



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

# SEMIANNUAL REPORT

April 2018 – September 2018

*Michael K. Atkinson*  
*Inspector General of the Intelligence Community*

# Table of Contents

<b>Message from the Inspector General of the Intelligence Community</b>	<b>3</b>
<b>Statutory Reporting Requirements</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>Audit Division</b>	<b>8</b>
<b>Inspections and Evaluations Division</b>	<b>10</b>
<b>Investigations Division</b>	<b>11</b>
<b>Center for Protected Disclosures</b>	<b>13</b>
<b>Office of the General Counsel</b>	<b>15</b>
<b>Management and Administration Division</b>	<b>17</b>
<b>Recommendations</b>	<b>18</b>
<b>Intelligence Community Inspectors General Forum</b>	<b>19</b>
<b>Abbreviations and Acronyms</b>	<b>24</b>
<b>Hotline Numbers</b>	<b>25</b>



DNI Dan Coats swears in Michael K. Atkinson as Inspector General of the Intelligence Community on May 17, 2018. (ODNI Photo)

## Message from the Inspector General of the Intelligence Community

On behalf of the Office of the Inspector General of the Intelligence Community (ICIG), I am pleased to submit this Semiannual Report highlighting the ICIG's activities from April 1, 2018 through September 30, 2018. This is the ICIG's 15th Semiannual Report, and the first issued since the United States Senate confirmed me as the Inspector General of the Intelligence Community on May 14, 2018.

This Semiannual Report details some of the excellent work the ICIG performed over the past six months. The completed reports issued during the review period detailed the results of reviews pertaining to numerous topics of interest to the Office of the Director of National Intelligence (ODNI) and the entire Intelligence Community (IC), including the Freedom of Information Act (FOIA), ODNI's information security program, and ODNI's payment programs.

During the reporting period, the ICIG addressed the ongoing problem of unauthorized disclosures within the Intelligence Community while improving awareness and reporting processes for protected disclosures. The ICIG initiated a program to permit the ICIG to fulfill its responsibilities to report and investigate unauthorized disclosures, as required by Intelligence Community Directive 701, entitled *Unauthorized Disclosures of Classified National Security Information*. The ICIG also restructured its whistleblower program in numerous ways to enhance the ICIG's efficiency and effectiveness in handling whistleblower complaints and concerns, particularly with regard to any claims of reprisal. Toward this end, the ICIG is establishing a Center for Protected Disclosures (CPD) and a Hotline Working Group within the IC to discuss common challenges and share best practices.

The ICIG also updated its whistleblowing website to increase the IC's awareness of how they may appropriately report allegations of waste, fraud, abuse, and mismanagement, without fear of retaliation or risk to national security. Since May 2018, the ICIG's Hotline Program made significant strides in reducing its backlog and establishing procedures to ensure the further reduction of processing times and to enhance efficiency and responsiveness.

During the reporting period, the ICIG also acted to enhance the transparency of its activities. By streamlining its procedures and hiring critical personnel, the ICIG completed 80 percent of its own FOIA cases, which significantly reduced its FOIA backlog; these improved procedures should reduce future case processing times by at least half. In addition, the ICIG for the first time in its history issued an ODNI management



Michael K. Atkinson testifies during an open hearing for his nomination as the Inspector General of the Intelligence Community before the U.S. Senate Select Committee on Intelligence on January 17, 2018. (ODNI Photo)

challenges statement summarizing what it considers to be ODNI's most serious management and performance challenges. This was the first year the ICIG presented a management challenges statement for ODNI before compiling a capstone management challenges statement for the entire IC, which will be included in the ODNI Chief Financial Officer's Summary of Performance and Financial Information Report.

The ICIG also conducted outreach events with multiple stakeholders in an effort to increase transparency and awareness concerning its mandate and activities. The ICIG participated in panel discussions and led information sessions for key events within ODNI, hosted information exchanges with whistleblowing advocacy groups, met with members of Congress and their staff, and engaged in discussions with the Government Accountability Office concerning whistleblower protections in the IC.

This report also illustrates the ICIG's continuing efforts to enhance communication, coordination, and collaboration among the Intelligence Community Inspectors General Forum. The Forum consists of the twelve

statutory and administrative Inspectors General who have oversight responsibility for an element of the Intelligence Community. One of the primary topics at our two Forum meetings this reporting period was the establishment of a joint Security Clearance Working Group with other Forum members. The joint review will build on the extensive work already completed on the security clearance process and concentrate on how the DNI might employ his existing authorities to improve the efficiency and effectiveness of the security clearance process.

As the ICIG assesses its successes over the past six months, and continues to take the requisite steps to increase those successes in the next, the ICIG must express its appreciation for the support provided by ODNI's leadership and workforce. The ICIG also thanks Congress and its staff for their professionalism and cooperation throughout this reporting period, and looks forward to working with them to address the many challenges facing the Intelligence Community.

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



The ICIG's main offices are located at 12290 Sunrise Valley Drive, Gate 3, Reston, VA 20191.

---

## Statutory Reporting Requirements

As required by its authorizing statute in Title 50, United States Code, Section 3033, all ICIG inspection and investigation activities conform to standards adopted by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The ICIG conducts all audit activities in accordance with generally accepted government auditing standards. The ICIG had full and direct access to all information relevant to perform its duties. The ICIG issued no subpoenas this reporting period.

A list of open and closed recommendations for this reporting period is located on page 18. Corresponding corrective actions are listed in the annex.

All ongoing and completed audits, inspections, and reviews begin on page 8.

Select completed investigations begin on page 11.

Updates on whistleblower matters begin on page 13.

## Introduction

### Authority and Organization

The Intelligence Authorization Act for Fiscal Year 2010 established the Office of the Inspector General of the Intelligence Community within the Office of the Director of National Intelligence. The ICIG has the authority to initiate and conduct independent audits, inspections, investigations, and reviews of programs and activities within the responsibility and authority of the Director of National Intelligence. The ICIG's senior management team includes the Inspector General, Principal Deputy Inspector General, General Counsel, four Assistant Inspectors General, and one Center Director. The principal operational divisions are Audit, Investigations, and Inspections and Evaluations. The Management and Administration Division and the General Counsel's Office support the operational divisions and the ICIG's Executive Office. The Center for Protected Disclosures processes whistleblower reports and supports whistleblower protections.



### Mission

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

### Strategic Goal

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

### Independence

The Inspector General is nominated by the President and confirmed by, and with the advice and consent of, the United States Senate. The Inspector General is independent, both in fact and appearance, and provides effective and objective leadership. The Office of the Inspector General of the Intelligence Community bases its findings and conclusions on independent and objective analysis of the facts and evidence that become known to it through its exhaustive audits, investigations, inspections, and programmatic reviews.

### Core Values

*Integrity*

*Commitment*

*Diversity*

*Transparency*

### Outreach Efforts

During the reporting period, consistent with its commitment to promote transparency regarding its Intelligence Community oversight responsibilities and activities, the ICIG conducted numerous outreach efforts. The ICIG held outreach events with the workforce of both ODNI

and the entire Intelligence Community as well as other stakeholders, including non-governmental organizations and advocacy groups. The ICIG will post this Semiannual Report, as it has in the past, on publicly accessible websites, and it will work to post the results of its inspections, evaluations, reviews, and audits on publicly accessible websites to the maximum extent permitted by law. The ICIG updated its unclassified and classified websites to inform individuals within the IC and other interested persons about whistleblower protections and rights. The ICIG held numerous meetings with members of Congress and their staff to inform them about key ICIG findings, recommendations, priorities, and initiatives. As the Chair of the Intelligence Community Inspectors General Forum, the ICIG also led the efforts to enhance communication, coordination, and collaboration among the Forum members.

The ICIG's Legislative Affairs Counsel and Congressional Liaison is Melissa Wright. The ICIG's Public Affairs Officer is Monica Tullos. They can be reached at 571-204-8149, or [IC\\_IG\\_PAO@dni.gov](mailto:IC_IG_PAO@dni.gov).

## Fortieth Anniversary of the Inspector General Act of 1978



This year marks the 40th anniversary of the Inspector General Act of 1978. President Jimmy Carter signed the Act, and described the new statutory Inspectors General as “perhaps the most important new tools in the fight against fraud.” The ICIG, one of 73 statutory Inspectors General collectively overseeing the operations of nearly every aspect of the federal government, looks forward to continuing to expand its efforts

to detect and prevent fraud, waste, and abuse within the Intelligence Community. The ICIG also looks forward to continuing to work with the Council of Inspectors General on Integrity and Efficiency on important issues that significantly affect productivity, transparency, and accountability throughout the federal government.



(ODNI Photo)

## Oversight.gov

On October 1, 2017, the Council of the Inspectors General on Integrity and Efficiency announced the official launch of Oversight.gov. This new website provides a “one stop shop” to follow the ongoing oversight work of all Offices of Inspectors General (OIGs) that publicly post reports.



The ICIG, like the other OIGs, will continue to post reports to its own website. But with Oversight.gov, users can sort, search, and filter the site’s database of public reports from all of CIGIE’s member OIGs to find reports of interest. In addition, the site features a user-friendly map to find reports based on geographic location, and contact information for each OIG’s hotline. Users can receive notifications when new reports are added to the site by following CIGIE’s Twitter account, @OversightGov.

## Resources

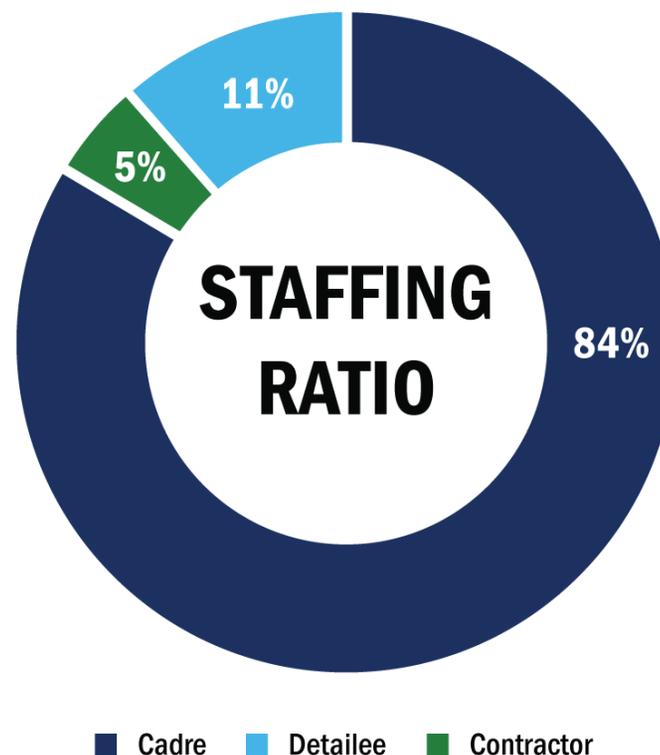
### Funding

During this reporting period, the Office of the Director of National Intelligence provided adequate funding to permit the ICIG to fulfill its mission. The budget covered personnel services and general support, including travel, training, equipment, supplies, Information Technology (IT) support, and office automation requirements. As the ICIG assessed IC programs and activities to promote effectiveness, economy, and efficiency, it also examined its own internal operations to develop and implement greater efficiencies in operations. To that end, the ICIG collaborated with its IT counterparts at ODNI to institute a just-in-time model for procuring and installing computers when staff actually report to duty, thereby eliminating costs associated with maintaining equipment in unoccupied spaces. This action resulted in a 61 percent reduction in the ICIG’s IT operations and maintenance costs.

## Personnel

The ICIG employs a diverse group of talented and highly skilled professionals who provide critical subject matter expertise. The ICIG workforce includes permanent employees (cadre), employees from other Intelligence Community elements on detail to the ICIG (detailees), and contractors.

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



# THE AUDIT DIVISION CONDUCTS PERFORMANCE AUDITS AND IC-WIDE PROJECTS RELATED TO **BUSINESS PRACTICES, ACQUISITION, PROJECT MANAGEMENT, INFORMATION TECHNOLOGY, AND FINANCIAL MANAGEMENT.**

## Completed Audit Projects

### *The Federal Information Security Modernization Act of 2014 (FISMA)*

#### *AUD-2018-001: Review of ODNI FY 2017 Policies and Procedures for Implementing FISMA*

FISMA requires an annual independent evaluation of federal agencies' information security programs and practices. The ICIG identified and assessed the status of ODNI information security program policies and procedures relevant to FISMA for the FY 2017 reporting period. The ICIG reported that ODNI established policies and procedures for two of the eight FISMA metric domains. ODNI Chief Information Officer (CIO) officials continue to develop information security program policies and procedures for the other six domains as part of their effort to implement a robust information security program; however, many of those policies remain in draft form or in coordination status.

The information contained in the report will be included in an Intelligence Community FISMA capstone report to be issued during the next fiscal quarter.

### *Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA)*

#### *AUD-2018-003: ODNI's FY 2017 Compliance with IPERIA*

IPERIA directs federal agencies to perform risk assessments of programs and activities to identify those that may be susceptible to significant improper payments, to estimate the amount of improper payments in susceptible programs and activities, and to report the estimates and actions taken to reduce improper payments in the materials accompanying the agency's annual Agency Financial Report (AFR). IPERIA also directs agencies to conduct recovery audits for each program and activity that expends \$1 million or more annually, if conducting such audits would be cost effective. The objective of the ICIG's review was to determine whether ODNI complied with the requirements of IPERIA in FY 2017.

The ICIG reported that for FY 2017, ODNI was compliant with IPERIA requirements. ODNI performed a program-specific risk assessment on contract vendor payments and determined that this activity's payments were not susceptible to significant improper payments, as defined by the Office of Management and Budget. Based

on this determination, ODNI was not required to prepare or report improper payment estimates or corrective action plans, or conduct recovery audits. As required by IPERIA, ODNI reported these results in its classified FY 2017 AFR.

## Collaboration and Outreach

The ICIG's Audit Division led collaboration efforts in areas of mutual interest across the IC Audit community. The Audit Division initiated meetings to share work plan ideas and identify areas that might benefit from joint audit work. In addition, it coordinated a joint IC OIG Audit response to the Chief Financial Office (CFO) working group's proposed solutions to intra-governmental transactions, one of the significant challenges faced by auditors across the IC pertaining to financial statement auditability. The ICIG's Audit Division also attended closed-session meetings with the Federal Accounting Standards Advisory Board during deliberations on the new Classified Activities Standard, which affects financial statement reporting practices for IC elements.

The Audit Division shared information with its IC Audit partners and coordinated their responses to drafts of the new standard. The ICIG Audit Division's collaboration with its IC Audit partners and the CFO working group built a foundation for future successes in identifying auditability solutions for financial matters of interest to the Intelligence Community.

The ICIG Audit Division and the National Reconnaissance Office OIG co-hosted the second Intelligence Community Information Technology Auditor Summit. The summit featured the IC Chief Information Officer's insight on strategies and challenges in IT developments for the IC. Speakers from across the community shared information on current topics including the use of data analytics for IT audits, privacy controls in the IC, and mitigating security and counterintelligence risks in the IT supply chain. Roundtable discussions provided participants the opportunity to share ideas on approaches and best practices, and to discuss challenges in conducting IT audits.



Intelligence Community IT professionals collaborate to discuss identity, credentials, and access management (ICAM) requirements to produce a community-wide ICAM reference architecture at an offsite held at ODNI. (Photo: ODNI IC CIO)

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

## Summary of Completed Review

*Additional details about the completed review are in the annex.*

### *INS-2018-001: Assessment of Intelligence Community Freedom of Information Act (FOIA) Programs*

The ICI's Inspections and Evaluations Division (I&E) examined the effectiveness of the FOIA programs of ODNI, the Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency. FOIA is the primary means for the public to access federal executive branch records. I&E focused on how IC programs prioritize, coordinate, and process FOIA requests to meet statutory requirements, including the timeliness of responses and the effectiveness of communications with requesters. I&E also reviewed ODNI's role as an IC-wide integrator. I&E initiated this assessment after determining that ODNI's Information Management Division had raised concerns with the Intelligence Community's FOIA program to the Executive Committee, its senior governance forum.

## Summary of Ongoing Review

### *INS-2018-003: Report of Inspection: The Cyber Threat Intelligence Integration Center, Office of the Director of National Intelligence*

I&E is preparing the final report concerning its inspection of ODNI's Cyber Threat Intelligence Integration Center (CTIIC). CTIIC was established pursuant to Presidential Memorandum, *Establishment of the Cyber Threat Intelligence Integration Center*, dated February 25, 2015. Among other responsibilities, CTIIC provides integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests.

Presidential Policy Directive 41, *United States Cyber Incident Coordination* (PPD-41), sets forth principles governing the federal government's response to any cyber incident, whether involving government or private sector entities. PPD-41 further directs that ODNI, through CTIIC, is the lead federal agency for intelligence support and related activities for significant cyber incidents.

I&E conducted a review of CTIIC's management effectiveness, mission performance, resource management, and enterprise oversight for the period of February 2016 through February 2018.

# 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 ICIG's Investigations Division continued its efforts regarding cross-IC fraud, public corruption, and counterintelligence matters. The Investigations Division worked jointly with the Federal Bureau of Investigation (FBI), other Offices of Inspectors General within the Intelligence Community, the Defense Criminal Investigative Service, the Air Force Office of Special Investigations, and other federal investigative agencies. The Investigations Division also coordinated its activities with various federal prosecuting offices, including the Counterintelligence and Export Control Section of the United States Department of Justice's National Security Division, the Public Integrity Section and the Fraud Section of the United States Department of Justice's Criminal Division, as well as the United States Attorney's Office for the Eastern District of Virginia.

ICIG's investigators also spent significant time on a continuing joint criminal investigation with the FBI and several other federal law enforcement organizations. This investigation will continue into the next reporting period.

The Investigations Division completed a number of investigations during the reporting period. For instance, the Investigations Division

substantiated labor mischarging by an ODNI contract employee who billed the government for hours that the contractor did not work, leading to an estimated loss to the government of approximately \$18,000. Because the matter was declined for criminal prosecution, the ICIG referred the matter to ODNI for any administrative action it deems appropriate against the contractor and the contractor's employer.

The ICIG's investigators substantiated allegations that a contractor employee misused a government computer, conducted unreported outside business activities while at work, failed to report potential unofficial foreign contacts, and billed for hours not worked. The estimated loss to the government was approximately \$28,400. Because the matter was declined for criminal prosecution, the ICIG referred the matter to ODNI for any administrative action it deems appropriate against the contractor (whose security clearance was subsequently terminated) and the contractor's employer.

The Investigations Division also substantiated government computer misuse by an ODNI contractor employee who routinely and improperly conducted electronic searches

related to sexual violence. As a result of the ICIG's investigation, ODNI removed the contractor from the contract and revoked the contractor's clearance.

During the review period, the Investigations Division also closed investigations related to unauthorized disclosures of information as well as allegations related to hiring improprieties, labor mischarging, and conflicts of interest.

## *Intelligence Community Directive 701, Unauthorized Disclosures of Classified National Security Information*

Beginning in June 2018, the Investigations Division began to take steps to permit the ICIG to fulfill its responsibilities under Intelligence Community Directive 701, *Unauthorized Disclosures of Classified National Security Information* (ICD 701). In December 2017, the DNI revised ICD 701 to improve the IC's efforts to detect, deter, report, and investigate unauthorized disclosures. The revised ICD imposed new responsibilities upon the ICIG to report and investigate unauthorized disclosures.

Under ICD 701, the ICIG will:

- Review unauthorized disclosure cases where the FBI decides not to investigate or the FBI investigates but the Department of Justice declines prosecution, in coordination with the other Office(s) of Inspectors General involved, to determine whether an Inspector General administrative investigation is warranted.
- Coordinate with other Offices of Inspectors General within the IC to determine, in consultation with the Department of Justice, which Tier 2 and Tier 3 cases (as defined in ICD 701, Annex B) may be suitable for administrative investigation.
- Coordinate with other Offices of Inspectors General within the IC to ensure cases suitable for administrative investigation are reviewed, appropriately investigated, and not closed prematurely.
- Coordinate with other Offices of Inspectors General within the IC to conduct independent investigations.
- Maintain a repository of notifications from IC elements regarding any loss or compromise of classified information, preliminary inquiries, and Crimes Reports on unauthorized disclosures submitted by IC elements, and monitor all submissions to final disposition.



The ICIG maintains a satellite office at ODNI's headquarters at Liberty Crossing. (Peterson Companies Photo)

The Investigations Division has begun to work with ODNI and the other IC elements and stakeholders to develop a program to meet the ICIG's obligations under ICD 701. The Investigations Division will begin to implement this new program during the next reporting period.

# AFTER SEEKING INPUT FROM KEY STAKEHOLDERS, INCLUDING CONGRESS, THE INTELLIGENCE COMMUNITY INSPECTORS GENERAL FORUM, AND ADVOCACY GROUPS, THE ICIG IS DESIGNING AND ESTABLISHING THE CENTER FOR PROTECTED DISCLOSURES.

Intelligence Community employees, contractors, supervisors, and managers detect, collect, and analyze information to develop the most accurate and insightful intelligence possible on external threats. The privileged access of those intelligence professionals carries with it the duty to lawfully disclose information regarding potential wrongdoing, including fraud, waste, and abuse.

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

First, the Center will receive and process whistleblower complaints through the ICIG's Hotline program. The ICIG's Hotline program receives whistleblower complaints and concerns through public and secure telephone numbers and website addresses as well as walk-in meetings at the ICIG's main office in Reston, Virginia, and its satellite offices in Bethesda, Maryland and Tysons Corner, Virginia. The Hotline program also receives and processes allegations of "urgent concerns," disclosed

pursuant to the Intelligence Community Whistleblower Protection Act (the ICWPA). The ICWPA established a process to ensure the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) receive disclosures of potential flagrant problems, abuses, violations of law or executive order, or deficiencies related to the funding, administration, or operation of an intelligence activity. The Center will track all such disclosures, ensure review of materials for classified information, and coordinate disclosures with other Offices of Inspectors General for appropriate review and disposition. During the reporting period, the ICIG transmitted 20 ICWPA disclosures to the SSCI and HPSCI, and the ICIG implemented new procedures for processing ICWPA submissions, including an internal review process by the ICWPA Working Group.

To increase the effectiveness of the ICIG's Hotline program, this reporting period the ICIG established the first IC-wide Hotline Working Group to share challenges and best practices with our IC Hotline partners. Participants in the first meeting included Hotline managers from the Offices of Inspector General of the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence

Agency (NGA), and National Reconnaissance Office (NRO). Participants reviewed their Hotline programs, identifying commonalities and differences regarding the software they use, their referral procedures, who in their respective offices vets complaints, and how they forward complaints to other Inspectors General. The Hotline Working Group intends to meet semiannually to further share their procedures and lessons learned.

Second, the Center will provide community outreach and guidance to individuals seeking more information about the options and protections afforded to those who may wish to make a protected disclosure to the ICIG or Congress, or who believe they suffered reprisal because they made a protected disclosure. As part of its outreach efforts, the ICIG leads the Intelligence Community Whistleblower Working Group. During the reporting period, the Working Group addressed topics including whistleblower protections under the 2018 Foreign Intelligence Surveillance Act (FISA) amendments, the new ICIG whistleblower website, and the use of alternative dispute resolution in whistleblower matters. The ICIG also conducted outreach and training activities within ODNI to ensure management stakeholders present consistent whistleblowing education. To that end, the

ICIG, in consultation with the Office of the Inspector General for the National Security Agency, reviewed and commented on ODNI's whistleblower protection training modules, which were revised and re-launched by ODNI to its workforce during the reporting period. The ICIG also held an outreach event for ODNI's workforce at ODNI's headquarters to celebrate Whistleblower Appreciation Day on July 30, 2018.

Third, the Center will administer requests by employees and contractors in the IC for the ICIG to review their allegations of reprisal under Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information* (PPD-19). PPD-19 ensures that employees serving in the Intelligence Community or those who are eligible for access to classified information can effectively report fraud, waste, and abuse while protecting classified national security information. It prohibits retaliation against employees for reporting fraud, waste, and abuse.

The ICIG has unique and important responsibilities under PPD-19. Specifically, PPD-19 created an external review process, administered by the ICIG, to examine allegations of whistleblower reprisal. Under PPD-19, an individual who believes they suffered reprisal for making a protected disclosure is required to exhaust their agency's applicable review process for whistleblower reprisal allegations prior to requesting an external review by the ICIG. Upon exhaustion of those processes and a request for review, PPD-19 permits the ICIG to exercise its discretion to convene an External Review Panel (ERP) to conduct a review of the agency's determination.

The ICIG received six new ERP requests this reporting period. Following initial assessment and review of materials submitted by both the complainants and their agencies on four of the requests, the ICIG denied three of the requests and closed the matters. The other request is pending a decision. The ICIG continues to assess the remaining two ERP requests. In addition, during this reporting period, the ICIG

reviewed historical ERP requests and began a comprehensive review of ERP processes to identify the policies, procedures, and tracking mechanisms necessary for efficient and timely processing of those requests. The ICIG appreciates the assistance provided by the NRO OIG in organizing the historical ERP requests.



DNI Coats (center) joins ICIG Atkinson (far left) and his staff members during a National Whistleblower Appreciation Day workforce outreach event held at ODNI HQ in July. (ODNI Photo)

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

The primary responsibility of the ICIG's Office of the General Counsel (OGC) is to ensure that the ICIG receives independent advice and counsel that is without any conflicts of interest, both in fact and in appearance. The OGC:

- Provides legal and policy advice;
- Conducts operational, administrative, and ethics reviews;
- Facilitates discussions by the Intelligence Community Inspectors General Forum; and
- Serves as the ICIG Congressional Liaison.

## Legal and Policy Reviews

The ICIG's Office of the General Counsel continued its outreach efforts to inform ICIG staff and the Intelligence Community Inspectors General Forum about legislation and policy affecting Inspectors General equities. OGC also engaged with ODNI legal and policy offices to ensure that they consider the ICIG's independence and equities when ODNI develops critical IC-wide policies. Such policy revisions pertained to unauthorized disclosures of classified information, efforts to provide effective ODNI whistleblower training to ODNI's workforce, and efforts to revise and improve the Security Executive Agent Directive on whistleblower protection. OGC reviewed and provided input regarding

these policies. OGC helped to facilitate and participate in discussions to ensure that the revised policies were consistent with the ICIG's policies and other Inspectors General's abilities to conduct independent and objective administrative investigations of alleged unauthorized disclosures. OGC also helped to ensure that such policies complied with PPD-19's requirements. OGC closely interacted with the ICIG's Center for Protected Disclosures on whistleblower education and outreach efforts to ensure consistency with evolving legal and policy developments.

## Operational, Administrative, and Ethics Reviews

OGC provides timely advice to the entire ICIG organization. OGC supports the Investigations Division throughout the investigative process by highlighting and providing guidance on potential legal issues meriting additional or redirected investigative efforts. OGC stays apprised of current legal trends and case law to ensure that investigative tools and methods are utilized in a manner consistent with protecting individuals' personal and legal rights.

OGC supports the Inspections and Evaluations Division and the Audit Division by identifying and interpreting key policy and contract provisions relevant to its observations, findings, and recommendations, as provided in its numerous

component and intelligence oversight reviews and audits.

OGC also provides legal and policy guidance regarding issues related to the ICIG's administrative personnel, training, and budgetary functions. During the reporting period, OGC assisted the Management and Administration Division in increasing the efficiency and effectiveness of the ICIG's FOIA program. Specifically, OGC reviewed the existing FOIA policy and procedures and met with internal and ODNI stakeholders to incorporate best practices and to clarify and streamline responsibilities; this review and related actions led to dramatically reduced FOIA processing times by the ICIG. In total, OGC provided legal reviews of 36 FOIA cases, including one case currently in litigation, and assisted in reducing the backlog of FOIA cases.

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

## Outreach

With assistance from the Management and Administration Division, OGC provided support for a summer law clerk event sponsored by the Council of Counsels to Inspectors General at CIA headquarters. Twenty-five summer interns, clerks, and attorneys from fifteen different departments, agencies, and entities across the federal government attended the event. The Inspector General of the Intelligence Community and the Acting Inspector General for the CIA provided overviews of their personal backgrounds, offices, and missions to the group. After a working lunch, the event concluded with a guided tour and a group photograph at the CIA seal in the Original Headquarters Building.

## Legislative Development and Congressional Engagements

OGC continues to engage on congressional mandates and relevant bills with members of Congress and their staff, ODNI's Office of General Counsel, ODNI's Office of Legislative Affairs, the Counsels Committee for the Intelligence Community Inspectors General Forum, the Government Accountability Office, and the Council of Inspectors General on Integrity and Efficiency.

Throughout this reporting period, the ICIG frequently engaged with Congress. Notably, following confirmation of the new Inspector General in May 2018, the ICIG's Legislative Counsel arranged and accompanied the Inspector General to several meetings with members of Congress and their staff to provide an opportunity for the Inspector General to discuss his vision and priorities for the ICIG, and to hear about priority issues from the members and their staff. Counsel also provided and

arranged for several bipartisan congressional briefings on recent ICIG activities, including ICIG efforts to reorganize the ICIG's whistleblower program to meet its responsibilities under the Intelligence Community Whistleblower Protection Act, the National Security Act of 1947, the Inspector General Act of 1978, and PPD-19.

The ICIG also engaged with the General Accountability Office (GAO) on several occasions. For example, OGC arranged an initial meeting between GAO and the Inspector General to discuss and respond to the ICIG's congressional mandate to review aspects of the Intelligence Community Whistleblower Program. The ICIG's Inspections and Evaluations Division

also met with GAO to discuss the findings of the ICIG's 2016 inspection of ODNI's Intelligence Community Campus-Bethesda (ICC-B) facility.

OGC continues to review and monitor proposed legislation and regulations potentially affecting ICIG operations specifically and the broader Inspector General community generally. Further, OGC regularly engages with congressional staff to discuss pending and potential legislation. For example, OGC closely tracked and commented on the House and Senate Intelligence Authorization Acts of 2018 and 2019, and discussed with staff the need for legislation aimed at enhancing the ICIG's ability to recruit and retain experienced investigators.



The Intelligence Community Campus in Bethesda, Maryland (ICC-Bethesda). The ICIG maintains a satellite office at ICC-B. (Whiting Turner Photo)

# THE MANAGEMENT AND ADMINISTRATION DIVISION PROVIDES FULL SPECTRUM MISSION SUPPORT ACROSS THE ICIG.

The Management and Administration Division (M&A) strengthens the ICIG's operations by providing programmatic support to enable strategic alignment with goals and priorities, and effective execution of the ICIG's statutory and other mandated responsibilities, including:

- Operational Planning and Management
- Quality Assurance
- Talent Development
- Communications

M&A ensured continuity in day-to-day office operations and realized several operational successes this reporting period. A summary of these successes follows.

M&A coordinated production of the ICIG's first ODNI Management Challenges (MC) report for inclusion in the FY 2018 Agency Financial Report. The Reports Consolidation Act of 2000 requires that each agency accountability report include a statement prepared by the agency's Inspector General summarizing what the IG considers to be the most serious management and performance challenges facing the agency, and briefly assessing progress in addressing those challenges. The ICIG writes an annual IC-wide MC statement for inclusion in the Chief Financial Officer's Summary of Performance and Financial Information Report. This is the first year the ICIG has written an MC statement for ODNI before compiling the IC-wide MC

statement. The ICIG found that ODNI's most serious management and performance challenges were in the following areas:

- Enhancing IC coordination, integration, and information sharing
- Reforming the security clearance process
- Producing auditable financial statements
- Strengthening information security
- Improving management of ODNI's workforce

Beginning in late May 2018, M&A cleared the longstanding Freedom of Information Act case backlog dating to 2012, mitigating ODNI's risk of litigation from processing delays. During this period, M&A gained the authorities necessary to streamline the FOIA review process and eliminated unnecessary actions on the front end. As a result, M&A was able to validate and reconcile a backlog of more than 50 outstanding cases, ultimately reducing the number of active cases by 80 percent. M&A will continue to take all necessary steps to timely satisfy FOIA compliance requirements in the future.

M&A is currently negotiating an agreement with ODNI's Information Management Division for the ICIG's new in-house classification expert to conduct internal classification reviews. This will dramatically reduce classification review time. In addition, M&A developed and delivered an ICIG-tailored classification training for current and incoming ICIG personnel.

M&A implemented and customized new technology to better support the ICIG's operations, including investigations case management through the Case Management Tracking System (CMTS), Teammate auditing software, and the IDEA data analytics application. M&A is also refining the ICIG's Hotline program processes with technology transcription services and IC-wide email databases.

Through a combination of internal and external stakeholder engagements, M&A is highlighting the ICIG's organization and mission. Recent events include:

- Hill engagements, new hire briefings, and Job/Joint Duty career fairs
- Council of Counsels to Inspectors General Summer Law Clerks Program
- National Whistleblower Appreciation Day workforce outreach
- Oversight Panel Discussions
- Whistleblowing information exchange with advocacy groups
- National Compliance Officer Day workforce outreach

## Recommendations Summary

Report Name	Date Issued	Total Issued	New This Period	Open	Closed This Period
<b>2018</b>					
Assessment of IC Freedom of Information Act (FOIA) Programs	September	10	10	10	0
Memo to COO re: Pending Travel Voucher	August	2	2	2	0
Inspection: Assessment of IC Information System Deterrence, Detection, and Mitigation of Insider Threats	March	4	0	4	0
Inspection: Multi-Sector Workforce: Determining the Accuracy of Numbers and Cost of the Civilian and Contractor Workforce	March	2	0	0	2
Assessment of a Controlled Access Program Information System Deterrence, Detection, and Mitigation of Insider Threats	January	16	0	5	10
<b>2017</b>					
Audit: FY 2016 Independent Evaluation of ODNI Compliance with FISMA	September	1	0	0	1
Inspection: Assessment of ODNI Information System Deterrence, Detection, and Mitigation of Insider Threats	September	19	0	4	4
<b>2013</b>					
Audit: Study: IC Electronic Waste Disposal Practices	May	5	0	1	0
<b>2012</b>					
Audit: IC Security Clearance Reciprocity	December	2	0	2	0
<b>Totals</b>		<b>61</b>	<b>12</b>	<b>28</b>	<b>17</b>

## Intelligence Community Inspectors General Forum Members



Office of the Inspector General of the Intelligence Community (Chair)



Central Intelligence Agency  
Office of the Inspector General



Defense Intelligence Agency  
Office of the Inspector General



Department of Defense  
Office of the Inspector General



Department of Energy  
Office of the Inspector General



Department of Homeland Security  
Office of the Inspector General



Department of Justice  
Office of the Inspector General



Department of State  
Office of the Inspector General



Department of the Treasury  
Office of the Inspector General



National Geospatial-Intelligence Agency  
Office of the Inspector General



National Reconnaissance Office  
Office of the Inspector General



National Security Agency  
Office of the Inspector General

# THE INTELLIGENCE COMMUNITY INSPECTORS GENERAL **FORUM** IS COMPOSED OF THE TWELVE STATUTORY AND ADMINISTRATIVE INSPECTORS GENERAL WHO HAVE **OVERSIGHT RESPONSIBILITIES** FOR INTELLIGENCE COMMUNITY ELEMENTS.

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

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

The Inspector General of the Intelligence Community chaired two Forum meetings during this reporting period. At the first meeting, in June 2018, the Forum discussed multiple topics, including how best to handle joint duty rotations, ways to reduce whistleblowing investigation processing times, issues pertaining to cyber security, best practices regarding hotline processes, and potential reviews to address the security clearance backlog and the problem of unauthorized disclosures.

The second Forum meeting, held in September 2018, was the first held under a new framework for Forum committees and working groups to present proposals for consideration and decision by the Inspectors General at the Forum meeting. The Security Clearance Working Group proposed a joint review by the Forum's members on the DNI's authorities as the Security Executive Agent, the established policies pertaining to those authorities, and the implementation of those policies by the elements within the IC. The study of this specific topic would have the desired effect of not having the Working Group repeating work already completed during previous assessments of the security clearance process. Forum members agreed on the proposed joint study and provided

guidance on the initial steps necessary to commence the study.

The Forum members also discussed the procedures for handling reprisal complaints against Inspectors General and certain of their designated staff members. More specifically, the Forum members discussed the relationship between protections provided to whistleblowers under Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information*, and the statutory authority of the CIGIE's Integrity Committee.

At the ICIG's request, the Forum members agreed to meet in mid-2019 to align work plans for FY 2020 in an effort to increase the number and scope of joint projects by Forum members and to minimize the duplication of efforts.

## Committee Updates

### *Deputy Inspectors General Committee*

The ICIG experienced several changes in the senior management ranks this reporting period. In May 2018, the United States Senate confirmed Michael K. Atkinson as the Inspector General of the Intelligence Community. Shortly thereafter, the ICIG's Principal Deputy Inspector

General, Acting Deputy Inspector General, and General Counsel left the ICIG for other opportunities.

In addition to these changes, in September 2018, the ICIG welcomed Robin Ashton as the Principal Deputy Inspector General. Robin brings a wealth of professional experience and expertise to the ICIG. She has worked over 30 years with the Department of Justice (DOJ), most recently as the head of DOJ's Office of Professional Responsibility (OPR), where she served since January 2011. Under her leadership, OPR successfully investigated allegations of misconduct involving DOJ attorneys, as well as allegations of misconduct by law enforcement personnel when related to allegations of attorney misconduct within the jurisdiction of OPR.

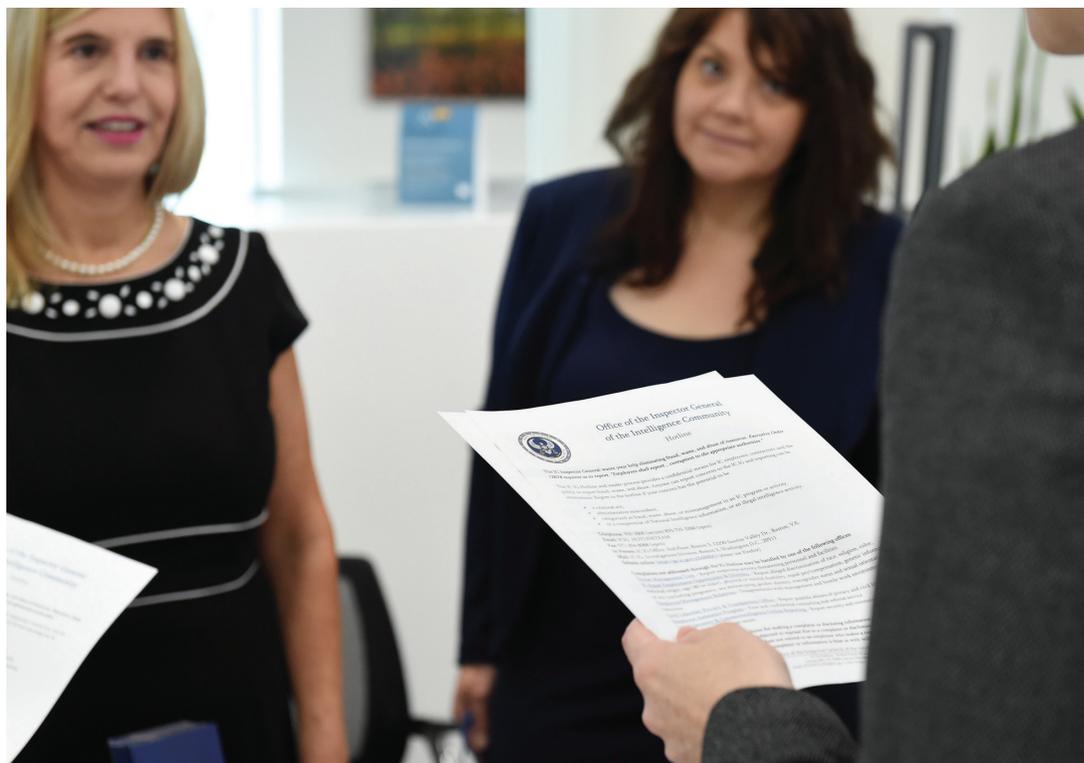
Ms. Ashton also spent two decades as an Assistant U.S. Attorney with the U.S. Attorney's Office for the District of Columbia. In that role she handled complex appeals in the U.S. Court of Appeals for the District of Columbia Circuit, prosecuted over 50 felony jury trials, supervised hundreds of grand jury investigations, and investigated police misconduct, public corruption, and national security cases. For four years, Ms. Ashton served as the Principal Deputy Director of the Executive Office for U.S. Attorneys, the DOJ component responsible for providing executive and administrative support to the 93 U.S. Attorneys' Offices nationwide. Ms. Ashton also served a one-year detail to the U.S. Senate Judiciary Committee.

During her career with DOJ, she was awarded the Attorney General's Claudia Flynn Award for Professional Responsibility, the Attorney General's Award for Outstanding Leadership in Management, the United States Attorney's Award for Meritorious Service, and the Executive Office for U.S. Attorneys Director's Award

for Excellence in Management. Ms. Ashton received her Bachelor of Arts degree from the University of Michigan, and her Juris Doctor degree from the College of William and Mary.

Ms. Ashton will serve as the Chair of the Deputy Inspectors General Committee for the Intelligence Community Inspectors General Forum. In this role, she will provide leadership in identifying and addressing matters of mutual interest among Forum members. Upcoming topics of interest include human capital management across the IC in order to enhance opportunities to rotate Forum members'

personnel through various elements of the IC in an effort to foster a broader community perspective, and to provide IC civilian joint duty qualifying experience(s) to those civilian personnel in the course of their careers. Preliminary discussions with the Deputy Inspectors General of the other Forum members have begun. The Committee anticipates addressing this topic at their next meeting in the first quarter of FY 2019, and providing their work for consideration by the Inspectors General at a future Forum session.



ICIG staff sensitize IC employees about reporting obligations during a National Compliance Officer Day observance in September. (ODNI Photo)

### *Counsels Committee*

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

During this reporting period, the Counsels collaborated on key initiatives, including:

- The ICIG's plan to restructure its whistleblower program;
- The best way to handle complaints submitted to the CIGIE Integrity Committee, and allegations of whistleblower reprisal against IC Inspectors General pursuant to PPD-19;
- The development of standards for handling External Review Panel reviews pursuant to PPD-19;
- How to effectively track and meaningfully discuss potential legislation impacting the Forum members, including the Senate and House versions of the Intelligence Authorization Acts of 2018 and 2019; and
- Views on the use of Nondisclosure Agreements by IC elements and Forum members.

### *Management & Administration Committee*

The Forum's Management & Administration Committee convened to discuss a number of activities and priorities of mutual interest. The Committee agreed to expand its structure to incorporate an Information Technology subcommittee and to establish an Information Review and Dissemination Working Group.

The Forum realigned the Human Capital Subcommittee, previously reported as an extension of the Management & Administration Committee, with the Deputies Committee.

The IT Subcommittee did not meet during this period, but the subcommittee lead continued to collect IT requirements from Forum members seeking to join the ICIG's applications in the Cloud. The subcommittee will propose solutions for IT integration based upon Forum members' expressed levels of interest.

At the ICIG's initiation, the Forum's Information Review and Dissemination Working Group held its inaugural meeting to analyze the information disclosure policies, processes, and procedures of Forum members and IC elements; information disclosure tracking and accountability practices; the use of Nondisclosure Agreements; and operational best practices. The Working Group will reconvene in the first quarter of FY 2019 to address identified concerns and begin to develop solutions.

### *Audit Committee*

The Forum's Audit Committee and Cybersecurity Subcommittee hosted a quarterly meeting to discuss multiple topics of IC interest. The meeting featured a guest speaker from the Cyber and National Security Unit within the Office of Management and Budget's Office of the Federal Chief Information Office, who shared information on FY 2018 Federal Information Security Modernization Act (FISMA) metrics and corresponding guidance, along with the framework for the annual FISMA report to Congress. The meeting also included a guest speaker from the Central Intelligence Agency (CIA) OIG, who discussed the successful use of data analytics on a recent Travel Card Program audit. In addition, an ICIG speaker presented the results of a recent inspection entitled, *Multi-Sector Workforce: Determining the Accuracy of*

*Numbers and Cost of the Civilian and Contractor Workforce*. The ICIG also provided an update on the Federal Accounting Standards Advisory Board actions to issue a new accounting standard for classified activities.

The Audit Committee and Cybersecurity Subcommittee hosted a second quarterly meeting. Featured guest speakers from offices within ODNI and the Departments of Defense and Justice shared information on programs to facilitate receiving and sharing cyber threat information across the federal government and with industry. In addition, a guest speaker from the IC Office of the Chief Information Officer discussed upcoming changes to its approach to evaluating cybersecurity measures of effectiveness.

### *Inspections Committee*

At the Forum's Inspections Committee's first quarterly meeting, the National Reconnaissance Office (NRO) OIG presented a proposal to the Inspections Committee to conduct a joint evaluation of Intelligence Oversight processes. The Inspections Committee agreed to stand up a working group to evaluate the merits of the proposal and, if warranted, to recommend the proposed scope, objectives, and framework to conduct a joint evaluation. The working group will present its deliverables at a future Forum session.

At the Inspections Committee's second quarterly meeting, the CIGIE Training Institute presented an overview of an online tool and methodology currently under development. The "I&E Navigator" is being designed to help OIG Inspections & Evaluations (I&E) professionals conduct their work in a more standardized, consistent, and efficient manner. OIGs will be able to tailor the tool to reflect the same look and feel as their home organization's processes and terminologies. Experienced inspectors



A CIGIE Training Institute staff member discusses an online tool and methodology currently under development. (ICIG photo)

from several OIG I&E offices are consulting on its development. Committee members generally agreed that the I&E Navigator, scheduled to be completed in late FY 2019, has the potential to be a helpful tool for inspectors in accomplishing their I&E oversight mission. CIGIE anticipates developing similar tools for investigations, audits, and OIG leadership.

The National Geospatial-Intelligence Agency OIG provided a presentation concerning their experiences audiotaping inspection interviews. Since FY 2017, NGA's Inspections Division has made recorded interviews an option for sources. These recorded interviews supplement traditional handwritten note taking. Both the recording and the handwritten notes form the basis of the official record. To date, 113 interviewees have selected this recording option while only one has declined. NGA found that the recordings can improve efficiency and effectiveness by increasing comprehension, de-confliction

between interviewers, transparency, level of detail, and the ability to have speech-to-text transcription. The recordings proved especially beneficial when interview subjects provided highly technical or complex information. NGA offered to provide further insights into recorded interviews for partner OIG inspection programs that may be considering adding the capability to their processes. The Department of Justice OIG inspection program uses recorded interviews as well.

ODNI Systems & Resource Analyses (SRA) provided an overview of the vision and foundational priorities of "IC2025," newly established guiding principles created with input from the IC elements meant to better execute community missions. The guiding principles are:

- Augmenting Intelligence Using Machines;
- The Right, Trusted, Agile Workforce;
- Comprehensive Cyber Posture;

- Modern Data Management and Infrastructure;
- Private Sector Partnerships; and
- Acquisition Agility.

ODNI anticipates embedding these priorities into IC strategy and budgetary guidance, and the IC elements are expected to consider them as they act on initiatives and prioritize them in their program builds. Cross-IC teams of visionary leaders will develop actionable recommendations for initiatives in line with these priorities. SRA encouraged OIGs to consider implementing the IC2025 vision in their future work plans.

### *Investigations Committee*

The Forum's Investigations Committee met twice during this reporting period to discuss several key initiatives related to unauthorized disclosure investigations, utilizing Financial Crimes Enforcement Network data, and best practices in implementing electronic case management tracking systems. The Committee held a robust discussion on intelligence-related exploitation of open source information. The Committee received a demonstration of various online investigative tools and techniques used to exploit open source information, including various social media platforms.

In the second quarterly Investigations Committee meeting, the Committee hosted a representative from the CIA's Open Source Enterprise who provided an overview of multiple talent recruitment programs for global experts. The presentation included examples of illegal activities identified in one of the programs, followed by a discussion of the potential role of OIGs in detecting potential fraud, waste, and abuse within those programs.

## Abbreviations and Acronyms

AFR	Agency Financial Report	ICC-B	ODNI Intelligence Community Campus-Bethesda facility
AUD	Audit Division (ICIG)	ICWPA	Intelligence Community Whistleblower Protection Act
CPD	Center for Protected Disclosures	IG	Inspector General
CFO	Chief Financial Officer (ODNI)	INS	Inspections Division (ICIG)
CIA	Central Intelligence Agency	INV	Investigations Division (ICIG)
CIGIE	Council of Inspectors General on Integrity and Efficiency	IPERIA	Improper Payments Elimination and Recovery Improvement Act
CIO	Chief Information Officer	IT	Information Technology
CMTS	Case Management Tracking System	M&A	Management & Administration Division (ICIG)
COO	Chief Operating Officer	MC	Management Challenges
CTIIC	Cyber Threat Intelligence Integration Center	NGA	National Geospatial-Intelligence Agency
DIA	Defense Intelligence Agency	NRO	National Reconnaissance Office
DIG	Deputy IG	NSA	National Security Agency
DNI	Director of National Intelligence	O&M	Operations & Maintenance
DOJ	Department of Justice	ODNI	Office of the Director of National Intelligence
ERP	External Review Panel	OGC	Office of the General Counsel (ICIG)
FBI	Federal Bureau of Investigation	OGE	Office of Government Ethics
FISA	Foreign Intelligence Surveillance Act	OIG	Office of the Inspector General
FISMA	Federal Information Security Modernization Act	OPR	Office of Professional Responsibility (DOJ)
FOIA	Freedom of Information Act	PDIG	Principal Deputy IG
FY	Fiscal Year	PPD	Presidential Policy Directive
GAO	Government Accountability Office	SRA	Systems & Resource Analyses
GC	General Counsel (ICIG)	SSCI	Senate Select Committee on Intelligence
HPSCI	House Permanent Select Committee on Intelligence	SPFIR	Summary of Performance and Financial Information Report (ODNI CFO)
I&E	Inspections & Evaluations Division (ICIG)		
IC	Intelligence Community		
ICIG	Office of the Inspector General of the Intelligence Community		



# ICIG 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 Intelligence Community employees, contractors, and the public to report fraud, waste, and abuse. This process includes secure and commercial email and phone numbers, U.S. mail, anonymous secure web application submissions, and walk-ins.

### NEW CONTACTS LOGGED BY ICIG THIS REPORTING PERIOD



### METHODS OF CONTACT

logged by the ICIG this reporting period,  
including repeat contacts and excluding walk-ins

