seven organizations (Department of Commerce, DoD, DOE, DHS, DOJ, DOT, and ODNI) to submit, in consultation with the IC IG and CIGFO, a joint interagency report to Congress on those agencies' implementation of the *Cybersecurity Information Sharing Act* requirements.

The Act also sets forth the content requirements of the report. We will jointly report on actions taken during the CY 2016 to carry out CISA requirements. Specifically, the report will include:

- 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;
- 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.

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

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. The safeguards and internal controls should address agency responsibilities for preventing and identifying illegal, improper, and erroneous purchases. Office of Management and Budget (OMB) Memorandum, "Implementation of the *Government Charge Card Abuse Prevention Act of 2012*," requires IGs 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 IGs should use risk assessment results to determine the scope and frequency of audits or reviews of those programs. Our objective is to review the ODNI charge card program to identify and assess the risk of illegal, improper, and erroneous purchases and payments. This assessment is scheduled to be completed in October 2017.

Audit Projects Planned, Not Initiated

FY 2017 ODNI Compliance with the Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act requires an annual independent evaluation of federal agencies' information security program and practices. We will evaluate ODNI's IS program effectiveness and status using the September 26, 2016 DHS FY 2016 Inspector General FISMA metrics.

FY 2017 Consolidated Federal Information Security Modernization Act of 2014 Capstone Report of the Intelligence Community Elements' Inspectors General

This project will focus on the FY 2017 FISMA report submissions from the OIGs for the IC elements operating or exercising control of national security systems. We will summarize eleven IC elements' information security programs and highlight the strengths and weaknesses their OIGs identified. We will also provide a brief summary of the recommendations made for IC information security programs. We will apply the September 26, 2016 DHS FY 2016 Inspector General FISMA metrics to perform this evaluation.

Evaluation of the Office of the Director of National Intelligence Fiscal Year 2017 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 to identify any programs or activity payments that may be susceptible to significant improper payments. OIGs are required to submit the review 180 days after the agency publishes its agency financial report (AFR). We will initiate our review once ODNI publishes its AFR in November 2017.

Pictured: Statue of George Washington in front of Federal Hall, New York


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-2017-004: Report of Inspection: National Counterterrorism Center, Directorate of Strategic Operational Planning Special Review

The Inspections & Evaluations Division completed an inspection of the National Counterterrorism Center's Directorate of Strategic Operational Planning (NCTC/DSOP). By law, one of NCTC's missions is to conduct strategic operational planning for counterterrorism activities across the U.S. Government (USG).

DSOP fulfills this responsibility by integrating all instruments of national power, including diplomatic, financial, military, intelligences, homeland security, and law enforcement, to ensure unity of effort. DSOP coordination officers and assessment officers work with National Security Council staff and all USG departments and agencies to develop strategies, action plans, and assessments to integrate and evaluate all USG counterterrorism capabilities. I&E last inspected NCTC in 2012.

Additional details of this report are in the classified annex.

INS-2017-007: Assessment of ODNI Information System Deterrence, Detection, and Mitigation of Insider Threats

In response to congressional direction, we assessed ODNI's progress implementing its insider threat program (ITP), implementation of safeguards to protect employee privacy and civil liberties, and measures of effectiveness used to determine whether ODNI's ITP detects and deters insider threats. We also assessed ODNI's efforts to identify and remediate information system vulnerabilities on classified networks that an insider threat could exploit.

Additional details of this report are in the classified annex.

Peer Review

During this reporting period, IC IG I&E Division underwent an external peer review by an interagency team led by DOS OIG, with participation from CIA, FBI, and NRO OIGs. The review was conducted under the auspices of the IC IG Forum Peer Review Program and in accordance with the 2017 CIGIE Guide for Conducting Peer Reviews of I&E Organizations of Federal OIGs. The IC IG I&E Division was last peer reviewed in 2014.

The external peer review team determined that IC IG I&E Division's policies and procedures generally met the seven Blue Book standards addressed in the external peer review. Of the four reports reviewed, all generally met the Blue Book standards, and complied with IC IG I&E Division's internal policies and procedures. The review team also provided two observations for improvement pertaining to quality control, and we fully concurred with these findings.

This reporting period, IC IG I&E Division inspectors collaborated with interagency teams to conduct external peer reviews of CIA, DIA, and NGA OIG inspections programs. The results of those peer reviews will be reported in those agencies' respective Semiannual Reports.

Ongoing Reviews

The IC IG I&E Division currently has four ongoing reviews.

Additional details of this report are in the classified annex.


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 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, ten other federal law enforcement organizations, and OIGs. We expect this investigation to continue into the next reporting period.

Select Completed Investigations

INV-2016-0004: Time and Attendance Fraud

IC IG initiated an investigation with DOJ OIG after receiving an allegation from an ODNI supervisor reporting concerns about an ODNI cadre employee's time and attendance, and possible misuse of Military Leave. The investigation concluded that the subject likely violated the statutory prohibition on dual compensation and made false statements in connection with his military duties. The U.S. Attorney's Office for the Eastern District of Virginia declined prosecution. The matter was referred to the Department of the Army for action as appropriate. The ODNI is separately pursuing collection of the improperly earned income.

INV-2017-0001: Unauthorized Media Contacts

The IC IG opened an investigation after learning an ODNI officer was alleged to have participated in an on-air discussion with a national media outlet. Her remarks were aired live during a call-in segment of the show during which she discussed the Benghazi attacks, military surveillance assets in the area, and CIA and DOS roles. This "covered matter" and her disclosure of her affiliation with the ODNI were unauthorized, and the officer received a Letter of Warning.

INV-2017-0003: Government Travel Card Abuse

IC IG initiated an investigation in response to an allegation that an ODNI cadre officer misused his Government Travel Card (GTC). An analysis of the subject's GTC statements indicated he used his GTC for personal charges and cash withdrawals totaling $4,495. The investigation also learned the subject received a $1,500 cash advance for training he did not attend. The U.S. Attorney's Office for the Eastern District of Virginia declined prosecution. The matter was referred to a Personnel Evaluation Board; and the officer, with eleven years of service, was terminated and his security clearance was revoked.

INV-2017-0007: Time and Attendance Fraud

An IC IG investigation substantiated significant time and attendance fraud along with GTC abuse. The subject falsely claimed 593 hours. Additionally, he knowingly and willfully misused his GTC for over $40,000 in personal expenses and ATM cash withdrawals. The U.S. Attorney's Office for the Eastern District of Virginia declined prosecution. The matter was referred to a Personnel Evaluation Board; and the officer, with 20 years of combined federal service, resigned in lieu of termination and his security clearance was revoked.

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

As intelligence professionals, our employees, supervisors, and managers detect, collect, and analyze information for the most insightful intelligence possible on external threats. Intelligence professionals also have a duty to lawfully disclose information regarding potential wrongdoing, including fraud, waste, abuse, and corruption. IC Whistleblowing reveals internal threats undermining the integrity of the IC. Collectively, both these duties with respect to external and internal threats reinforce the national security mission.

Performance by IC Whistleblowing Mission-Function

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 is the program manager for the IC Whistleblowing program.

ICW&SP executed PPD-19 and ICD120 through focused activities in four primary functional areas:

Congressional Disclosures

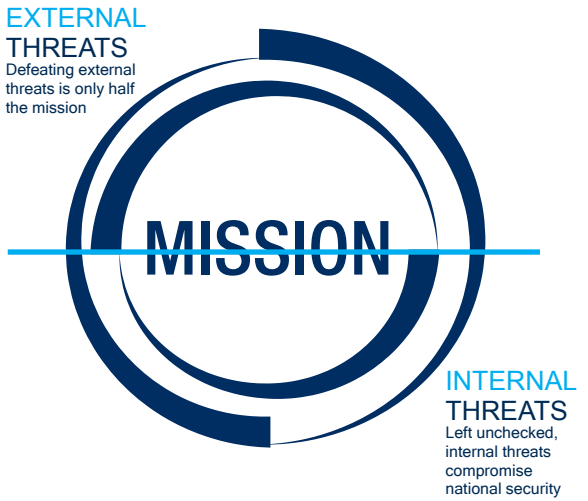
The ICW&SP assists the processing of lawful *Intelligence Community Whistleblower Protection Act* (ICWPA) disclosures to Congress. ICW&SP advises the IC IG as the IC IG Hotline prepares disclosure materials in coordination with the IC IG General Counsel Office.

Six congressional disclosures were processed this reporting period. Disclosers included current or former IC and federal employees and contractors. Content included allegations ranging from reprisal against Congressional sources to mishandling of classified information.

The IC IG forwards both urgent concerns and non-urgent concerns to the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) for review and disposition.

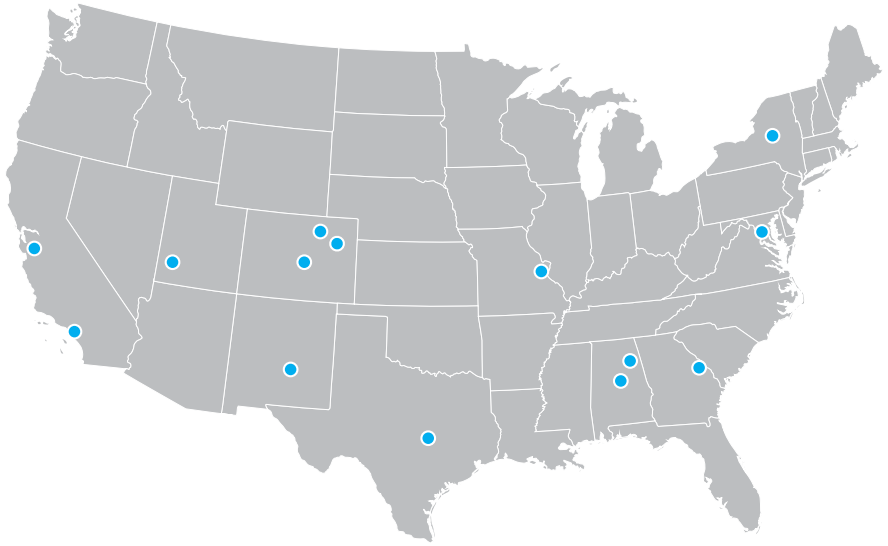
External Reviews

PPD-19 not only ensures a safe path for IC employees and contractors to lawfully report wrongdoing, it also prohibits retaliation against employees and contractors who do. As part of this policy, PPD-19 allows employees to request an external review once an employee/contractor 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 requesting an



THIS REPORTING PERIOD

CONGRESSIONAL DISCLOSURES	EXTERNAL REVIEW REQUESTS	OUTREACH EVENTS	TRAINING EVENTS
6	6	19	11



FY 2017

CONGRESSIONAL DISCLOSURES	EXTERNAL REVIEW REQUESTS	OUTREACH EVENTS	TRAINING EVENTS
15	11	61	50

external review. ICW&SP reviews information provided by the requestor and the home agency and provides a recommendation to the IC IG as to whether a specific case warrants convening the three IG-member PPD-19 ERP. ICW&SP briefs summaries and statistics to 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.

ICW&SP received six ERP requests in the second half of FY 2017 for a total of eleven in FY 2017. ICW&SP also continues to process cases carried over from previous years. During this reporting period, the IC IG completed its second full ERP determination under PPD-19 and determined that the reprisal allegations were unsubstantiated.

Additional details of this review are in the classified annex.

Outreach

ICW&SP supported deployment of a beta version of the IC Whistleblowing Outreach Web Tool for IC stakeholder review. The final version will be available on the IC IG unclassified website in FY 2018. The IC workforce, including supervisors and managers, as well as whistleblowing stakeholders across the legal, academic, corporate, and government communities will benefit from this wonderful information tool.

In addition, the ICW&SP has been a valued resource to other IC IG Forum offices as they promote their own internal policies and procedures for whistleblower protections. To this end, the ICW&SP continue to provide tailored support to those OIGs in their efforts as requested.

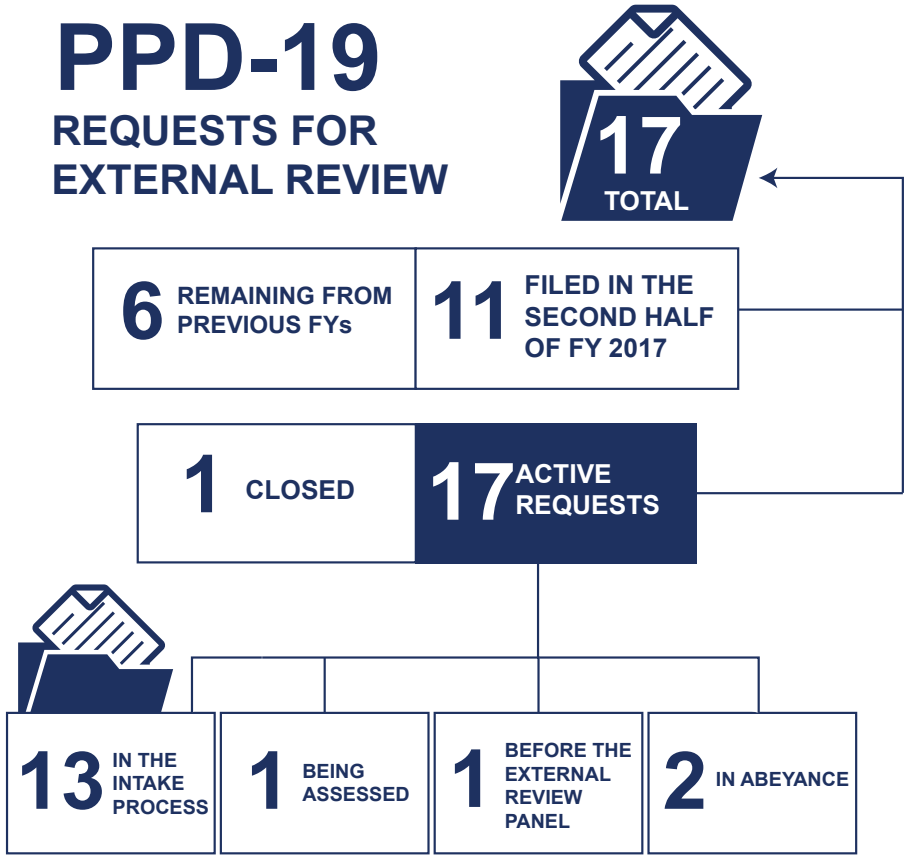
ICW&SP completed **15** events in this reporting period. These included events for the University of the District of Columbia, American University, the National Counterterrorism Center, and the National Intelligence University.

Training

ICW&SP formerly conducted training – distinct from outreach – for IG personnel executing PPD-19 and ICD 120. ICW&SP did not conduct agency workforce training, but rather trained IG and other personnel to enable the IC whistleblowing mission.

In addition, ICW&SP prepared tailored training materials for IG supervisors and managers as they provide specialized instruction to their workforce on implementing PPD-19. **Eleven** training events were completed this reporting period for a total of **50** training events in FY 2017.

INTELLIGENCE PROFESSIONALS ALSO 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. 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 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 Reviews

We continued our outreach to educate IC IG staff, ODNI components, and fellow IC counsel about IG equities, and statutory and regulatory requirements. We reviewed and provided appropriate, timely feedback on proposed ODNI and IC authorities that preserve and advocate for IG equities and independence.

We worked closely with the Executive Director for ICW&SP 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 methods for disclosing concerns within the IC; including IC employee and contractor whistleblower protections; and the IG whistleblower reprisal allegation review processes. The IC IG Forum Counsels Committee provided legal reviews to further the goal of launching the tool by the end of this fiscal year.

The IC IG General Counsel also engaged with ODNI legal and policy offices to protect IC IG equities on critical IC-wide policy issues, notably including revisions related to unauthorized disclosures of classified information – an administration high priority concern. We 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.

Operational, Administrative, and Ethics Reviews

The IC IG General Counsel staff provides timely advice to the entire IC IG organization. We support the Investigations Division generally and 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.

For the I&E Division, we identified and interpreted key policy and contract provisions dispositive to its observations, findings, and recommendations as provided in its numerous component and intelligence oversight reviews.

The General Counsel staff also provided 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 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 might impugn the work of an auditor, inspector, or investigator under these functional area 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. We provided several bipartisan Congressional briefings on recent IC IG activities, submitted **six** ICWPA disclosures to the Intelligence Oversight Committees, submitted several legislative proposals for inclusion in the *Intelligence Authorization Act of Fiscal Year 2018*, and provided technical assistance on proposed legislation.

In addition, we updated the Congressional committees on ICWPA 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 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 General Counsel's office closely tracked and commented on the *Office of Special Counsel Reauthorization Act of 2017*, the *Geospatial Data Act of 2017*, the *Intelligence Authorization Acts for Fiscal Year 2017*, the *Consolidated Appropriations Act of 2017*, and the *House and Senate Intelligence Authorization Acts of 2018*.

On June 29, 2017, the Acting IC IG, along with the Acting NSA IG, Acting CIA IG, and Acting DoD IG, provided testimony to the HPSCI on OIG oversight. They highlighted 2017 priorities as well as past, ongoing, and future work related to the current insider threat challenges facing the IC.

The Hearing was both well-received and well-attended by HPSCI members. Chairman Nunes and Ranking Member Schiff expressed their gratitude for the testimony and reiterated Congress' reliance upon OIGs as trusted sources for insight into agency operations and resources to better enable informed decision-making.

6
DISCLOSURES ★

1
HEARING ★

0
CONGRESSIONAL NOTIFICATIONS ★

5
HILL BRIEFINGS ★

These numbers reflect this reporting period.

Abbreviations and Acronyms

AFR	Agency Financial Report
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
CLPT	Civil Liberties, Privacy and Transparency
CMO	Chief Management Officer (ODNI)
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
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
GTC	Government Travel Card
HPSCI	House Permanent Select Committee on Intelligence
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
ICW&SP	Intelligence Community Whistleblower & Source Protection Office
ICWPA	Intelligence Community Whistleblower Protection Act
IGs	Inspectors General
INV	Investigations Division (IC IG)
IPERIA	Improper Payments Elimination and Recovery Improvement Act
IS	Information Security
IT	Information Technology
M&A	Management & Administration (IC IG)
NASA	National Aeronautics and Space Administration
NCTC	National Counterterrorism Center
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
SRA	Systems and Resources Analyses (ODNI)
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.

THE IC IG LOGGED

183 NEW EXTERNAL CONTACTS

THIS REPORTING PERIOD

THE IC IG LOGGED

54 NEW INTERNAL CONTACTS

THIS REPORTING PERIOD

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