OFFICE *of the* INSPECTOR GENERAL
of the INTELLIGENCE COMMUNITY

SEMIANNUAL REPORT

April–September 2016

The Honorable I. Charles McCullough, III

Table *of* Contents

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

DISCLAIMER: Cover, p. 6 & 26 photos by James Williams. Stock photos were purchased through Shutterstock. Questions may be directed to the IC IG at 571-204-8149.

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

During this reporting period we (the Office of the Inspector General of the Intelligence Community) conducted inspections and investigations in accordance with standards adopted by the Council of the Inspectors General on Integrity and Efficiency. Audits were conducted in accordance with Generally Accepted Government Auditing Standards.

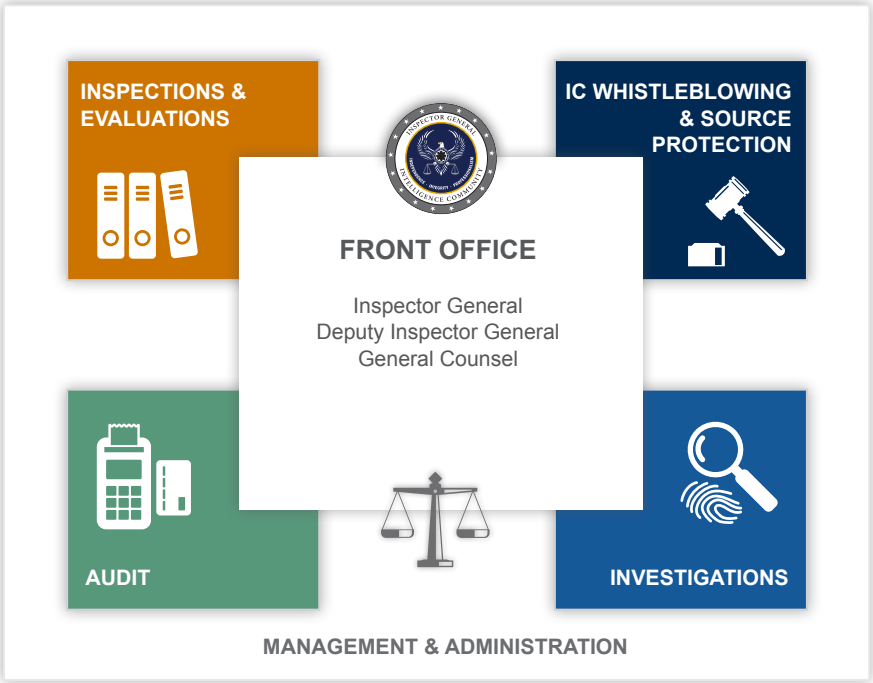
- We had full and direct access to all information relevant to perform our duties.
- The Investigations Division did not issue any subpoenas during this reporting period.
- Select closed investigations are described on page 19.
- The status of whistleblower issues begins on page 21. We processed 14 congressional disclosures and 11 requests for external review in FY 2016.
- A list describing all ongoing and completed audits, inspections, and reviews begins on page 12.
- A list of open recommendations, as well as ones closed this period, can be found on page 10. Corresponding corrective actions are listed in the classified annex of this report.

Our Counsel provided insights on legislation impacting our oversight mission including the Intelligence Authorization Act for 2017. At the request of both the House and Senate Intelligence Committees, we provided technical drafting assistance on provisions in their respective bills that impact IG equities. We also provided input for the IG Empowerment Act, which gives enhanced authorities for federal IGs including testimonial subpoena authority.

ODNI held 30 conferences with cost estimates exceeding $20,000. Details are in the classified annex of this report.

Pictured above: IC IG I. Charles McCullough, III (left) moderated an IG-panel at the 2016 IC IG Annual Conference. Pictured panel members include NGA IG Joseph Composto; DoD Acting IG Glenn Fine; and State IG Steve Linick. Photo by NGA's Office of Corporate Communications.

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 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.

The organization's senior management team includes the Inspector General, Deputy IG, a General Counsel, four Assistant Inspectors General and two program Executive Directors. The principal operational divisions are Audit, Inspections & Evaluations, and Investigations.

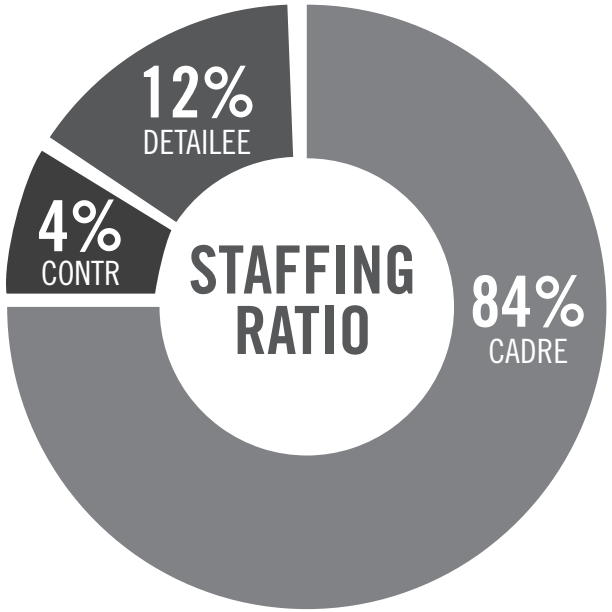
The Management & Administration Division and the General Counsel's office support the operational divisions and the IC IG Front Office. The Executive Director for IC Whistleblowing supports IC-wide Inspector General activities.

Outreach

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

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

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. Staff includes cadre (permanent ODNI employees), joint duty detailees (employees from other IC organizations), and contractors.

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

IC IG FORUM

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

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

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

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

At the end of September, the IC IG Forum welcomed Susan Gibson, NRO's first presidentially appointed and senate confirmed IG. The Forum also welcomed acting NSA IG, Russell Decker, who was Deputy IG under former NSA IG George Ellard, who departed in the spring.

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

Committee Updates

Audit

The Audit Committee met to discuss FY 2017 project plans and ongoing work. They looked at leveraging sampling to improve audit quality, identifying common training needs, and determining how to best respond to sections 107 and 406b of the 2015 Cybersecurity Act.

The committee also focused on gaining a better understanding of the Intelligence Community Information Technology Enterprise (IC ITE). They hosted guest speakers from IC ITE's Desktop Environment, Commercial Cloud Services program offices, and the IC Chief Information Officer to provide an overview of their services and progress made delivering these capabilities to the IC. These briefings assisted committee members' understanding of the IC-wide audit being led by the IC IG on the transition to the IC cloud.

Counsels

The Counsels Committee met several times during the reporting period to discuss matters raised by IC IG Forum members. The committee continued to review and update procedures for IC whistleblowers to request an External Review Panel pursuant to Presidential Policy Directive 19, Section C.

The Counsels also reviewed employee rotational policies and their impact on IG's independence.

Finally, the Counsels discussed enhancing IG oversight efforts in support of PPD-28, which outlines the United States' processes for collecting, retaining, and disseminating foreign intelligence and providing privacy protections for personal information regardless of nationality.

Information Technology

The IC IG Forum established an IT Committee during the last reporting period. The primary focus of this committee is to discuss shared IT challenges, capability gaps, applications, and best practices for collective awareness. The committee is led by co-chairs from the IC IG.

During this reporting period, the committee met with IT representatives from each of the IC IG Forum members. They focused on an initiative to compile a directory of current OIG IT applications, and to identify future IT Committee efforts.

Inspections

The Inspections Committee hosted speakers from the IC Chief Human Capital Office to provide an overview of the annual IC Employee Climate Survey methodology and process, and how survey results can shape action plans to maintain strengths and improve weaknesses.

Another speaker discussed how the recent IC Joint Duty Program expansion to non-IC agencies increases OIG professional career opportunities.

In addition to briefings, committee members shared their experiences using the unclassified, secure collaboration sites Intelink-U and MAX.gov for joint inspection work and information sharing. These sites are more efficient than traditional email and allow multi-agency teams to directly edit products and help eliminate problems with version control. The ongoing joint OIG evaluation by DOJ, DHS, and IC IG on Field-Based Information Sharing Entities is currently being supported by Intelink-U.

Members also discussed plans to be peer reviewed, as well as participate in external peer reviews in FY 2017 and beyond. The Inspections Committee chair will work with CIGIE on peer review schedules for CIA, DIA, IC IG, NGA, NRO, and NSA.

Investigations

The Investigations Committee continued to emphasize the need for community integration. They focused on promptly sharing investigation results among IC elements to safeguard against employees with significant suitability issues from being re-hired in other IC elements.

Management & Administration

M&A committee members supported the IT committee stand-up and prepared for the upcoming IC IG Awards ceremony, but did not have a formal meeting this reporting period.

Five Eyes Review Council

In the previous Semiannual Report, we noted our plans to host the International Intelligence Review Agencies Conference, which meets every two years to discuss IG Intelligence Oversight matters. Due to scheduling complexities and constrained budgets, we scaled the conference down to a meeting with select representatives from Intelligence Oversight Agencies in each of the "Five Eyes" countries.

Pictured above: Dan Meyer, Executive Director for Intelligence Community Whistleblowing & Source Protection (left), and I. Charles McCullough, III, Inspector General of the Intelligence Community during a group discussion at a FVEY intelligence oversight meeting in September 2016. Photo by Andrea Williams.

Pictured above: IC IG General Counsel serving as the new Five Eyes Review Council Executive Secretariat. Photo by Andrea Williams.

Representatives from Australia, the United Kingdom, Canada, New Zealand, and the United States had a successful meeting that resulted in participants agreeing to form a new Intelligence Oversight and Security Review Council.

We offered to serve as the Executive Secretariat for the new Review Council, and plan to organize meetings each calendar quarter. The review group construct will closely mirror other IC international groups, and will assist the IC IG in collaborating on international intelligence oversight issues.

Recommendations Summary

Report Name	Issued	Total	Open	Closed this period
2016				
Inspection: ODNI Mission Support Division	September	10	9	1
Inspection: Intelligence Community Campus-Bethesda	September	5	3	2
Inspection: Program Manager-Information Sharing Environment	February	11	0	4
Inspection: Public Affairs Office	March	3	0	3
2015				
Inspection: Intelligence Community Chief Information Officer	September	4	0	2
2014				
FY 14 Independent Evaluation of ODNI Compliance with FISMA	November	2	1	0
2013				
Study: IC Electronic Waste Disposal Practices	May	5	1	0
2012				
FY 12 Independent Evaluation of ODNI Compliance with FISMA	December	12	1	0
Audit: IC Security Clearance Reciprocity	December	2	2	0
	Totals	**54**	**17**	**12**

The list of open recommendations and ones closed this period is in the classified annex of the report.

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-2015-005: Audit of FBI Compliance with ODNI NIP Guideline for Reprogramming and Transfer Actions of Funds for Fiscal Year 2014

In Fiscal Year 2013, the Congressional Intelligence Committees directed the IC IG to conduct a review of the FBI's National Intelligence Program (NIP) budget reprogramming authorities and execution processes. The audit reviewed FBI NIP reprogramming and transfer actions for FY 2014 to determine compliance with new ODNI NIP reprogramming guidelines.

We found that FBI complied with the Above Threshold Reprogramming (ATR) guidance the DNI issued in FY 2014. The Assistant DNI/ Chief Financial Officer officials stated that reprogramming requests submitted by the FBI were typical of other IC components, but were made during the fourth quarter of FY 2014 and did not afford the DNI sufficient time to determine potential alternatives and recommendations. Differences in the FBI appropriated budget structure and its NIP authorization budget structure impact FBI NIP reprogramming.

We observed the combined efforts of OMB, ODNI, and FBI to improve FBI NIP budget processes, and support the suggestion to embed an ODNI NIP analyst in the FBI Budget Office. Embedding a budget analyst would:

- Facilitate an understanding of the total FBI budget and NIP-funded activities; and increase transparency of FBI NIP-related decisions before they are finalized.
- Keep ODNI staff informed of FBI budget alternatives and reprogramming requests to ensure NIP priorities are addressed; and that adequate support for FBI NIP programs is readily available throughout the budget cycle.
- Ensure a ready awareness of inconsistencies and deficiencies in existing processes and systems.

The ability to keep ODNI and FBI staff informed of ongoing issues and deliberations would mitigate reporting inconsistencies in the FBI NIP, and result in more congruent report formats and timelier submissions. By viewing budgets from the perspective of total NIP and total FBI, the budget analyst could assist each agency in formulating fiscal strategies and adjustments to accommodate both organizations' missions and need for funding flexibilities. The FBI and ODNI are taking steps to adopt this suggestion.

AUD-2016-001: Assessment of the ODNI FY 2015 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 risk assessments to determine the scope, frequency, and number of periodic audits of these programs.

We provided the ODNI Chief Management Officer a memo stating that we determined the risk associated with ODNI purchase card use in FY 2015 to be "low." We found that ODNI had local policies and procedures that address requirements of applicable federal purchase card laws and governing regulations, and reduce the risk of illegal, improper, and erroneous purchases

made using the charge cards. We believe ODNI must continuously monitor its program to ensure the level of service and support card use provided to its geographically dispersed components is maintained; and internal controls in place are operating as intended.

We issued a recommendation status report to OMB on Jan. 7, 2016, stating there were no outstanding audit recommendations pertaining to the ODNI purchase and travel card program.

AUD-2016-002: Evaluation of the Office of the Director of National Intelligence Fiscal Year 2015 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. In accordance with OMB's required three-year risk assessment cycle for low-risk programs, the ODNI was not required to and did not conduct a risk assessment for FY 2015. Therefore, the evaluation and basis for compliance was limited to the IPERIA-related information published in ODNI's FY 2015 Agency Financial Report (AFR).

We also reviewed the corporate functions controls testing that ODNI leveraged to assess improper payment controls, as well as the contract invoice audit process ODNI used to determine the cost-benefit decision for a Recapture Audit in FY 2015. ODNI published IPERIA information in its annual AFR for FY 2015, as required. For FY 2015, ODNI was not required to:

- Conduct a risk assessment for low-risk programs;
- Publish improper payment estimates;
- Publish programmatic corrective action plans in its AFR;
- Publish reduction targets; or
- Publish a gross improper payment rate of less than ten percent for each program with a published improper payment estimate.

ODNI stated in its AFR that it leveraged Corporate Functions controls testing to assess improper payment controls and did not find any areas in its business processes susceptible to significant improper payments. We evaluated ODNI Corporate Functions controls for improper payments and determined that each key Contracts Management process control identified and tested was operating effectively.

Additionally, ODNI conducted a limited scope contract invoice audit of major contractors that did not identify any significant improper payments, which provided the basis for its decision not to conduct a Recapture Audit in FY 2015. We determined ODNI's contract invoice audit process supports the ODNI assertion that a recapture audit was not cost-beneficial for FY 2015. Based on our work, we did not make any recommendations.

The ODNI is required to perform a new risk assessment for FY 2016 of the improper payment risk level for each program and activity susceptible to improper payments. We encourage the ODNI to continue to improve its efforts to prevent and reduce improper payments.

AUD-2016-006: Audit of ODNI's Readiness to Implement the Digital Accountability and Transparency Act of 2014

The Digital Accountability and Transparency Act (DATA) required establishing government-wide financial data standards for federal funds made available to, or expended by, federal agencies and entities receiving federal funds. Beginning in May 2017, agencies are required to report financial and payment information data in accordance with these standards.

DATA also requires federal agency IGs to assess and report on the overall implementation of the standards. We initiated an audit of ODNI's readiness for meeting the requirements of the Act in a timely manner.

After announcing the audit, the OMB's Chief of National Security Division informed us in writing that ODNI was exempt from implementing and reporting these requirements. Consequently, we terminated the audit. If at some point ODNI becomes subject to the requirements, we will initiate an audit in accordance with DATA.

Ongoing Audits

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

The DNI, along with IC leadership, determined that establishing common information technology architecture across the IC could advance intelligence integration and information sharing, and enhance security while creating efficiencies. This common IT architecture is known as the Intelligence Community Information Technology Enterprise (IC ITE).

One key component of IC ITE establishes sharing data, systems, and applications across the IC through a cloud-based architecture known as the

IC Cloud. Transitioning to IC ITE's cloud environment is fundamental to achieving the initiative's overarching goals. However, systems working together in a cloud environment create potential security concerns. In particular, security risks or vulnerabilities to one IC element operating within IC ITE may put all IC elements at risk.

A joint IG survey commissioned by the IC IG Forum, of ten IC elements suggested there may be differing interpretations of policies and requirements, or that the IC elements are not fully aware of their responsibilities for transitioning to the IC Cloud. These observations prompted the IC IG to initiate an audit that:

- Assesses how the IC elements are planning to transition to the IC ITE Cloud environment;
- Determines IC elements' progress in implementing cloud transition plans; and,
- Compares how IC elements are applying the risk management framework to obtain authorizations to operate on the IC Cloud.

The audit team held initial meetings with the 17 IC elements and completed the necessary planning work.

The report is scheduled to be completed during FY 2017.

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 on information related to covered computer systems. Our objective is to review and report the status of policies, procedures, and practices related to system use and data security management. We are conducting our review of ODNI covered computer systems in place as of Dec. 31, 2015.

The report is scheduled to be completed during FY 2017.

AUD-2016-004: FY 16 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, and the IC IG performs this evaluation for ODNI. We are assessing the information security 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 recommendations.

The report is scheduled to be completed during FY 2017.

AUD-2016-005: FY 16 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 identified by their OIGs, 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.

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.

Collaboration

Team members from the Inspections & Evaluation division worked with NSA, NRO, NGA, and three military IGs on a joint inspection of Aerospace Data Facility Colorado. I&E also participated in an NSA-led peer review of NRO Inspections during this reporting period.

Completed Reviews

INS-2016-001: Evaluation of IC Compliance with Foreign Employment Reporting Requirement

We evaluated seven Intelligence Community agencies' compliance with a relatively new reporting requirement regarding post-IC employment for IC government staff. The National Security Act of 1947, as amended, requires the heads of each IC element to issue regulations that require employees in certain positions to report employment by foreign countries and entities.

We conducted interviews and analyzed compliance documentation from the CIA, DIA, NGA, NRO, NSA, FBI, and ODNI. We found those agencies complied with 50 U.S.C. § 3073a requirements. While the agencies effectively implemented the statutory requirements, there are opportunities for more consistency across the IC.

We recommended the DNI consider whether an Intelligence Community Directive would be beneficial to address three areas.

1. When IC employees should sign post-employment reporting agreements.
2. How to provide employee's training on these reporting requirements.
3. How IC element security offices receive such reporting for counterintelligence purposes.

INS-2016-004: Inspection: ODNI Mission Support Division

The Mission Support Division (MSD) reports to the ODNI Chief Management Officer and is responsible for eight support business functions of the ODNI. These functions include:

- Human Resources
- Information Technology and Infrastructure
- National Intelligence Emergency Management Activity
- Security
- Counterintelligence
- Corporate Policy Management
- DNI Watch
- Facilities

MSD brokers support from other agencies for additional services, including logistics, travel, and medical support. MSD's role is to deliver a range of services that enable the core business functions to achieve mission success.

This inspection focused on MSD's management effectiveness, mission performance, resource management, and enterprise oversight.

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

INS-2016-005: Evaluation of ODNI Progress Under the Reducing Over-Classification Act

We assessed ODNI's progress to address policies, procedures, rules, regulations or management practices that may contribute to persistent misclassification of material that we identified in 2014 under the ROCA. This follow-up was directed under the Reducing Over-Classification Act, Public Law 111-258 (Oct. 7, 2010).

In 2014, we identified five deficient areas and made six recommendations for improvement, all of which ODNI successfully closed. The following is a summary of ODNI's corrective actions.

- ODNI restructured the IC Classification Management Program to align monitoring authorities and reporting responsibilities under a single office to provide more effective and efficient oversight.
- ODNI initiated corrective actions for minor discrepancies in Original Classification Authority training records and business processes used to monitor that training.
- The DNI updated ODNI Instruction 10.03, which reduced the number of ODNI positions granted Original Classification Authority from 24 to ten. This helped ensure uniformity and compliance with the minimum number required as outlined in Executive Order 13526.
- The IC Chief Information Office and Mission Support Division began monitoring new ODNI employee training to ensure mandatory derivative classifier training is completed within ten days of arrival. If training isn't complete within that time frame, employee online access is suspended until the training is complete. Related to the training, the Information Management Division enhanced/ updated the derivative classification training online module.
- The Chief Management Officer reminded the ODNI workforce that supervisors and managers are accountable for ensuring classification marking training and processes are in place. The Information Management Division also developed a continuous education campaign to remind managers they must check for over-classification on their reports and products.

ODNI is exploring additional initiatives to address over-classification.

INS-2016-007: Inspection: Intelligence Community Campus-Bethesda

Until 2011, the Bethesda site was home to the National Geospatial-Intelligence Agency and its predecessor agencies. ODNI purchased the 30-acre campus in December 2011 to establish the ICC-B. The Defense Intelligence Agency was appointed the Executive Agent to manage ICC-B construction and operations for members of the IC. This inspection focused on specific ICC-B security, safety, and accessibility issues.

Pictured left: An aerial view during Intelligence Community Campus-Bethesda construction. Photo by ODNI Public Affairs.

Additional details are in the classified annex of this report.

Ongoing Reviews

INS-2015-005: Joint Evaluation of Field-Based Information Sharing Entities

Together with OIG partners at the Departments of Homeland Security and Justice, we are evaluating 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 is in response to a request from Senate committees on Judiciary; Homeland Security and Governmental Affairs; and Intelligence.

This report is scheduled to be completed during FY 2017.

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

We are evaluating how foreign intelligence information was acquired under Title V of the Foreign Intelligence Surveillance Act of 1978 between January 2012 and December 2014. This review will assess how the IC collected, retained, analyzed, and disseminated FISA information, as required by section 106A of the USA PATRIOT Improvement and Reauthorization Act of 2005, as amended by section 108 of the USA Freedom Act of 2015.

This report is scheduled to be completed 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 on 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 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 OIGs. We expect this to continue into the next reporting period.

We continued to make significant investments in employee training. One of our IC IG investigators completed the Federal Law Enforcement Training Center's Criminal Investigator Training Program, graduating with academic distinction. This is our second consecutive investigator to graduate the program with honors, and we have another scheduled to graduate in early 2017. Having Federal Law Enforcement Training Center-trained investigators ensures our officers are trained to the highest professional standards.

Select Completed Investigations

INV-2014-0012: Fraud

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 U.S. Government. The Department of Energy debarred the researcher for ten years and he is now on the GSA's Excluded Parties List System. The researcher pled guilty in federal court to one count of mail fraud and will be sentenced during the next semiannual reporting period.

INV-2015-0005: Labor Mischarging

A joint IC IG/Defense Intelligence Agency criminal investigation substantiated labor mischarging by an Intelligence Advanced Research Projects Activity contract employee while on a Defense Intelligence Agency contract, resulting in a total loss to the U.S. Government of approximately $137,000. The subject was indicted in April 2016 on 13 counts of Theft and False Statements.

INV-2016-0005: Referral

IC IG opened an investigation after learning an individual with Intelligence Community affiliation was arrested by local law enforcement after shooting an acquaintance during a domestic altercation. The subject's identity was confirmed and this case was closed after promptly notifying the respective IC organizations for appropriate action. Within one week of the referral, the subject's clearance was terminated, revoking eligibility for access to classified information.

Conference Reporting

ODNI is required to report conferences it funds with $20,000-$100,000 within 15 days of the date of the conference to IC IG. Between April 1, 2016 and Sept. 30, 2016, ODNI reported 28 conferences meeting this criteria. ODNI is also required to report annually to the IC IG conferences it funds with more than $100,000. ODNI reported two conferences meeting this criteria.

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."

During this reporting period, the IC Whistleblowing program exceeded performance goals in all functional areas: congressional disclosures, requests for external review, training, and outreach. We also decreased the open case load by 60 percent.

Operations

IC Whistleblowing operations fall into two categories:

- Promoting and facilitating lawful disclosures to the Congress through the Intelligence Community Whistleblower Protection Act; and
- Processing requests for external review of PPD-19 whistleblower reprisal investigations conducted by the local Agency inspectors general of the Executive Branch.

In FY 2016, we processed 14 congressional disclosures from employees and contractors across the IC. All congressional disclosures, some of which were considered "urgent concerns," were provided to the House and Senate Intelligence Committees for their review.

The FY 2016 IC Whistleblower Protection Act disclosure content varied and included allegations of compromise of inspector general independence; reprisal by inspectors general; inappropriate giving and acceptance of signing bonuses; reprisal against congressional sources; reprisal for reporting time and attendance violations; failure of communications security; failure of personnel security adjudication systems; and collection failures.

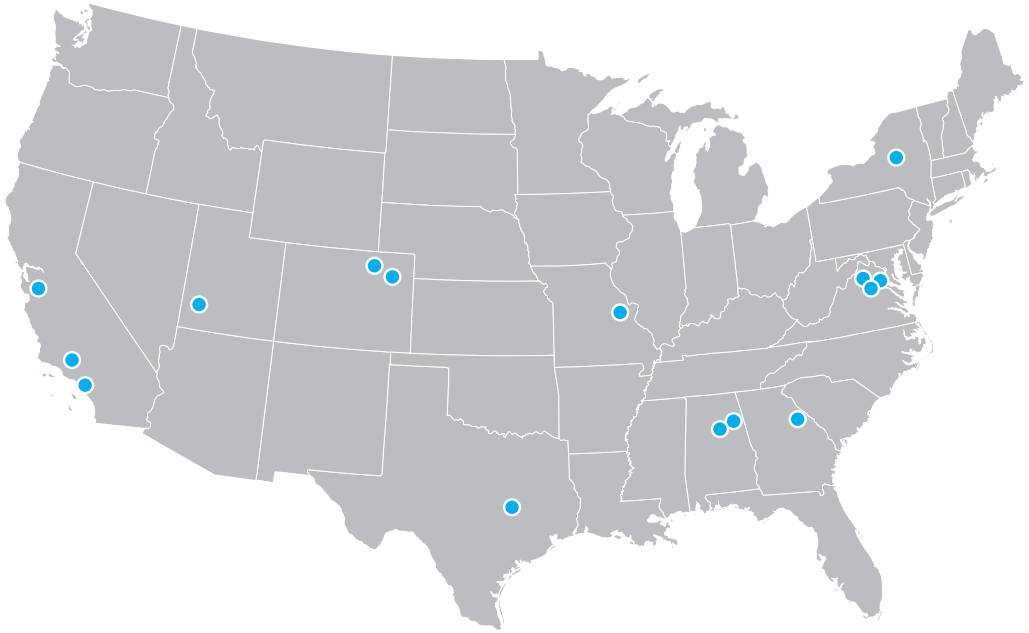
Once a congressional disclosure is made, the IC IG will typically refer the allegations when able to federal entities in a position to address the alleged wrongdoing.

Training

Within IC Whistleblowing's three mission components, the training function is reserved for instructing and educating IG leadership and staff. This is done to preserve the IC IG's independence of agency management of workforce training. While inspectors general may provide subject-matter expertise on a variety of training topics, they are barred from executing workforce training plans in order to preserve the IG's oversight capabilities.

Our training component is focused on IG personnel, congressional personnel, and other oversight personnel responsible *for implementing* PPD-19 and ICD 120. We participated in and hosted the following significant events to advance this mission component in the second half of FY 2016:

- Provided briefings to intelligence and security oversight officials from Australia, Canada, New Zealand, and the United Kingdom;
- Briefed ODNI and DIA supervisors, managers, and employees at the Liberty Crossing and Reston 3 campuses on IC Whistleblowing rights and responsibilities;
- Addressed the House of Representatives Whistleblower Protection Caucus; and
- Briefed the IC IG Forum leadership on local agency requirements under PPD-19 and ICD 120.



IC WHISTLEBLOWING

IC WHISTLEBLOWING HAS LAUNCHED ITS OUTREACH EFFORTS TO:

1. Missouri
2. Texas
3. Georgia
4. Alabama
5. Colorado
6. New York
7. Washington, D.C.
8. California
9. Utah

CONGRESSIONAL DISCLOSURES +127% **14**

EXTERNAL REVIEW +550% **11**

TRAINING EVENTS +146% **51**

OUTREACH EVENTS +172% **67**

We also continue to serve as the Intelligence Community's liaison to the Council of Inspectors General on Integrity and Efficiency's Whistleblower Protection Ombuds working group. This is our primary means of reaching the Executive branch agencies covered under Part B of PPD-19.

Outreach

This function is distinct from the training component of the IC Whistleblowing program. Outreach is directed to those who use the program – the sources who would make disclosures and receive subsequent protections – as opposed to the training function, which is directed toward IG personnel executing the IC Whistleblowing mission. The good governance and civil society stakeholders receiving outreach are typically potential whistleblowers or review requesters, and the opinion leaders and enablers who either inform or assist potential whistleblowers.

To aid in reaching more IC constituents, ICW&SP worked throughout FY 2016 to develop an IC Whistleblowing outreach tool on both the classified and unclassified information systems. This tool will be accessible by IC supervisors, managers, and employees, as well as stakeholders in the overall whistleblowing system. We expect to launch the tool in FY 2017.

Site Visits

To aid local agencies in meeting their Section D PPD-19 requirement to make their IC employees aware of whistleblower protections, we continued quarterly visits to IC element offices located outside the Washington Metropolitan Area. These visits typically included briefings with senior leadership, enabling local offices, and contracting officials. By reaching one of these facilities each quarter of the Fiscal Year, we are helping local agencies execute PPD-19 and ICD 120.

We spoke to employees, contractors, and general federal security clearance holders located in Salt Lake City, Utah, and Dublin, California.

Pictured above: Dan Meyer, Executive Director for IC Whistleblowing & Source Protection speaking to a group of Intelligence Community members about IC Whistleblowing responsibilities and protections. Photo by Andrea Williams.

Our local outreach included visits to Fort Belvoir, Virginia; National Intelligence University; University of the District of Columbia's David A. Clark Law School; the Georgetown Government Affairs Institute; and the Bar of the District of Columbia.

PPD-19 External Review

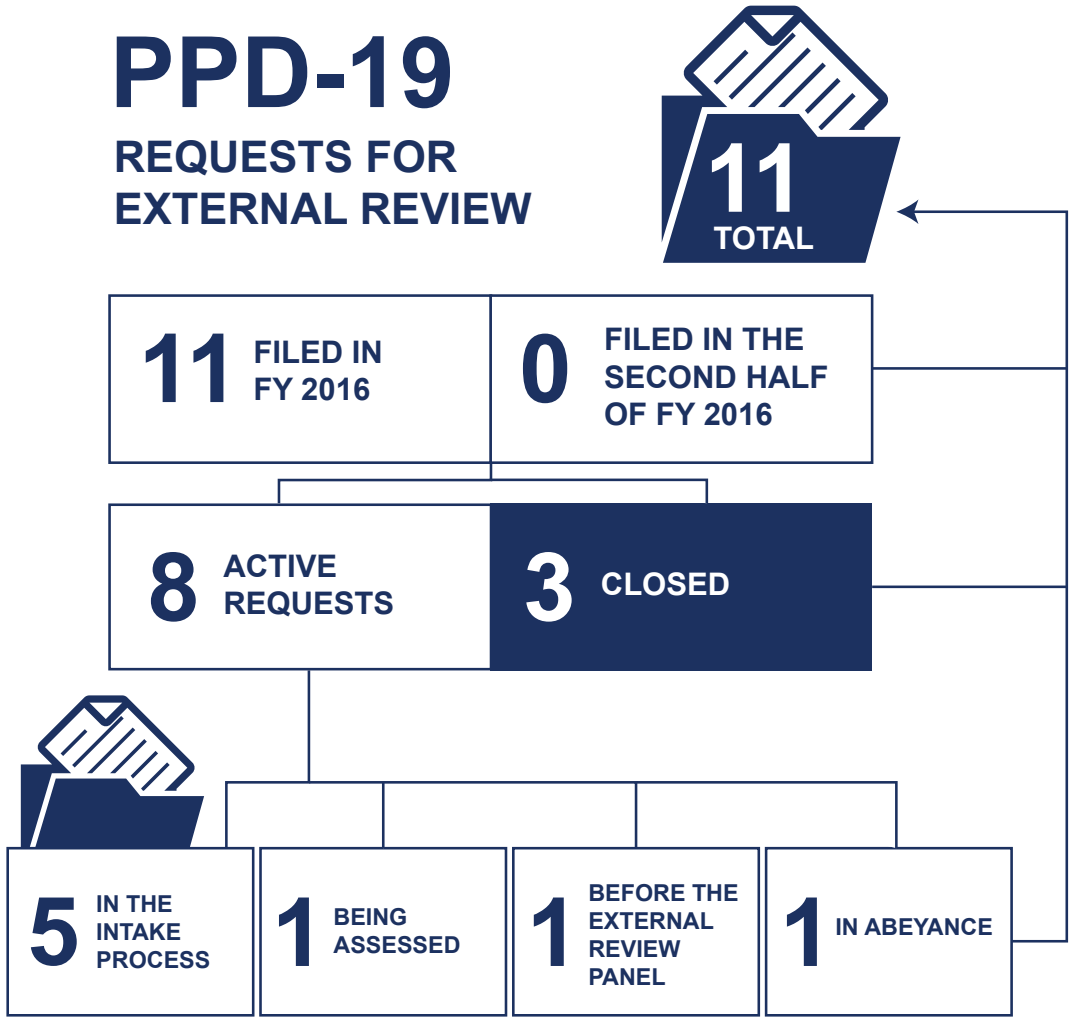
Detailed in the adjacent graphic, we saw an increase in requests for external review with 11 filed in FY 16

The first PPD-19 External Review Panel convened in October 2015 after a request for a review from an Intelligence Community employee.

The ERP conducted a *de novo* review and in May 2016, issued a final decision overturning the local agency IG, in part, and substantiating whistleblower reprisal. The ERP's report detailed that the employee was entitled to appropriate relief from the agency.

The agency's director agreed with the ERP's decision; and the recommendations were still being implemented at the end of this reporting period.

Additional details are in the classified annex of this report.



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.

Legal and Policy Reviews

During this reporting period, we continued outreach to IC IG staff, ODNI components, and fellow IC Counsels to ensure IG equities and statutory requirements were incorporated into policy guidance.

We worked closely with the Executive Director for IC Whistleblowing to ensure education and outreach was appropriate and consistent with the latest legal and policy developments.

We finalized an internal policy for processing Freedom of Information Act and Privacy Act requests for IC IG materials. This new policy is designed to provide for the fullest possible public disclosure, limited only by the obligations to redact information required by statutes to maintain confidentiality and administrative necessity.

These efforts will help streamline IC IG's oversight structure, as well as maximize transparency, which is especially difficult given the classified nature of the IC IG's oversight mission.

Legislative Reviews

During this reporting period, our office closely tracked and reviewed the Intelligence Authorization Act for Fiscal Year 2016, the Inspector General Empowerment Act of 2015, and the Cybersecurity Information Sharing Act of 2015. In fact, in the Cybersecurity Act, Inspectors General are required to report to Congress on the agency's cybersecurity policies, procedures, practices, and capabilities for national security systems and systems that provide access to personally identifiable information.

We continue to engage with appropriate committees and other IG Counsels on these congressional mandates and other relevant bills as they progress through the 114th Congress.

Ethics

During this reporting period, we received several inquiries about identifying partisan political activities in the workplace, which if substantiated, would violate the Hatch Act. Given the heightened political season, we worked closely with IC IG staff to identify such activities and assist in referring matters to the Office of Special Counsel for their review and disposition.

IC Whistleblower Protection Act

We submitted eight disclosures to the Senate and House Intelligence Oversight Committees this reporting period. In addition, we worked with the committees to educate them on the Intelligence Community Whistleblower Protection Act procedures and the IG process for reviewing employee complaints of urgent concern.

Our office also supported the Executive Director for IC Whistleblowing by coordinating several congressional staff briefings on specific IC Whistleblower Protection Act disclosures, to include briefings with whistleblowers.

Congressional Engagements

On July 7, 2016, the IC IG provided testimony to the House Oversight and Governmental Reform Committee (HOGR) regarding the IC IG's assistance to the Department of State Office of Inspector General's review of former Secretary Hillary Clinton's use of a personal email server during her tenure as Secretary of State.

Chairman Chaffetz and Ranking Member Cummings were grateful for the testimony and appreciated the review and efforts from the IC IG personnel.

In addition to the hearing on the Clinton Email Review, the IC IG and staff met with several members and appropriately cleared congressional staffers to provide insights into the review. These briefings assured both majority and minority committee members that the IC IG was conducting the review in an objective and unbiased manner. We also provided timely responses to several letters from congressional members interested in IC IG's ongoing work.

Pictured above: I. Charles McCullough, III, testified at a HOGR committee hearing on July 7, 2016. Photo courtesy of a HOGR video capture.

8
DISCLOSURES ★

1
HEARING ★

2
CONGRESSIONAL NOTIFICATIONS ★

8
HILL BRIEFINGS ★

These numbers reflect this reporting period.

Abbreviations and Full Name

AFR	Agency Financial Report
ATO	Approval to Operate
ATR	Above Threshold Reprogramming
AUD	Audit Division (IC IG)
CFO	Chief Financial Officer (ODNI)
CI	Counterintelligence
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer (ODNI)
CITP	Criminal Investigator Training Program
CMO	Chief Management Officer (ODNI)
DATA	Digital Accountability and Transparency Act
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
EO	Executive Order
ERP	External Review Panel
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Modernization Act
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
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
ICC-B	Intelligence Community Campus-Bethesda
ICD	Intelligence Community Directive
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)
NIP	National Intelligence Program
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OSC	Office of Special Counsel
PPD	Presidential Policy Directive
ROCA	Reducing Over-Classification Act
SCI	Sensitive Compartmented Information
SCOR	Security & Counterintelligence Online Report
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

109 CONTACTS

THIS REPORTING PERIOD

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