Office of the Inspector General of the Intelligence Community

Semiannual Report
April 2019 – September 2019

Michael K. Atkinson
Inspector General of the Intelligence Community

TABLE OF CONTENTS

Message from the Inspector General of the Intelligence Community 3

Introduction 6

- Authority 6
- Organization 6
  - Audit Division 6
  - Investigations Division 7
  - Investigative Activity Overview 7
  - Summaries of Substantiated Investigations 8
  - Inspections and Evaluations Division 8
  - Management and Administration Division 9
  - Office of the General Counsel 10
  - The Center for Protected Disclosures 10

Independence 12

ICIG Mission 12

ICIG Strategic Goal 12

ICIG Core Values 12

The Inspector General Community 12

ICIG Programmatic Objectives 13

Improving the Efficiency and Effectiveness of the IC's Cyber Posture, Modern Data Management, and IT Infrastructure 14

- Management of Privileged Users of Office of the Director of National Intelligence Information Systems 14
- Fiscal Year 2019 Independent Evaluation of the Office of the Director of National Intelligence's Information Security Program and Practices, as Required by the *Federal Information Security Modernization Act of 2014* 14
- Cybersecurity Information Sharing Act of 2015 14
- ODNI Oversight of IC Major System Acquisition Cybersecurity Risks 15

Enhancing Workforce Management 16

- Security Clearance Working Group 16

Compliance with the *Improper Payments Elimination and Recovery Act of 2010* 16
Conference Spending 17
ODNI's Charge Card Program 17
Assessment of the Office of the Director of National Intelligence Methods Used to Substantiate Post-Secondary Education Claims Made by ODNI Cadre Employees Subsequent to Entry-on-Duty 18
Championing Protected Disclosures 19
Intelligence Community Directive 701 20
Improving Oversight of Artificial Intelligence 22
Integrating the Intelligence Community 24
Intelligence Community's Foreign Language Program 24
European Union-United States Privacy Shield 24
Management Challenges Facing the ODNI 25
Intelligence Community Information Sharing Working Group 25
Inspections and Evaluations Navigator Training Tool 25
Collaboration within the Audit Community 26
Peer Reviews 27
Intelligence Community Inspectors General Forum 28
Forum Committee Updates 28
Audit Committee 29
Counsels Committee 31
Inspections and Evaluations Committee 33
Investigations Committee 35
Management and Administration Committee 36
Whistleblower Committee 38
Intelligence Community Data Analytics Community of Interest Working Group 39
Community-Wide Outreach Activities 40
Recommendations Summary 44
ICIG Hotline 46
Abbreviations and Acronyms 47

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 objectives, achievements, and activities from April 2019 through September 2019.

Transparency might not be the first thought that comes to mind when thinking about the U.S. Intelligence Community, but transparency is one of our core values at the Office of the Inspector General of the Intelligence Community. Although Inspectors General have been part of the United States federal government for over 40 years, it seems there may be uncertainty or even confusion about their role in our government, and for those familiar with Inspectors General, perhaps a degree of apprehension about them. There are those who may have the mistaken belief that Inspectors General appear only when something has gone wrong, or when someone has engaged in an activity involving fraud, waste, or abuse. The work of Inspectors General, however, is multi-faceted, and their responsibilities and opportunities to be positive forces for change in the U.S. government extend far beyond delivering unpleasant tidings.

The primary role of Inspectors General is to prevent and detect waste, fraud, corruption, mismanagement, and abuses of authority relating to the programs and activities they oversee. An abuse of authority can take many forms, and Inspectors General are empowered, by law, to review and investigate such abuses of authority, from the minor to the more serious. In the most egregious matters, abuses of authority may involve an intentional violation of the law. In those most egregious matters, I view Inspectors General as among our nation's "first responders."

As so-called first responders, Inspectors General must act swiftly and appropriately when – through audits, investigations, inspections, or reviews – possible wrongdoing is revealed. They must identify, stop, or correct the problem, and in the process they may need to alert those who can assist in the response, whether it be Congress, law enforcement authorities, or others. This call for assistance requires a degree of transparency and openness, which might not seem a natural fit for the U.S. Intelligence Community because, to a great extent, the Intelligence Community is more effective when it operates in secrecy.

Although transparency may seem an incongruous value for organizations that depend on secrecy, the Intelligence Community itself recognizes, as others have said, that secrecy is not a grant of power; it is a grant of trust. Circumstances may arise where the desire and recognized need for secrecy must find a meaningful way to co-exist with the need for transparency. In accordance with laws intended to protect information about intelligence sources, methods, and activities from unauthorized disclosure, the work of Inspectors General must sometimes pierce the shield of secrecy in order to achieve a higher good – the need to shed light on problems, inefficiencies, or even malfeasance – so that the American people can benefit from the most efficient and effective, and truly accountable, government possible.

Inspectors General are able to fulfill their critical oversight function because, by law, they are independent of the agencies they oversee. They are not involved in policymaking; they are not partisan; and Presidentially-appointed Inspectors General do not change with each administration. As part of their independence, Inspectors General have dual reporting obligations. The law, for example, requires me to keep both the Director of National Intelligence and the Congressional Intelligence Committees currently and fully

informed of my activities. It is imperative that Inspectors General exercise their duty to remain independent from both Congress and the agencies they oversee, while fulfilling their responsibility to keep them informed, and simultaneously leading the office that must provide objective oversight to the agency of which they are a part. Inspectors General must strike the appropriate balance between these sometimes-competing objectives, while never forgetting their sworn oath to well and faithfully discharge the duties of their offices.

Like all "first responders," Inspectors General are dependent upon those who first raise an alarm, particularly whistleblowers, who are often the first people on the ground to observe or hear about wasteful practices or possible wrongdoing. Intelligence Community employees, detailees, and contractors collect and analyze information to develop the most accurate and insightful intelligence possible on threats to our national security. These Intelligence Community professionals serve in a classified work environment in which information about intelligence programs and activities is not available for public review, which makes their duty to lawfully disclose information – or sound the alarm – regarding potential wrongdoing that much more critical to the oversight process. Pursuant to Executive Order, federal government employees have an affirmative legal obligation to disclose waste, fraud, abuse, and corruption to appropriate authorities. As part of that affirmative obligation, one of the core *Principles of Professional Ethics for the Intelligence Community* states the following:

> We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, protect intelligence sources and methods diligently, report wrongdoing through appropriate channels; and remain accountable to ourselves, our oversight institutions, and through those institutions, ultimately to the American people.

The past few months have been a searing time for whistleblowers' rights and protections. Much has been written and much has been said about whistleblowers recently, some of it accurate and helpful, and some not. Time will tell whether whistleblowers' rights and protections will emerge from this period with the same legal, ethical, and moral strength they had previously. For my part, however, I am confident that those rights and protections will ultimately emerge stronger, and will not be diminished in any respect. My optimism comes from my belief that the American people want an honest and effective government that reflects their hard-fought values. Such a government benefits when individuals who suspect fraud, waste, abuse, or malfeasance in their government are encouraged to speak up. Those who demonstrate the personal ethics and moral courage expected of individuals who have the honor and privilege of working for the American people should not suffer from or fear reprisal when they do speak up.

More than anything, the future of whistleblowers' rights and protections in the federal government will depend on integrity. In this sense, integrity means more than being honest. It also signifies that government agencies and the federal workforce must be consistent in word and deed; in other words, we must do what we promise we will do. For example, if we instruct individuals in the Intelligence Community, as part of their core *Principles of Professional Ethics for the Intelligence Community*, to "report wrongdoing through appropriate channels," then they must do precisely that. And when they do so, their agencies cannot ignore the reports or block the channels. One of the most important responsibilities for any Office of an Inspector General is to demonstrate this type of consistency in word and deed. This is particularly important when one of our most significant responsibilities is to ensure that whistleblowers in the federal government are protected from reprisal, or threat of reprisal, when they disclose allegations of wrongdoing in good faith and in an authorized manner.

Since I had the honor of becoming the Inspector General of the Intelligence Community in May 2018, the ICIG has made it a priority to strengthen its Whistleblowing Program by, among other things, extensively restructuring the program and spearheading numerous informational and educational outreach events. We created

the Center for Protected Disclosures, which comprises the Source Protection Program, Disclosure Reporting Program, and Source Support Program. When developing the new Center for Protected Disclosures, we sought input from the Intelligence Community Inspectors General Forum,[1] Congressional Members and staff, representatives from the Government Accountability Project, Project on Government Oversight, the Government Accountability Office, and other interested parties. Our goal was to develop a strong program that would provide greater clarity to whistleblowers as they navigate the often confusing and difficult process of bringing their concerns to light. In an effort to strengthen this focus among the Intelligence Community Inspectors General Forum, we established a Whistleblowing Subcommittee to bring together experts from across the Intelligence Community on whistleblowing matters to discuss recent developments, work together to address perceived gaps in existing programs, and increase the Intelligence Community's knowledge about whistleblowing rights and the lawful ways whistleblowers can make protected disclosures. The ICIG is grateful for the many Congressional Members and staff, for the Council of the Inspectors General on Integrity and Efficiency, and for Inspectors General from across the federal government and others who have lent their unwavering support to whistleblowers.

During my confirmation hearing, when I was asked repeatedly by numerous senators on both sides of the aisle about my commitment to the ICIG's Whistleblowing Program and to whistleblowers generally, I testified under oath that I would work with Congress "to encourage, operate, and enforce a program for authorized disclosures within the Intelligence Community that validates moral courage without compromising national security and without retaliation." I said that I would:

> enforce a safe program where whistleblowers do not have fear of retaliation and where they're confident that the system will treat them fairly and impartially, so that we can secure national security and allow whistleblowers to make their complaints of unethical or illegal behavior without risking unauthorized disclosures.

I am committed to doing what I promised I would do, and living up to and upholding that oath. It is my hope that recent events will not have a chilling effect on the willingness of individuals within the Intelligence Community to continue to shed light on suspected fraud, waste, abuse, or malfeasance in an authorized manner. In the meantime, the ICIG will continue to work on behalf of the American people to ensure that individuals in the Intelligence Community and throughout the federal government have a consistent, authorized, effective, and protected means to report their concerns.

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

Michael K. Atkinson
Inspector General
October 31, 2019

[1] The Intelligence Community Inspectors General Forum consists of the twelve statutory or administrative Inspectors General with oversight responsibility for an element of the Intelligence Community.

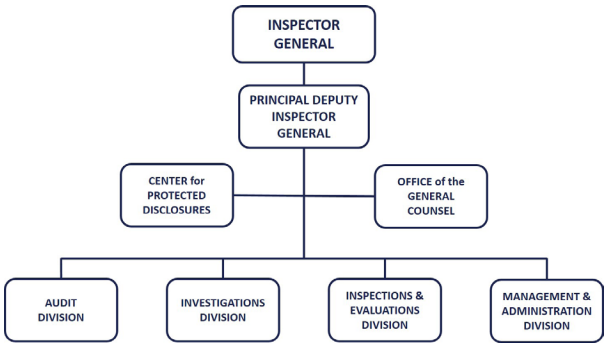
INTRODUCTION

Authority

The Office of the Inspector General of the Intelligence Community (ICIG) was established within the Office of the Director of National Intelligence (ODNI) by the *Intelligence Authorization Act for Fiscal Year 2010*. 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.

Organization

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 organizational divisions are Audit, Investigations, Inspections and Evaluations, and Management and Administration. The ICIG employs a highly skilled, committed, and diverse workforce, including permanent employees (cadre), employees from other Intelligence Community (IC) elements and other government entities on detail to the ICIG (detailees), and contractors. Additional personnel details are listed in the classified Annex of the ICIG's Semiannual Report.

Audit Division

The Audit Division conducts independent and objective audits and reviews of ODNI programs and activities, including those nondiscretionary audits required by law, such as the annual independent evaluation of ODNI's information security program and practices required by the *Federal Information Security Modernization Act* (FISMA); the annual review of ODNI's compliance with the *Improper Payments Elimination and Recovery Act* (IPERA); the annual risk assessment of purchase and travel card programs; and the biennial report to Congress – prepared jointly with the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury – on the actions taken to carry out the Cybersecurity Act of 2015. The Audit Division participates with other federal agencies and departments in conducting joint reviews of IC programs and activities.

Audit Division activities improve business practices to better support the Intelligence Community's mission; help reduce fraud, waste,

abuse, and mismanagement; and promote the economy, efficiency, and effectiveness of programs and operations throughout ODNI and the IC. Audit work focuses on information technology and security, acquisition policies and practices, project management, business practices, human capital, and financial management. Auditors assess whether programs are achieving intended results and whether organizations are complying with laws, regulations, and internal policies in carrying out programs.

The ICIG's audit activities are conducted in accordance with generally accepted government auditing standards.

Investigations Division

The Investigations Division is authorized to conduct proactive and reactive criminal and administrative investigations arising from complaints or information from any person concerning the existence of an activity within the authorities and responsibilities of the Director of National Intelligence constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety. As part of its work, the Investigations Division identifies and reports internal control weaknesses that could render ODNI or other IC programs and systems vulnerable to exploitation, and which could potentially be leveraged for illicit activity resulting in ill-gotten gains. The Investigations Division also plays a principal role in tracking, monitoring, and investigating unauthorized disclosures of classified information.

The Investigations Division has unique authority to investigate programs and activities across the IC within the responsibility and authority of the Director of National Intelligence. Through this authority, the Investigations Division is able to coordinate and assist with the prosecution of criminal matters arising from the six independent intelligence agencies: the National Reconnaissance Office, National Geospatial-Intelligence Agency, National Security Agency, Defense Intelligence Agency, Central Intelligence Agency, and the Office of the Director of National Intelligence.

The ICIG's investigation activities conform to standards adopted by the Council of the Inspectors General on Integrity and Efficiency.

Investigative Activity Overview

The Investigations Division continued its efforts to investigate, among other things, cross-Intelligence Community fraud, public corruption, and counterintelligence matters. It is currently working on five joint criminal investigations involving ten other law enforcement organizations, including the Federal Bureau of Investigation (FBI), Intelligence Community Offices of Inspectors General, Defense Criminal Investigative Service, and other local and federal investigative agencies, as well as the Department of Justice Public Integrity Section, the U.S. Attorney's Office for the Eastern District of Virginia, and the Fairfax County Commonwealth Attorney's Office. The Investigations Division expects these investigations to continue into the next reporting period due to the size, scope, and nature of the matters.

One of those matters resulted in a former Assistant Inspector General for the United States Department of Housing and Urban Development, Office of Inspector General, being charged in a seven-count indictment, which was returned on June 26, 2019. The indictment charged that individual with engaging in a scheme to conceal material facts, making false statements, and falsification of records. An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Additionally, the Division's investigative efforts and internal coordination with the Office of the Director of National Intelligence (the Chief Operating Officer, Contracting Activity, and the Chief Financial Executive) resulted in the recoupment of $229,497 to the United States Treasury resulting from a substantiated labor mischarging investigation previously reported in the ICIG's October 1, 2018 through March 31, 2019 Semiannual Report. The Investigations Division initiated the investigation through proactive counter-fraud efforts, which identified discrepant time and attendance records versus hours billed to a government contract. As a

further result of the investigation, the Office of the Director of National Intelligence removed the contract employee from working on the government contract.

The Investigations Division also completed a joint investigation with the National Geospatial-Intelligence Agency Office of Inspector General and the Defense Criminal Investigative Service, regarding procurement issues with a sensitive software used by the U.S. government. Although the investigation resulted in unsubstantiated findings as to the allegations, information uncovered in the investigation resulted in a recommendation to include a clause requiring a software developer to identify potential foreign origin software to agencies purchasing software under a Blanket Purchase Agreement. The clause was added to 5 of the 14 existing agreements with the developer, and will be included in all IC Enterprise License Agreements and Enterprise Agreements for software as they are presented for renewal. The inclusion of this clause will enhance the ability of the agencies to make informed decisions about whether foreign origin software is acceptable for their particular agencies and operations.

Currently, the Investigations Division has 20 ongoing investigations, of which nine were initiated during this reporting period (*see* table below). The Investigations Division substantiated two investigations involving time and attendance fraud, misuse of government property, and false statements. It closed three investigations.

Summaries of Substantiated Investigations

Time and Attendance Fraud

An investigation substantiated allegations of time and attendance fraud by an ODNI cadre employee. Investigators determined that the employee fraudulently submitted and certified time and attendance records, claiming 303 regular work hours that the employee had not actually worked, and for which he was not present at the worksite. The loss to the government was approximately $16,000. Recoupment of funds and potential disciplinary actions are pending.

Alleged Misuse of Government Property

The Investigations Division, in coordination with the Central Intelligence Agency Office of the Inspector General, substantiated the allegation that a government contractor employee misused government systems when the employee accessed a sensitive database to conduct unofficial and unauthorized searches. The employee was removed from the contract and the ICIG is awaiting information regarding additional actions taken, if any.

Table: Ongoing Investigations

Number of Cases	Case Subject/Allegation
1	Qui Tam – Contract and Procurement Fraud
1	Unauthorized Disclosure
3	Conflict of Interest
6	Contract Cost Mischarging (Labor)
2	Misuse of Government Property (Computer)
3	Abuse of Authority/Retaliation
1	Time and Attendance Fraud
1	False Official Statement
1	Use of Illegal Drugs
1	Mismanagement
20	

The ICIG did not issue any subpoenas during this reporting period.

Inspections and Evaluations Division

The Inspections and Evaluations Division works to improve the performance and integration of ODNI and the broader Intelligence Community. The Division conducts independent assessments of the design, implementation, and results of agency and community operations, programs, and policies. It issues evidence-based findings that are timely, credible, and useful for managers and other stakeholders. The Inspections and Evaluations Division often recommends ways

to improve performance, and identifies when administrative action is necessary.

The Inspections and Evaluations Division's findings typically focus on program, workforce, financial, contracts, and facilities management; information technology security; and integration, coordination, and sharing of information. The Inspections and Evaluations Division also highlights best practices and promising approaches.

The ICIG's inspection activities conform to standards adopted by the Council of the Inspectors General on Integrity and Efficiency.

Management and Administration Division

The Management and Administration Division provides mission support to the operational divisions of the ICIG. The Division is composed of multidiscipline officers who provide expertise in financial management, human capital and talent management, facilities and logistics management, continuity of operations, administration, classification, Freedom of Information Act requests, information technology, communications, and quality assurance. The Management and Administration Division also delivers executive support to the Intelligence Community Inspectors General Forum and its associated committees.

During this reporting period, ODNI provided the ICIG adequate funding to fulfill its mission. The budget covered personnel services and general support, including travel, training, equipment, supplies, information technology support, and office automation requirements. As the ICIG assessed IC programs and activities to promote effectiveness, economy, and efficiency, it also continued to examine its own internal operations to develop and implement greater accountability and operational efficiencies. Some of the Management and Administration Division's notable achievements during this reporting period include:

- Developing and delivering training to Inspector General offices across several IC components on classification management issues, including: sensitive reviews, public releases, and communications with Congress.
- Instituting processes and procedures to streamline Freedom of Information Act (FOIA) reviews, thereby enabling the ICIG to receive and process 117% more FOIA cases compared to this time last year, and to increase the ICIG's closure rate by 92% compared to the prior fiscal year.
- Developing significant updates to three ICIG System of Record Notices (SORNs) to ensure compliance with National Archives and Records Administration (NARA) regulations.
- Securing additional legal support for the Center for Protected Disclosures and Office of the General Counsel to enhance the ICIG's ability to timely respond to mission critical matters, such as whistleblower and FOIA matters.
- Developing and implementing the first ICIG Recruitment Program, with the initial phase focused on recruiting critical, hard-to-fill auditor positions, which has proved a systemic issue across the federal government. The ICIG is the first ODNI component to be granted approval to use new recruitment methods, such as posting to various websites and professional associations, including *Indeed.com*, the *Virginia Society of Certified Public Accountants*, and the *Association of Government Accountants*. ICIG representatives also attended college recruiting events at the University of Maryland, Loyola University-Maryland, Hampton University, American University, and Norfolk State University to optimize and broaden the pool of candidates who possess specialized skills and experience in the audit or accounting arenas. Posting the auditor vacancies on these external websites and participating in college recruiting events has increased and diversified the pool of entry- and mid-level candidates with the skills and experience required for the auditor positions within the ICIG.

Office of the General Counsel

The ICIG's Office of the General Counsel (OGC) ensures that the ICIG receives independent and confidential advice and counsel that is without any conflicts of interest in fact or appearance.

The Office of the General Counsel supports the Investigations Division throughout the investigative process by highlighting and providing guidance on potential legal issues meriting additional or redirected investigative efforts.

OGC supports the Audit Division and the Inspections and Evaluations Division by identifying and interpreting key policy, contract, and legal provisions relevant to reported observations, findings, and recommendations. OGC also provides legal and policy guidance, and reviews issues related to ICIG personnel, administration, training, ethics, independence, and budgetary functions.

The Office of the General Counsel also serves as the ICIG's Congressional Liaison. During the reporting period, OGC arranged for and participated in several congressional briefings with the Inspector General and senior ICIG leadership, including briefings to Members of Congress and dozens of bipartisan staff, responded to formal congressional requests for information, and reported on completed audits in response to congressional interest and legislative mandates. Engagements during this reporting period included the following:

- Appearing before members of the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI), to discuss matters related to a disclosure submitted to the ICIG of an alleged "urgent concern" pursuant to 50 U.S.C. § 3033(k)(5)(A).
- Engaging with bipartisan SSCI and HPSCI Members and staff to timely respond to inquiries related to ongoing matters within the ICIG.
- Arranging for and leading a joint, bipartisan, bicameral discussion with the ICIG and Inspectors General from the National Reconnaissance Office, Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, and the Central Intelligence Agency, along with staff from both the SSCI and HPSCI to discuss provisions within the *Intelligence Authorization Act for Fiscal Year 2018, 2019, and 2020*, that have significant impact on the Intelligence Community Inspectors General.
- Facilitating a meeting with the Comptroller General of the United States and the ICIG to discuss ongoing matters, issues of common concern, and initiatives to enhance coordination between the Government Accountability Office (GAO) and the Intelligence Community Inspectors General.
- Cooperating with GAO in its review of whistleblower protections in the Intelligence Community.
- Facilitating a joint exit conference with the GAO and representatives of the Inspectors General of the Intelligence Community, Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency to discuss the IGs' thoughts and comments related to GAO's draft report regarding Intelligence Community Whistleblower Programs.
- Responding to letters, emails, and phone calls from Members and staff from numerous congressional committees, including the Senate Judiciary Committee, Senate Committee on Homeland Security and Governmental Affairs, Senate Finance Committee, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence, to address committee questions regarding pending legislation and other matters within the ICIG's jurisdiction.

The Center for Protected Disclosures

In 2018, the ICIG formed a new Center for Protected Disclosures (the Center), which has as one of its primary functions the processing of complaints from whistleblowers under the *Intelligence Community Whistleblower*

Protection Act (ICWPA). In early 2019, the ICIG hired a new Hotline Program Manager as part of the Center for Protected Disclosures to oversee the ICIG's Hotline. In June 2019, a newly hired Director for the Center for Protected Disclosures entered on duty.

The Center for Protected Disclosures processes whistleblower reports and supports whistleblower protections. In addition, the Center administers requests by employees and contractors in the Intelligence Community for the ICIG to review their allegations of reprisal under Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*. The Center also provides guidance to whistleblowers, as well as community outreach on whistleblower protections and training.

The Center also processes complaints or information with respect to alleged urgent concerns in accordance with the ICWPA and the ICIG's authorizing statute, 50 U.S.C. 3033 § (k)(5)(A). In order to file an urgent concern, the law requires that a complainant be "[a]n employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community." *Id*. at § 3033(k)(5)(A).

The law also requires that a complainant provide a complaint or information with respect to an "urgent concern," which is defined, in relevant part, as:

> A serious or flagrant problem, abuse, violation of the law or Executive order, or deficiency relating to the funding, administration, or operation of an intelligence activity within the responsibility and authority of the Director of National Intelligence involving classified information, but does not include differences of opinions concerning public policy matters." *Id*. at § 3033(k)(5)(G)(i).

In addition, the law requires the Inspector General of the Intelligence Community within 14 calendar days to determine whether information with respect to an urgent concern "appear[s] credible." *Id*. at § 3033(k)(5)(B). The law does not require that the complaint be based on first-hand information. In fact, by law, any individual in the Intelligence Community who wants to report information with respect to an urgent concern to the congressional intelligence committees need not possess first-hand information.

After the Center for Protected Disclosures was formed in 2018, and since the new Director and other managers started on duty in 2019, the ICIG has been reviewing the forms it provides to whistleblowers who wish to disclose allegations of potential wrongdoing to the ICIG, including information with respect to an alleged urgent concern to the congressional intelligence committees. In the process of reviewing and clarifying those forms, the ICIG understood that certain language in some of its forms and, more specifically, the informational materials accompanying the forms, could be read – incorrectly – as suggesting that whistleblowers must possess first-hand information in order to file an urgent concern complaint with the congressional intelligence committees. The ICIG has taken the necessary steps to correct that misconception, as the ICIG cannot add conditions to the filing of an urgent concern that do not exist in law.

Accordingly, the ICIG's Center for Protected Disclosures has developed three new forms entitled, "Report of Fraud, Waste, and Abuse UNCLASSIFIED Intake Form"; "Disclosure of Urgent Concern Form – UNCLASSIFIED"; and "External Review Panel (ERP) Request Form – UNCLASSIFIED." These three new forms are now available on the ICIG's open website and were also added to the ICIG's classified system. The ICIG will continue to update and clarify its forms and its websites to ensure its guidance to whistleblowers is clear and strictly complies with statutory requirements. Consistent with the law, the new forms do not require whistleblowers to possess first-hand information in order to file a complaint or information with respect to an urgent concern.

In making these changes, the ICIG is working to effectuate Congress' intent, within the rule of law, and will continue in those efforts on behalf of all whistleblowers in the Intelligence Community.

INDEPENDENCE

The Inspector General of the Intelligence Community is nominated by the President of the United States and confirmed by, and with the advice and consent of, the United States Senate. 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 are revealed through exhaustive audits, investigations, inspections, and programmatic reviews. During this reporting period, the ICIG had full and direct access to all information that relates to the programs and activities with respect to which the ICIG had responsibilities.

ICIG MISSION

The Inspector General of the Intelligence Community'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.

ICIG STRATEGIC GOAL

The ICIG's goal is to have a positive and enduring impact throughout the Intelligence Community, to lead and coordinate the efforts of an integrated Intelligence Community Inspectors General Forum, and 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.

ICIG CORE VALUES

INTEGRITY

INDEPENDENCE

COMMITMENT

DIVERSITY

TRANSPARENCY

THE INSPECTOR GENERAL COMMUNITY

This year marks the 41st 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 Office of the Inspector General of the Intelligence Community, one of 74 Inspectors General collectively overseeing the operations of nearly every aspect of the federal government, looks forward to continuing to work with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) on important issues that significantly affect productivity, transparency, and accountability throughout the federal government.

Oversight.gov

Oversight.gov provides a "one stop shop" to follow the ongoing oversight work of all Offices of Inspectors General (OIGs) that publicly post reports. CIGIE manages the website on behalf of the federal Inspector General community. The ICIG, like other OIGs, will continue to post reports to its own website as well as to *Oversight.gov* to afford users the benefits of the website's search

and retrieval features. *Oversight.gov* allows users to sort, search, and filter the site's database of public reports from all CIGIE member OIGs to find reports of interest. In addition, the site features a user-friendly map that allows users 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 @OversightGov, CIGIE's Twitter account.

The ICIG's main office is in Reston, Virginia.

ICIG PROGRAMMATIC OBJECTIVES

In the ICIG's Semiannual Report for the period of October 2018 – March 2019, the ICIG identified five programmatic objectives that served as measures by which the ICIG categorized its projects and activities. These areas were selected after a comprehensive review of reports, including the *2019 U.S. National Intelligence Strategy*; the *Consolidated Intelligence Guidance for Fiscal Years 2020-2024*; the *IC2025 Vision and Foundational Priorities*; the *Office of the Inspector General of the Intelligence Community's Management and Performance Challenges for the Office of the Director of National Intelligence*, as well as Management and Performance Challenges for the Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency; the Government Accountability Office's High Risk Series reports; and the Council of Inspectors General on Integrity and Efficiency FY 2018 report, *Top Management and Performance Challenges Facing Multiple Federal Agencies.*

The objectives, established in early 2019, are again recognized in this Semiannual Report. The ICIG has selected the following five programmatic objectives to focus upon:

1. Improving the Efficiency and Effectiveness of the Intelligence Community's Cyber Posture, Modern Data Management, and IT Infrastructure
2. Enhancing Workforce Management
3. Championing Protected Disclosures
4. Improving Oversight of Artificial Intelligence
5. Integrating the Intelligence Community

1 Improving the Efficiency and Effectiveness of the IC's Cyber Posture, Modern Data Management, and IT Infrastructure

The Intelligence Community has identified cybersecurity as one of its most important priorities, as reflected in the 2019 National Intelligence Strategy, the DNI's IC2025 Vision and Foundational Priorities, the 2018 Management and Performance Challenges for the Office of the Director of National Intelligence (ODNI), and budget requests spanning multiple fiscal years. Ongoing and future projects selected by the ICIG will review and evaluate the effectiveness of ODNI's information security and the cohesiveness of cyber and information technology (IT) integration across the Intelligence Community.

Management of Privileged Users of Office of the Director of National Intelligence Information Systems

During the reporting period, the Audit Division completed an audit of the management of privileged users. Privileged users are authorized and trusted to perform security-related functions over information systems that ordinary users are not authorized to perform. Privileged users have important roles in protecting ODNI information security due to their broad administrative and technical privileges. The misuse of privileged user functions increases the risk for compromise of the confidentiality, integrity, and availability of ODNI information systems.

ICIG auditors determined that ODNI needs to improve controls to efficiently and effectively manage and mitigate the risk that a trusted privileged user could inappropriately access, modify, destroy, or exfiltrate classified data. The report includes nine recommendations, six of which are significant. ICIG auditors also made an observation on the ODNI compliance monitoring of internal policies.

Additional details are included in the classified Annex of the ICIG Semiannual Report.

Fiscal Year 2019 Independent Evaluation of the Office of the Director of National Intelligence's Information Security Program and Practices, as Required by the *Federal Information Security Modernization Act of 2014*

During the reporting period, the Audit Division continued its work, started in April 2019, to assess the effectiveness and maturity of ODNI's information security program and practices for Fiscal Year 2018, as required by the *Federal Information Security Modernization Act of 2014* (FISMA). FISMA requires an annual independent evaluation of federal agencies' information security programs and practices. The ICIG performed this evaluation using the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* developed by the Office of Management and Budget, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency.

The ICIG anticipates releasing its final report early in the first quarter of Fiscal Year 2020.

Cybersecurity Information Sharing Act of 2015

In early 2019, the ICIG initiated an audit of ODNI's implementation of the *Cybersecurity Information Sharing Act of 2015* (CISA). As required by § 107(b), CISA, *Oversight of Government Activities – Biennial Report on Compliance*, the Inspectors General of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury, and the Intelligence Community, in consultation with the Council of Inspectors General on Financial Oversight, must jointly submit an interagency report to Congress. The results of the audit

will be reported to ODNI and included in the interagency report.

This audit will evaluate, among other things, the sufficiency of ODNI's policies and procedures related to sharing cyber threat indicators within the federal government; proper classification of cyber threat indicators or defensive measures; actions taken by the federal government based on shared cyber threat indicators or defensive measures; and barriers to sharing information about cyber threat indicators and defensive measures. The audit of ODNI and the joint project are ongoing.

ODNI Oversight of IC Major System Acquisition Cybersecurity Risks

In November 2018, due to the criticality of cybersecurity and cascading incidents worldwide, the ICIG launched a review to evaluate the efficiency and effectiveness of existing authorities, policies, and processes applicable to the Office of the Director of National Intelligence's oversight of IC Major System Acquisition cybersecurity risks. The *Intelligence Reform and Terrorism Prevention Act of 2004* empowered the Director of National Intelligence with milestone decision authority for Intelligence Community Major System Acquisitions. In accordance with Intelligence Community Directive 801, *Acquisition*, the Office of the Director of National Intelligence conducts acquisition oversight of National Intelligence Program-funded Major System Acquisitions. Recent initiatives such as the *Improving Cybersecurity for the Intelligence Community Information Environment (IC IE) Implementation Plan* have increased the focus on cybersecurity and, when fully implemented, should significantly improve the IC cybersecurity posture. In conjunction with these initiatives, the review identified opportunities to assist ODNI in improving the efficiency and effectiveness of Major System Acquisition cybersecurity risk oversight throughout the acquisition lifecycle.

2 Enhancing Workforce Management

The ICIG established this objective based on the Right, Trusted, Agile Workforce foundational priority as identified in the Director of National Intelligence's IC2025 Vision and Foundational Priorities and the People enterprise objective outlined in the National Intelligence Strategy. The projects highlighted below contribute to this priority by ensuring that the workforce has the necessary tools to carry out the mission of the Intelligence Community.

Security Clearance Working Group

An effective and efficient government-wide personnel security clearance process helps ensure that relevant security information is identified and assessed in a timely manner to enable agencies to recruit and retain qualified and trusted employees and contractors. Executive Order 13467 assigns the Director of National Intelligence responsibility, as the Security Executive Agent, for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information and to hold a sensitive position. The Director of National Intelligence has instituted a variety of reform efforts designed to improve background investigation and adjudication timeliness, and improve the quality of information used to make security clearance decisions, compile system-wide metrics, and assess and oversee personnel security program implementation across the Executive branch. Despite these reform efforts, the processing of security clearances within the IC has been a longstanding and continuing challenge.

To appropriately plan oversight work on this critical challenge, in November 2018, the Office of the Inspector General of the Intelligence Community initiated preliminary research to collect information concerning policies and practices for reporting on the security clearance process. Based on the ICIG's research, ideas for a number of projects were developed and prioritized based on risk. During Fiscal Year 2020, the ICIG will initiate two projects. The Audit Division will conduct an audit of the integrity and use of security clearance data reported to ODNI by the following Intelligence Community elements: the Central Intelligence Agency, Defense Intelligence Agency, Department of State, Federal Bureau of Investigation, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, and Office of the Director of National Intelligence. The objectives of the audit are to determine whether Intelligence Community elements accurately capture, document, and report required security clearance processing timeliness information; Intelligence Community elements calculate processing timeliness in a consistent manner; the Security Executive Agent accurately compiles and reports data provided by the Intelligence Community elements, as required; and whether the Security Executive Agent uses timeliness data to address the security clearance backlog and inform security clearance-related policy decisions. The Inspections and Evaluations Division will engage in a review of the IC's implementation of security clearance reciprocity.

Compliance with the *Improper Payments Elimination and Recovery Act of 2010*

The *Improper Payments Elimination and Recovery Act of 2010* (IPERA) directs 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). IPERA 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 this review was to determine whether the Office of the Director of National Intelligence complied with the requirements of IPERA for Fiscal Year 2018.

The ICIG reported that for Fiscal Year 2018, the Office of the Director of National Intelligence complied with IPERA. The ODNI published its Fiscal Year 2018 Agency Financial Report on November 14, 2018, and posted the report on its internal website. In Fiscal Year 2018, the third year of the ODNI risk assessment cycle, ODNI tested payment controls and determined that none of its programs and activities were susceptible to significant improper payments, as defined by the Office of Management and Budget. Based on this determination, the ODNI was not required to prepare or report improper payment estimates, corrective action plans, reduction targets, or improper payment rates for its programs and activities. As required by IPERA, ODNI supported its determination that conducting payment recapture audits would not be cost effective. This report had no recommendations.

Conference Spending

During the reporting period, the Audit Division completed an audit of ODNI's management and oversight of conference spending. The objective of the audit was to determine whether ODNI-sponsored conferences were appropriately justified, approved, funded, and reported in accordance with applicable laws, policies, and procedures.

The audit determined that:

- ODNI components generally provided appropriate justifications for ODNI-sponsored conferences.
- Conference approvals were not always occurring before the obligation of funds or prior to the conference start date.
- Two of the 44 conferences tested were not approved by the appropriate authority.
- ODNI components did not always provide sufficient documentation in the Conference Coordination Database to determine whether appropriate funding was used and expenses were recorded to the proper budget object class.
- In contradiction to the bona fide needs rule of federal appropriations law, ODNI used Fiscal Year 2017 funds for a conference held in Fiscal Year 2018.
- As of February 2019 – more than 120 days after the end of Fiscal Year 2018 – nearly half (84) of ODNI's 172 Fiscal Year 2018 conferences were still listed in an "approved" status, meaning that components had not reported the final costs.
- Of the conferences tested by the auditors with a "completed" status, almost all of these conferences did not include sufficient information to support final costs.

The report included recommendations calling for ODNI's Chief Financial Executive to establish and implement processes to correct control weaknesses identified in the report, and to identify and record appropriate funding to cover the Fiscal Year 2018 conference expenses.

ODNI's Charge Card Program

The ICIG's Audit Division is continuing its review of ODNI's charge card program for Fiscal Years 2016 and 2017. The objective of the audit is to determine whether internal controls are sufficient to prevent and detect illegal, improper, and erroneous use of government travel cards. The results of this audit will be reported in the next Semiannual Report.

Assessment of the Office of the Director of National Intelligence Methods Used to Substantiate Post-Secondary Education Claims Made by ODNI Cadre Employees Subsequent to Entry-on-Duty

In November 2018, the Inspections and Evaluations Division initiated a review of methods used to substantiate ODNI employees' post-secondary education claims made after their Entry-on-Duty as ODNI employees. The review uncovered no reported cases of ODNI cadre officers making false post-secondary education claims. The review found, however, that ODNI lacked policies and procedures related to the validation of such declarations creating a potential opportunity for the falsification of qualifications of personnel performing national security functions. The ICIG had three findings and recommended actions to mitigate insufficient verification controls and reduce vulnerabilities. On August 29, 2019, the (Acting) Director of National Intelligence acknowledged the ICIG review and recommendations.

Additional details are listed in the classified Annex of the ICIG's Semiannual Report.

3 Championing Protected Disclosures

Intelligence Community employees and contractors collect and analyze information to develop the most accurate and insightful intelligence possible on threats to our national security. These Intelligence Community professionals serve in a classified work environment in which information about intelligence programs and activities is not available for public review, which makes their duty to lawfully disclose information – or blow the whistle – regarding potential wrongdoing, including fraud, waste, abuse, and corruption, that much more critical to the oversight process.

Whistleblowing is the lawful disclosure to an authorized recipient of information a person reasonably believes evidences wrongdoing. It is the mechanism to relay the right information to the right people to counter wrongdoing and promote the proper, effective, and efficient performance of the Intelligence Community's mission. Whistleblowing in the IC is extremely important as it ensures that personnel can "say something" when they "see something" through formal reporting procedures without harming national security and without retaliation.

To support this effort, the ICIG established the Center for Protected Disclosures (the Center). The Center covers three functional areas critical for whistleblowers in the Intelligence Community.

First, the Center receives and processes whistleblower complaints through the ICIG's Hotline program. The 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 McLean, Virginia, and Bethesda, Maryland. The Center also receives complaints filed via drop boxes located in various ODNI facilities.

The Hotline program also receives and processes allegations of "urgent concerns" disclosed pursuant to the *Intelligence Community Whistleblower Protection Act* (ICWPA). The ICWPA established a process to ensure that the Director of National Intelligence, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence receive disclosures of allegedly serious or flagrant problems, abuses, violations of law or executive order, or deficiencies relating to the funding, administration, or operation of an intelligence activity. The Center tracks all ICWPA disclosures, ensures review of materials for classified information, and coordinates disclosures with other Inspectors General for appropriate review and disposition. During the reporting period, the ICIG transmitted one ICWPA disclosure to the DNI, which was subsequently provided to the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence.

To increase the effectiveness of the ICIG's Hotline program, the ICIG hosted the third Intelligence Community Hotline Working Group to discuss challenges and share best practices with IC Hotline partners. Participants included Hotline managers from the ICIG and the Offices of Inspector General of the Central Intelligence Agency, Defense Intelligence Agency, and the National Reconnaissance Office. The Hotline Working Group intends to meet semiannually to further share procedures and lessons learned.

Second, the Center for Protected Disclosures provides guidance to individuals seeking more information about the options and protections afforded to individuals who may wish to make a protected disclosure to the ICIG and/or Congress, or who believe they have suffered reprisal because they made a protected disclosure. The ICIG also conducts community outreach and training activities to ensure stakeholders present and receive accurate and consistent whistleblowing information relating to these and other matters.

During this reporting period, the Center for Protected Disclosures celebrated *National Whistleblower Appreciation Day* with an event at ICC-B featuring remarks by then-Director of National Intelligence (DNI) Daniel Coats on the importance of whistleblowers and their contributions to good governance. The DNI's remarks were followed by a panel discussion with representatives from across ODNI about complaint resolution and coordination of efforts to receive and respond to whistleblower concerns. This event was streamed live to various IC locations to ensure that people unable to attend in person could nevertheless view the event.

The Center also engaged the ODNI workforce with a *National Compliance Officer Day* event on September 26, 2019. The outreach program was held at ODNI Headquarters in McLean, Virginia. The event highlighted and provided information on the importance of reporting suspected fraud, waste, and abuse, and how to contact the ICIG Hotline.

Third, the Center administers requests by employees and contractors in the Intelligence Community 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 protects employees serving in the IC, or those who are eligible for access to classified information, by prohibiting reprisal for reporting fraud, waste, and abuse, while protecting classified national security information. The ICIG has unique and important responsibilities under PPD-19, including the administration of external review processes to examine allegations of whistleblower reprisal. Under PPD-19, an individual who believes they have suffered reprisal for making a protected disclosure is required to exhaust their agency's applicable review process for whistleblower reprisal allegations before requesting an ICIG external review. 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 eleven new ERP requests during the current reporting period, five of which were denied and closed following an initial assessment and review of materials submitted by both the complainant and the complainant's employing agency. The ICIG is conducting initial assessments of the remaining six new ERP requests. The Center is conducting one ERP on a request filed during the previous reporting period. The ICIG monitored an ERP request being evaluated by an Inspector General under the procedures in PPD-19, Section C. In addition, an ERP request was completed during this reporting period by another Inspector General, under the procedures in PPD-19, Section C, and the results were reported to the Requestor and the component.

Intelligence Community Directive 701

There is a need to clearly distinguish between whistleblowers and those individuals who make unauthorized disclosures by taking it upon themselves to decide what classified information should be disclosed to the public. Whistleblowers make use of formal reporting procedures that will protect both the classified information and the whistleblower. Any disclosure of classified information falling outside of these established procedures constitutes an unauthorized disclosure – not protected whistleblowing – and falls into the realm of insider threat behavior. Unauthorized disclosures put sensitive operations and intelligence sources and methods at risk. In addition, failing to effectively address unauthorized disclosures reduces the incentive for the IC's workforce to use formal reporting procedures to make protected disclosures to report allegations of fraud, waste, or abuse involving classified information.

The ICIG is conducting an evaluation of the implementation of Intelligence Community Directive (ICD) 701, *Unauthorized Disclosure of Classified Information*. Specifically, ICD 701 governs Intelligence Community efforts to deter, detect, report, and investigate unauthorized disclosures of classified national security information. ICD 701 directs the Intelligence Community to accomplish these tasks by training personnel, developing comprehensive personnel security programs, conducting audits and system monitoring, and devising other appropriate

measures to deter and detect unauthorized disclosures. Additional requirements of ICD 701 are to conduct preliminary inquiries into possible unauthorized disclosures, provide notifications and reports to appropriate authorities, and conduct investigations as required. This cross-Intelligence Community evaluation of ICD 701 is ongoing.

The Investigations Division continued its efforts during the review period to meet its responsibilities under ICD 701. These efforts included outreach and liaison discussions related to the status of ICD 701 reporting programs, formalizing reporting processes to ensure that appropriate notifications are made in a timely fashion, and engaging in benchmarking efforts to identify obstacles to appropriate implementation. The liaison and outreach efforts included multiple IC elements, and leveraged the expertise and institutional knowledge from all agencies and elements.

In May 2019, the Intelligence Community Inspectors General Forum's Investigations Committee hosted representatives from the IC elements, their legal counsels, and ODNI's Policy and Strategy Division to discuss, among other things, the threshold and process for reporting unauthorized disclosures. The goal is to increase transparency, develop community principles, and enhance the understanding and consensus on the implementation requirements of ICD 701. The Investigations Division will continue to further identify areas to increase efficiencies and effectiveness related to ICD 701.

4 Improving Oversight of Artificial Intelligence

Data is one of the cornerstones of work conducted by Offices of Inspectors General. Whether text dense criteria documents or structured databases of transactional or financial data, Offices of Inspectors General face mounting challenges in finding, sorting, and analyzing vast amounts of data. The ICIG selected artificial intelligence as an objective for review due to the presence it has played in multiple documents and reports published by ODNI. In the Augmenting Intelligence using Machines (AIM) Initiative, former Director of National Intelligence Daniel Coats identified artificial intelligence as a vehicle to increase mission capability and enhance data interpretation throughout the IC.

As noted in the ICIG's previous Semiannual Report, the ICIG is coordinating Intelligence Community Offices of Inspectors Generals' efforts to identify both the opportunities and challenges presented by machine learning and artificial intelligence. In light of the Director of National Intelligence's *IC2025 Vision and Foundational Priorities'* "Augmenting Intelligence using Machines (AIM)" Initiative, the ICIG took initial actions to build general awareness and common understanding among Intelligence Community oversight authorities in the following areas:

- **Building a Community of Interest:** Drawing from the interest expressed by participants in the *Making Better Use of Data: Automation, Analytics, and AI* break-out session at the *2019 Intelligence Community Inspectors General Annual Conference*, the ICIG has begun exploring the viability of establishing an Intelligence Community Offices of Inspectors General Community of Interest (CoI) as a forum for follow-on discussion. The ICIG intends to leverage the perspectives of 30 session participants who expressed their interest in future collaboration. They represent 12 Intelligence Community Offices of Inspectors General: the Office of the Inspector General of the Intelligence Community, Central Intelligence Agency, Defense Intelligence Agency, Department of Defense, Department of Energy, Department of Justice, Department of State, Department of Treasury, Federal Bureau of Investigation, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency. Their work spans eight distinct functional areas: Audit, Data Analytics, Front Office, Forensic Analysis, Inspections and Evaluations, Investigations, Management and Administration, and Overseas Contingency Operations Oversight. Their input will help shape how the CoI is formed and how it relates to the Intelligence Community Inspectors General Forum and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and their subordinate entities having shared areas of interest.
- **Enhancing individual and collective understanding:** The ICIG continues exploring opportunities for Offices of Inspectors General to advance their understanding of this transformative field, and their capabilities to audit, investigate, inspect, and evaluate its implementation. The ICIG has engaged subject matter experts and stakeholders across the Intelligence Community, the federal government, academia, and industry to begin mapping the landscape of AIM-related research, planning, implementation, and governance activities. The ICIG's outreach to ODNI's AIM Champion resulted in ground-breaking presentations to the Intelligence Community Inspectors General Forum principals, the Inspections and Evaluations Committee, and the Data Analytics Working Group. The ICIG conducted initial discussions with the IC Artificial Intelligence Ethics Working Group, the Intelligence Community Chief Data Officer, the Office of the Director of National

Intelligence's Strategic Priorities Division, and the Intelligence and National Security Alliance (INSA). The ICIG also participated in and will share insights developed from the 2019 annual *IC Data Science Technical Exchange*, the *Kalaris Intelligence Conference 2019 – AI and National Security*, Federal Computer World's *2019 Emerging Technologies Summit*, the Association of Government Accountants/Chief Financial Officers Council/CIGIE *Impacts of Emerging Technologies on the Workforce Forum*, and data analysis/visualization user groups within the intelligence and defense communities.

- **Developing criteria and measures:** The ICIG has begun to compile a listing of existing and projected efforts being pursued under the aegis of the AIM Initiative. Combined with the ICIG's concurrent efforts to identify and leverage ongoing discussions across government, industry, and advocacy groups about artificial intelligence governance, the ICIG will advance Intelligence Community Offices of Inspectors General's ability to develop criteria and measures for evaluating investments in oversight of artificial intelligence in terms of personnel, training, and technology.
- **Information exchanges and collaboration:** The ICIG has expanded its own previous outreach efforts to and engagements of CIGIE's Data Analytics Working Group and CIGIE's newly established Emerging Technology Subcommittee. The ICIG has identified areas of mutual interest for potential collaboration, including a future offering of CIGIE's 2017 day-long *Data Analytics Forum*, and planning a proposed Emerging Technology Subcommittee-sponsored half-day event focused on defining the parameters of meaningful oversight in this revolutionary new landscape. The ICIG continues its work to enable shared situational awareness within the Inspector General community, both in the Intelligence Community and the broader federal government.
- **Education and training resources:** The ICIG has begun to research and compile an initial list of government and academic entities with existing classes, courses, and seminars that could substantively broaden and deepen Intelligence Community Offices of Inspectors General's expertise in addressing data and artificial intelligence-related issues and topics. The ICIG plans to share these for consideration by the Intelligence Community Inspectors General Forum, CIGIE's Professional Development Committee, CIGIE's Emerging Technology Subcommittee, and the CIGIE Training Institute for discussion and expansion.

5 Integrating the Intelligence Community

The ICIG identified Integrating the Intelligence Community as a programmatic objective because it is fundamental to ODNI's mission and national security. When created by the Intelligence Reform and Terrorism Prevention Act of 2004, ODNI was given the responsibility to improve information sharing and ensure integration across the IC. Strategic prioritization, coordination, and deconfliction of IC collection, analysis, production, and dissemination of national intelligence are essential to optimizing IC resource management, decision-making, and accomplishing ODNI's mission. ODNI's Integrated Mission Strategy for 2019-2023 and the National Intelligence Strategy identified developing collaborative collection and analysis capabilities, as well as sharing and safeguarding information, as enduring challenges.

Intelligence Community's Foreign Language Program

The Office of the Inspector General of the Intelligence Community continues its work, launched in February 2019, to evaluate the effectiveness of the Intelligence Community Foreign Language Program (ICFLP) in achieving IC mission objectives. The Program was authorized via the *Intelligence Authorization Act of Fiscal Year 2005*, with the mission "to improve the education of IC personnel in foreign languages critical in meeting the long-term intelligence needs of the United States." The Director of National Intelligence implemented this mandate through Intelligence Community Directive (ICD) 630, *Intelligence Community Foreign Language Capability*, establishing "an integrated approach to develop, maintain, and improve foreign language capabilities across the IC." This evaluation marks the first Inspector General review of the ICFLP since its inception. It focuses on enterprise management in the areas of governance effectiveness, outcomes against ICFLP strategic objectives, and advocacy for budgetary resources and linking allocations to impacts. The goal of this evaluation is to inform ODNI leadership decisions related to the future of the ICFLP within ODNI's current organizational structure and *IC2025 Vision* initiatives.

Though the project was originally focused on the Fiscal Year 2015-2018 timeframe, the ICIG expanded that window to cover the entirety of ODNI's charge to develop and manage the ICFLP, from Fiscal Year 2005 through Fiscal Year 2019. To date, our research and preliminary analysis, informed by interactions with process-owners, partners, and stakeholders indicates the ability to derive knowledge from information in foreign languages is fundamental to conducting the foreign intelligence/counterintelligence mission across all Intelligence Community organizations.

That same research and analysis further indicates that to achieve ICD 630's objective of "an integrated approach to develop, maintain, and improve foreign language capabilities across the IC," effective enterprise management must include all lines of business, such as policy, budget planning and execution, human resources management, technology research and development, and strategic and operational mission planning.

The ICIG anticipates releasing its final report late in the first quarter of Fiscal Year 2020.

European Union-United States Privacy Shield

In September, the Inspector General of the Intelligence Community participated in the third annual review of the European Union-United States Privacy Shield framework held in Washington, D.C. The Privacy Shield regulates and protects personal data transferred from the European Union to the United States for commercial purposes. The terms of the Privacy Shield require an annual review by the European Commission.

Senior United States government officials from the Office of the Director of National Intelligence, and United States Departments of Commerce, Justice, State, and Transportation joined with representatives from the European Union to review privacy issues, compliance monitoring, surveillance activities, and artificial intelligence. Mr. Atkinson provided an overview of the work conducted by Inspectors General in the United States, and the important role they play in protecting the rule of law. He also provided information on the role the ICIG performs in working to ensure the United States fulfills its obligations under the terms of the Privacy Shield framework.

The European Commission will publish its findings of the review in the upcoming months.

Management Challenges Facing the ODNI

The *Reports Consolidation Act of 2000* requires that the Inspector General of the Intelligence Community identify the most serious management and performance challenges facing the Office of the Director of National Intelligence. In September 2019, the ICIG issued its statement outlining what it considered to be the most significant challenges facing ODNI. These were:

1. Reforming the Security Clearance Process
2. Strengthening Information Security and Management
3. Enhancing Intelligence Community Coordination, Integration, and Information Sharing
4. Producing Auditable Financial Statements
5. Improving Management of the Office of the Director of National Intelligence's Workforce
6. Strengthening the Office of the Director of National Intelligence's Management of its Policies

As part of its statement, the ICIG noted one enduring management challenge in the Intelligence Community, highlighted by recent events, relates to efforts to champion protected disclosures, and that one newly emerging topic that will be examined in future projects conducted by the ICIG relates to artificial intelligence (AI).

Additional details are listed in the classified Annex of the ICIG's Semiannual Report.

Intelligence Community Information Sharing Working Group

Since September 11, 2001, the President, Congress, independent commissions, and think tanks have placed greater emphasis on the need for information sharing within the Intelligence Community. The *Intelligence Reform and Terrorism Prevention Act of 2004* and Executive Order 12333 assigned the Director of National Intelligence authorities and responsibilities to provide oversight of the Intelligence Community; this includes the development of guidelines for how information or intelligence is provided to or accessed by the Intelligence Community.

Last year, the Intelligence Community Inspectors General Forum's Inspections Committee noted that no reviews of the Director of National Intelligence's implementation of intelligence and information sharing responsibilities have been conducted to date. The Committee launched an Intelligence Oversight working group to evaluate the merits of a member proposal to review the Director of National Intelligence's implementation of intelligence and information sharing. The working group completed its effort during this Semiannual reporting period. The working group deemed there was merit in conducting a review of the Director of National Intelligence's implementation of intelligence and information sharing responsibilities and forwarded a consensus proposal to the Inspections Committee.

Inspections and Evaluations Navigator Training Tool

The Inspections and Evaluations (I&E) Division continued to partner with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to develop and deploy the *I&E Navigator* training tool pilot project. This is the cornerstone

of the CIGIE Training Institute's initial venture into web-based instruction.

When fielded and integrated with CIGIE's new performance-focused training design, leading-edge Inspections and Evaluations learning, covering Inspections and Evaluations policy, procedure, and workflow, will be accessible to Offices of Inspectors General staff anywhere. It will augment and replace the current, formal, in-person classroom delivery model. Over time, CIGIE plans to develop and field similar training and performance-enhancing support systems for the investigation and audit communities.

The ICIG's interest in the project stems from the dual goals of leveraging the *I&E Navigator* tool to enhance its own on-boarding training and operations support needs, and to serve as the Intelligence Community's champion for making it available on classified networks to members of the Intelligence Community Inspectors General Forum as a service to address common needs.

During this reporting period, the Inspections Committee hosted CIGIE's Inspections and Evaluations Program Manager to provide an *I&E Navigator* update. The presentation focused on the tool's upcoming launch in October and the accompanying "Jump Start" user familiarization training. In response to the briefing, six Intelligence Community Offices of Inspectors General (the Defense Intelligence Agency, Department of Energy, Department of Justice, Department of State, the National Reconnaissance Office, and the ICIG), will participate in a "Jump Start" pilot program in October 2019.

Projecting into the next reporting period, the ICIG has requested access to *I&E Navigator* for its team that is exploring options for a new inspectors and evaluators on-boarding training program that is intended to blend CIGIE Blue Book standards and ICIG-specific processes and procedures required for oversight activity in the Inspections and Evaluations Division. The ICIG will also consider holding an initial technical exchange meeting between counterparts from CIGIE, the ICIG, and the Office of the Intelligence Community Chief Information Officer. Outcomes of this meeting will help inform the ICIG of programmatic decisions about funding and personnel resources necessary to further explore options for making *I&E Navigator* readily accessible on computer systems most commonly used by Intelligence Community Offices of Inspectors General.

Collaboration within the Audit Community

During the reporting period, the Audit Division led multiple collaboration and outreach efforts in areas of mutual interest across the IC Audit community. The Audit Division hosted working group meetings with Offices of Inspectors General officers from the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, who are required to report on the *Implementation of the Cybersecurity Information Sharing Act of 2015 (CISA) – Section 107(b)*. The meetings were beneficial in coordinating the Offices of Inspectors Generals' individual audits, the results of which will be consolidated by the ICIG into a joint report due to Congress in December 2019. The Audit Division hosted meetings with Intelligence Community audit colleagues to share ideas regarding common challenges and audit requirements, and discuss topics for joint audits.

The Audit Division also coordinated plans for a future financial summit, designed to include speakers from across the Intelligence Community to provide insight on emerging issues and strategies to improve financial audit approaches. In addition, an ICIG auditor was assigned to assist the National Reconnaissance Office and Department of Energy Offices of Inspectors General in their joint audit of intragovernmental transfers.

In June 2019, the ICIG Audit Division sponsored an Intelligence Community Procurement Audit Summit hosted by the Central Intelligence Agency Office of Inspector General to provide insight on emerging issues and promote discussion on strategies to improve procurement audit approaches. Auditors from the ICIG, Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence

Agency (NGA), National Reconnaissance Office (NRO), and National Security Agency (NSA) attended the Summit.

The Summit's keynote speaker was the Assistant Deputy Director of National Intelligence (ADDNI) for Acquisition, who shared insights on the IC's Major Systems Acquisitions. The ADDNI for Acquisition discussed using the Intelligence Community Acquisition Model, defining capability requirements, and producing robust independent cost estimates. Information on the Intelligence Community Acquisition Score Card and Metric History for cost, schedule, and performance of Major Systems Acquisitions were also shared.

The Summit also included a panel of senior procurement officials from the CIA, NGA, and NRO who shared their agencies' challenges in managing procurements in an environment of advancing technologies, achieving quicker turnaround in procurement processes, and focusing on hiring, developing, and retaining contracting officers.

In addition, Offices of Inspectors General investigators from the CIA, NRO, and the Department of Homeland Security (DHS) each presented procurement fraud cases and discussed how auditors can look for indicators of procurement fraud and handle situations that may involve criminal activity. The presenters emphasized the importance of soft skills in eliciting information and the use of data analytics to proactively identify procurement fraud indicators.

The Summit provided opportunities for auditors to discuss challenges in conducting procurement audits and share ideas on approaches and best practices with their Intelligence Community colleagues. A list of ongoing and planned procurement audits was shared to facilitate discussion and aid in furthering the development of working relationships and cross-community collaboration.

Peer Reviews

Throughout the reporting period, the ICIG's Inspections and Evaluations Division supported their IC counterparts by participating in peer reviews. During a peer review, an interagency team of peer inspectors assesses whether an OIG Inspections and Evaluations Division's projects and reports complied with CIGIE's *Quality Standards for Inspection and Evaluation* (Blue Book), and the organization's associated internal policies and procedures. Such reviews provide a level of objectivity and independence in making these determinations. The team issues a final peer review report to the reviewed organization and to CIGIE. The reviewed organization may provide copies of the final report to the head of its agency and appropriate congressional oversight bodies. The organization stands to benefit from constructive feedback and/or validation of its work products and processes. In addition, review team members gain exposure to different approaches to conducting Inspections and Evaluations work that they can share with their organizations.

The ICIG's Inspections and Evaluations Division maintains the peer review schedule for the ICIG, NSA, CIA, DIA, NGA, and the NRO inspection programs. The composition of a typical four-person peer review team is flexible, and IC teams tend to be composed of inspectors from multiple OIGs. Qualified inspectors from any OIG inspection program may serve on an IC peer review team as long as they meet the security clearance requirements of the organization to be reviewed. The Inspections and Evaluations Division provides CIGIE with an updated IC peer review schedule every six to twelve months or as events dictate.

During the reporting period, an Inspections and Evaluations Division inspector collaborated with an interagency team from CIA, DIA, and NSA to conduct an external peer review of NRO's Office of Inspector General, Inspections Program. The results of the peer review will be reported in a future NRO Office of Inspector General Semiannual Report.

Government Auditing Standards require audit organizations performing audits in accordance with generally accepted government auditing standards to have an independent, external peer review at least once every three years. The ICIG's Audit Division will undergo an external peer review in Fiscal Year 2020.

INTELLIGENCE COMMUNITY INSPECTORS GENERAL FORUM

One of the most significant ways the Office of the Inspector General of the Intelligence Community works to improve the integration of the Intelligence Community is through the Intelligence Community Inspectors General Forum (the Forum). By statute, the Forum consists of the twelve statutory or administrative Inspectors General with oversight responsibility for an element of the IC. The Inspector General of the Intelligence Community is the Chair of the Forum.

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 Intelligence Community Inspectors General Forum met twice during the reporting period. The first meeting, held in June 2019, included a review of the Fiscal Year 2020 projects under consideration for each of the elements. In addition to individual audits and inspections, the Inspectors General discussed mutual areas of concern that could be potential topics for joint and concurrent projects. The session also included a dialogue on Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*, followed by an exchange on how Inspectors General respond to requests for information from law enforcement.

The Forum met again in September to continue its discussion of PPD-19 as its requirements relate to the Council of the Inspectors General on Integrity and Efficiency. The group also received an update on Security Clearance Reform by senior officials from the National Counterintelligence and Security Center and Office of Personnel Management. The Forum will reconvene in December 2019.

Forum Committee Updates

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. Summaries of the Forum committees held during the reporting period are provided below.

Audit Committee

In May 2019, the Audit Division hosted the Audit Committee and Cybersecurity Subcommittee quarterly meeting to discuss multiple topics of community interest. The meeting included a guest speaker from CIA's Office of Inspector General who provided a demonstration on the features of TeamMate+ audit software. TeamMate, the audit software used by the majority of Intelligence Community audit divisions to document audit evidence, is moving to a new web-based version of the software. The version currently utilized by most Offices of Inspectors General will no longer be supported. The demonstration provided visualization of the new web-based version and highlighted both improvements to and losses of functionality.

The Committee brought the OIG Community together to discuss updated web-based audit software used across the IC.

The quarterly meeting also featured a speaker from the Department of State Office of Inspector General, who presented the unique challenges in conducting that agency's *Federal Information Security Modernization Act* (FISMA) evaluation, and a speaker from NRO's Office of Inspector General, who shared lessons learned in using a contractor to conduct NRO's annual FISMA evaluation. Both speakers discussed the advantages and challenges of using contractors to perform the FISMA evaluation, as well as key requirements to include in formulating a statement of work.

In August 2019, the Audit Division hosted the Audit Committee quarterly meeting that featured the Director and Deputy Director of the Defense Contract Audit Agency (DCAA) - Field Detachment as guest speakers. A joint presentation with the Forum's Investigations Committee featured guest speakers from the DCAA. The presentation covered topics of collaborative investigative efforts by both auditors and investigators to identify procurement fraud and current trends and issues, particularly searching for and identifying suspected irregularities in audits and investigations. The presentation also outlined and exhibited key attributes of a collaborative effort and the benefits of sharing information and proactive joint fraud projects. The meeting also featured the Deputy Chief, DCAA Investigative Support Division, who provided an overview of the Division and explained the auditor's role in the investigative process and the types of investigations the Division supports.

In addition, the meeting included a guest speaker from the Department of Transportation Office of Inspector General, who delivered a presentation on the

Audit Committee

Department of Transportation's recent selection of a new automated audit software package. As noted above, the audit software package used by a majority of the IC elements, TeamMate, is moving to a web-based version, which will require most IC elements to prepare for a significant transition or undergo the selection of another vendor's package for automated audit software. The presentation was helpful in sharing the challenges and timeline involved in the software selection process, as well as the key factors involved in making the final software selection.

The Audit and Investigations Committees hosted a joint meeting with the Department of Defense to identify ways in which elements can work together to detect procurement fraud.

Counsels Committee

The Counsels Committee meets regularly to discuss issues of common interest to the IC, and to promote the consistent interpretation of laws, policies, and Executive Orders. The Counsels 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 discussed and, when appropriate, collaborated on key initiatives, including the following:

The Counsels participated in a joint quarterly meeting with the Investigations Committee, in which the topic of discussion was Intelligence Community Directive (ICD) 701, *Unauthorized Disclosures of Classified National Security Information.* Questions regarding processes, procedures, and implementation challenges were discussed with relevant stakeholders from across the IC Offices of Inspectors General community, as well as representatives from ODNI's National Counterintelligence and Security Center and ODNI's Policy and Strategy Division.

The Counsels Committee led a discussion to advance the initiative to revise and enhance the standards for handling External Review Panel (ERP) requests pursuant to Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*, Section C.

In addition, the ICIG Counsels led a teleconference to discuss the standards for handling External Review Panel (ERP) requests pursuant to Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*, Section C.

The ICIG Counsels also led a discussion of the language contained in S. 1589 and H.R. 3494, the draft *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020.* The Counsels' discussion focused on the legislative provisions related to enhancing protections for whistleblowers and efforts to increase information sharing amongst the ICIG Forum.

Counsels Committee

The Counsels most recently met and discussed the ongoing Government Accountability Office (GAO) review of whistleblower protections in the Intelligence Community. GAO's review covers whistleblower matters within the IC, including whistleblower reprisal investigations and senior leader misconduct investigations conducted by the ICIG, CIA Inspector General (IG), DIA IG, NGA IG, NRO IG, and NSA IG. During this reporting period, the IC IGs continued to engage with the GAO in furtherance of the review. The ICIG Counsel's office hosted the GAO exit conference with the Intelligence Community IGs to review the draft *Statement of Facts, Intelligence Community Whistleblower Programs*, GAO Engagement Code 102577. Stakeholders participated in a discussion and collaborative review and later submitted comments and edits to the GAO.

The Committee focused on the legislative provisions related to the draft *Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*.

Inspections and Evaluations Committee

During the third quarter Inspections Committee meeting, the Intelligence Oversight working group shared with the Inspections Committee the final results of their research on the merits of conducting an inspection of intelligence oversight, a very broad topic. Working group members consisted of inspectors from the Offices of Inspectors General of the Intelligence Community, CIA, DIA, Department of Energy, Department of Homeland Security, NGA, NRO, and NSA. The working group reached consensus regarding a proposed way ahead and narrowed the scope to intelligence information sharing. The working group's recommended approach is to conduct a joint intelligence oversight evaluation of the Director of National Intelligence's implementation of intelligence information sharing responsibilities and authorities as prescribed in the *Intelligence Reform and Terrorism Prevention Act of 2004*, and Executive Order 12333.

For the final session of Fiscal Year 2019, Inspections Committee members discussed their Fiscal Year 2020 work planning, as well as common challenges and projects that could be conducted jointly or concurrently. The Inspections and Evaluations Division team leads briefed the Committee on each of the ongoing projects in the Division.

The Inspections and Evaluations Committee addressed an opportunity for conducting a joint intelligence oversight evaluation across the Intelligence Community.

The Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) Training Institute Inspections and Evaluations Program Manager updated attendees on the *I&E Navigator*, the CIGIE Training Institute's initial venture into web-based instruction. When fielded and integrated with the Training Institute's new performance-focused training design, leading-edge Inspections and Evaluations learning will be available to Offices of Inspectors General staff anywhere. During the meeting, CIGIE extended an invitation to Committee members to participate in the *I&E Navigator* Jump Start training pilot program in October 2019.

In addition, the Deputy Augmenting Intelligence using Machines (AIM) Champion for the Office of the Director of National Intelligence shared the Intelligence Community's vision for artificial intelligence and machine learning. AIM is based on a progression of capabilities. The Deputy Champion described the Intelligence Community's Strategic Objectives, Mission Initiatives, Foundational Initiatives, and the AIM operating model.

Inspections and Evaluations Committee

The idea of a sharable Inspections Committee product first surfaced as an outcome of a joint effort between two Committee members to present "lessons learned" in conducting projects on controlled access programs (or other activities with special controls). Attendee response to the material was very positive, with several members asking how they could obtain copies of the briefing. This level of interest prompted initial work – as other mission requirements permitted – to develop a tri-fold pamphlet by which the Committee can disseminate these collaboratively developed tradecraft tips.

Renewed interest in some form of "sharable package" came in the spring of 2019 as the ICIG developed a list of nominations for learning/training resources relevant to CIGIE's *I&E Navigator* framework. With that in mind, the ICIG advanced development of the pamphlet from conceptual mock-up to a print-ready coordination draft state. The draft pamphlet was circulated to Committee members in late September 2019 for review and comment. With those comments, the ICIG plans to present the pamphlet to the wider Intelligence Community Inspectors General Forum for comment prior to publication and initial dissemination.

The Deputy Augmenting Intelligence using Machines (AIM) Champion for the Office of the Director of National Intelligence briefed the Committee on the IC's vision for artificial intelligence and machine learning.

Investigations Committee

The Intelligence Community Inspectors General Forum's Investigations Committee met twice during this reporting period. In May 2019, the Investigations Committee held discussions regarding Intelligence Community Directive (ICD) 701, *Unauthorized Disclosure of Classified Information*. The meeting included representatives from Intelligence Community elements and ODNI's Policy and Strategy Division. Discussions primarily focused on understanding media leaks versus all unauthorized disclosures of classified information. Other matters discussed included notification requirements to the ICIG and to the respective agency Offices of Inspectors General. Leadership from ODNI's Policy and Strategy Division also discussed contents of the Directive to enhance the understanding of the notification thresholds and timelines. The Committee also disseminated ICD 701 resources, including Fact Sheets, a list of Frequently Asked Questions, and internal workflow graphics. In addition, the Committee continued discussions focusing on increasing collaborative investigations and identifying de-confliction strategies in the case of overlapping areas of responsibility.

Later in the reporting period, the Investigations Committee held a joint meeting with the Forum's Audit Committee that featured a presentation by guest speakers from the Defense Contract Audit Agency. The presentation covered topics of collaborative investigative efforts by both auditors and investigators to identify procurement fraud, as well as current trends and issues, particularly searching for and identifying suspected irregularities in audits and investigations. The presentation also outlined and exhibited key attributes of a collaborative effort and the benefits of sharing information and conducting proactive joint fraud projects.

The Investigations Committee focused on collaborative investigations and identifying de-confliction strategies in the case of overlapping areas of responsibility.

Management and Administration Committee

During this reporting period, the Management and Administration Committee continued its efforts to strengthen cross-Intelligence Community collaboration through engagement on the following topics: employee recruitment through shared web-based resume portals, approaches to employee recognition, strategies to improve employee retention, and best practices for records management and retention. The Committee also continued engagement on the topic of workforce training and development, with a representative from CIGIE's Training Institute leading a discussion on training resources and opportunities available through its Training Academies. The group considered the challenges associated with the majority of CIGIE's training being delivered in the classroom setting, and the requirement to expand course offerings to address the needs of those in mission support discipline areas through both classroom and virtual offerings.

The Management and Administration Committee highlighted recruitment challenges across the Intelligence Community and discussed a more streamlined employment application process.

Continuing efforts to address recruitment challenges from an IC-wide perspective, the Committee welcomed a representative from the Office of the Director of National Intelligence's Human Resources Division to present an overview of the new Intelligence Community Applicant Gateway tool. The Applicant Gateway was created to be a shared, consolidated Intelligence Community job application platform to attract applicants, enable job exploration across the IC, and facilitate a streamlined application process. ODNI, NSA, and NGA are current users, with DIA and DHS scheduled to adopt the tool in the near future. The aspect of the tool the Committee found most beneficial is the ability for applicants to share their resumes with all participating IC agencies in which they have an interest through a streamlined process, and for agencies to directly source applicants based on specific skillsets or needs.

The Committee discussed successes and the contributing factors thereto, when recruiting for most IG discipline areas, and shared lessons learned to overcome the challenges associated with recruiting auditors and other difficult-to-fill positions. Members shared the types of incentives employed at their respective agencies to aid recruitment and retention efforts, including global mobility, team assignment mobility, internal rotational opportunities that allow for employee portfolio diversification; and recruiting more junior level persons through the USAJobs

Management and Administration Committee

Pathways Program and the Wounded Warrior Program. All members continued to cite the lengthy security clearance process as a notable factor contributing to recruitment challenges, as well as an impediment to allowing interested employees to take advantage of joint duty opportunities.

The Information Technology (IT) Subcommittee falls under the purview of the Management and Administration Committee. Federal agencies will be required to transition business processes and recordkeeping to a fully electronic environment by 2022, as outlined in the Office of Management and Budget/National Archives and Records Administration's (NARA) Memorandum (M-19-21). In preparation for that transition, the Information Technology Subcommittee invited representatives from NARA, NRO, and the Information Management Services Office to lead a discussion on updates to regulations, and provide guidance on how to effectively transition to fully electronic recordkeeping, including a review of electronic storage systems, proper formatting, and metadata requirements. The group discussed current tools that are available to assist with transition by automating data collection and digitizing hard copy documents in the proper format for retrieval. The IT Subcommittee also discussed establishment of a common virtual environment to support cross-IC Inspector General projects, how that might be accomplished, the best IT platform on which to host such an effort, and the current practices at each agency.

The Information Technology Subcommittee examined electronic business procedures and recordkeeping tools available to meet requirements established by the Office of Management and Budget and the National Archives and Records Administration.

Whistleblower Committee

The Forum's Whistleblower Committee met in September and included representatives from the CIA, DIA, NRO, NGA, Department of Defense, Department of Justice, and other federal agencies. The Committee discussed many whistleblower issues of common interest to the members, including proposed legislation relevant to the entities' shared mission, effective report writing for administrative investigations, and proposed training topics for IG investigators conducting whistleblower reprisal investigations. Committee members were particularly interested in the possibility of having the ICIG provide training about best practices in whistleblower reprisal investigations, and evaluating protected disclosures and personnel actions consistent with Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*, 50 U.S.C. § 3341, and 5 U.S.C. § 2302(b)(8). The Committee also discussed requests for External Review Panels under PPD-19, Section C, how those requests are processed by the ICIG, and trends in requests filed with the ICIG. Finally, the group discussed the important role of the Whistleblowing Protection Coordinator in their respective Offices of Inspectors General and how to best use that position to further the mission of their offices.

The Whistleblower Committee collaborated with Intelligence Committee elements to enhance information sharing related to whistleblower investigations, evaluating protected disclosures, and External Review Panels.

Intelligence Community Data Analytics Community of Interest Working Group

The Office of the Inspector General of the Intelligence Community hosted the fourth session of the Intelligence Community Data Analytics Community of Interest Working Group. The Working Group meets quarterly and includes members of the Intelligence Community Inspectors General Forum. The Working Group was established to explore and share ideas on data collection and analysis, enhance insights into trends and risks, and improve operations to identify potential waste, fraud, and abuse. Representatives from DIA, NGA, NSA, NRO, the Department of Justice, and the ICIG attended and discussed the Office of the Director of National Intelligence's initiative on Augmenting Intelligence using Machines (AIM).

Representatives from ODNI's AIM team provided an overview of the AIM initiative. The AIM initiative seeks to use cognitive technologies, particularly artificial intelligence (AI), to enable the Intelligence Community to fundamentally change the way it produces intelligence. The ICIG has identified the improved oversight of AI as one of its primary programmatic objectives. The ICIG extended the offer to ODNI's AIM team to make their presentation to the Working Group as part of the ICIG's ongoing efforts to bring together thought leaders on AI and related oversight challenges.

The Intelligence Community Data Analytics Community of Interest Working Group continued to explore Augmenting Intelligence using Machines (AIM) and data collection and analysis when identifying potential waste, fraud, and abuse in the federal government.

Community-Wide Outreach Activities

During the reporting period, consistent with its objective of working to improve integration of the Intelligence Community, the ICIG joined with other oversight authorities and mission operators to conduct 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-government organizations.

Security Clearance Processing

At the annual coordination meeting between the U.S. Government Accountability Office and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Inspector General Atkinson discussed the current challenges related to security clearance processing and the contributions various Offices of Inspectors Generals (OIGs) are making to improve the efficiency and effectiveness of the process. As the Security Executive Agent for the Executive Branch, the Director of National Intelligence has government-wide responsibility to develop, implement, and oversee effective, efficient, and uniform policies and procedures for conducting security clearances and sensitive national security position investigations and adjudications. Last year, the Office of the Director of National Intelligence announced the implementation of a new initiative entitled *Trusted Workforce 2.0*, which "convene[d] leaders in government and the private sector 'to identify and establish a new set of policy standards that will transform the U.S. government's approach to vetting its workforce, overhaul the enterprise business processes, and modernize information technology.'"

Inspector General Atkinson identified numerous ways OIGs can improve the security clearance process across the federal government, including by closing recommendations in a timely manner following audits, inspections, and other projects related to the security clearance process; ensuring their agencies are collecting required security clearance data and responding to calls to submit said data; and by testing the reliability of the above-mentioned data.

Investigations

The Investigations Division's outreach efforts for this reporting period consisted of collaborative meetings with members of the Army Criminal Investigation Command, Major Procurement Fraud Unit, and Defense Criminal Investigative Service, Northern Virginia Resident Agency, to discuss potential joint proactive and reactive investigations and information sharing.

The Center for Protected Disclosures

Throughout the reporting period, leadership from the Center for Protected Disclosures participated in multiple Whistleblower Reprisal Investigator courses sponsored by the Department of Defense's Office of the Inspector General. The presentations offered opportunities to share interview techniques and provide an overview of the ICIG Center for Protected Disclosures.

National Whistleblower Appreciation Day

The Office of the Inspector General of the Intelligence Community hosted *National Whistleblower Appreciation Day* on July 30, 2019, at the Intelligence Community Campus in Bethesda, Maryland. *National Whistleblower Appreciation Day* celebrates America's first whistleblower law, passed unanimously by the Continental Congress on July 30, 1778, and acknowledges the contributions of whistleblowers in combating waste, fraud, abuse, and violations of laws and regulations of the United States. *National Whistleblower Appreciation Day* seeks to inform employees and contractors working on behalf of the people of the United States, and members of the public, about the legal right of U.S. citizens to "blow the whistle" to the appropriate authority by honest and good faith reporting of misconduct, fraud, or abuse.

The event, which included remarks by then-Director of National Intelligence Daniel Coats, highlighted the contributions of whistleblowers throughout the United States Government, particularly the Intelligence Community, in providing the proper authorities with lawful disclosures that save U.S. taxpayers billions of dollars each year, and serving the public interest by ensuring that the United States remains an ethical and safe place. A panel discussion, moderated by Inspector General Atkinson, featured senior leaders from ODNI's Office of Civil Liberties, Privacy, and Transparency, the National Counterintelligence and Security Center, Office of General Counsel, Office of the Intelligence Community Equal Employment Opportunity and Diversity, and the Office of the Ombudsman. The panel provided attendees with information on various programs and services to get the "right information" to the "right people."

ICIG Hotline

Representatives from the ICIG's Hotline met with their Intelligence Community counterparts to discuss referral processes between elements; collaboration and engagement opportunities; solutions for processing complaints; best practices on Hotline Operations; and training and outreach events.

National Compliance Officer Day

The Office of the Inspector General of the Intelligence Community also engaged with the ODNI workforce at the 2019 National Compliance Officer Day event at ODNI Headquarters.

National Compliance Officer Day honors the contributions of those who are committed to the profession of combating waste, fraud, abuse, and violations of laws and regulations. Each year, professionals who have dedicated their careers to the fields of ethics, compliance, and responding to allegations of misconduct, are acknowledged for their contributions to upholding the law and providing an avenue to report wrongdoing.

The event highlighted the importance of reporting suspected fraud, waste, and abuse, and provided an overview of the ICIG Center for Protected Disclosures which processes whistleblower reports and supports whistleblower protections. Resource materials to advise the workforce how to contact the ICIG Hotline were made available.

RECOMMENDATIONS SUMMARY

Following publication of an inspection report, the ICIG's Inspections and Evaluations Division interacts with the inspected elements at least quarterly to ensure actions are taken to implement report recommendations. A description of the actions are entered into the ICIG's recommendations tracking database. Inspections and Evaluations leadership has the responsibility for approving the closure of a recommendation once it has been demonstrated that responsive actions have met the intent of a recommendation. The Inspections and Evaluations Division may revisit closed recommendations to ensure there is no slippage or back-tracking in their fulfillment or to inform follow-on reviews.

For the ODNI to realize the maximum benefit from ICIG audits, management should ensure that adequate corrective action is taken in a timely manner to address audit recommendations. The Audit Division closely monitors implementation of its recommendations through continuous communication with stakeholder points of contact on progress and actions. The status of open recommendations is periodically conveyed to ODNI senior managers. The Audit Division issues a formal closure of audit memorandum when it determines that all recommendations in a report have been addressed.

Report Name	Date Issued	Total Issued	New This Period	Open	Closed This Period
2019					
Audit: Office of the Director of National Intelligence's Fiscal Year 2018 Conference Spending	September	2	2	2	0
Audit: Management of Privileged Users of Office of the Director of National Intelligence Information Systems	September	9	9	9	0
Inspection: Assessment of the ODNI Methods Used to Substantiate Post-Secondary Education Claims Made by ODNI Employees Subsequent to Entry-on-Duty	August	7	7	7	0
Audit: FY 2018 Independent Evaluation of Federal Information Security Modernization Act (FISMA)	February	11	0	10	1
Inspection: Cyber Threat Intelligence Integration Center	January	9	0	7	2
2018					
Inspection: IC Freedom of Information Act (FOIA) Programs	September	10	0	4	3
Audit: Memorandum to the Chief Operating Officer re: Charge Card Program	August	2	0	1	1
Inspection: Assessment of IC Information System Deterrence, Detection, and Mitigation of Insider Threats	March	4	0	1	0
2017					
Inspection: Assessment of ODNI Information System Deterrence, Detection, and Mitigation of Insider Threats	September	19	0	1	3
2013					
Audit: Study: IC Electronic Waste Disposal Practices	May	5	0	0	1
2012					
Audit: IC Security Clearance Reciprocity	December	2	0	1	1
	Totals	**80**	**18**	**43**	**12**

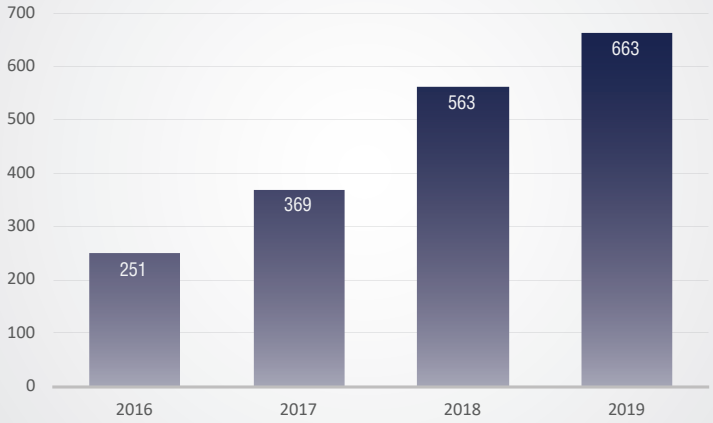
ICIG HOTLINE

ICIG HOTLINE
Report suspected fraud, waste, and abuse
Open: 855-731-3260 • www.dni.gov/ICIG
Secure: 933-2800 • https://go.ic.gov/hotline

The ICIG Hotline provides a confidential means for Intelligence Community employees, contractors, and the public to report information concerning suspected fraud, waste, and abuse of programs and activities within the responsibility and authority of the Director of National Intelligence.

The ICIG Hotline's website features three new forms that allow individuals to select the type of complaint they wish to report: "Report of Fraud, Waste, and Abuse Intake Form," "Disclosure of Urgent Concern Form," and "External Review Panel (ERP) Request Form." The Hotline can be contacted via classified and unclassified email and phone lines, U.S. mail, secure web submissions, walk-ins, and drop boxes located in select ODNI facilities.

NEW HOTLINE CONTACTS BY FISCAL YEAR



NEW CONTACTS THIS REPORTING PERIOD

366

METHODS OF CONTACT
including repeat contacts

947 Phone Calls	**15** USPS Mail	**3** Drop Boxes
9 Faxes	**1** Walk-Ins	**24** Email/Web

ABBREVIATIONS AND ACRONYMS

ADDNI ..... Assistant Deputy Director of National Intelligence
AI ..... Artificial Intelligence
AIM ..... Augmenting Intelligence using Machines
The Center ..... The Center for Protected Disclosures
CIA ..... Central Intelligence Agency
CIGIE ..... Council of Inspectors General on Integrity and Efficiency
CISA ..... Cybersecurity Information Sharing Act of 2015
CoI ..... Community of Interest
DCAA ..... Defense Contract Audit Agency
DIA ..... Defense Intelligence Agency
DHS ..... Department of Homeland Security
DNI ..... Director of National Intelligence
EO ..... Executive Order
ERP ..... External Review Panel
FBI ..... Federal Bureau of Investigation
FISMA ..... Federal Information Security Modernization Act of 2014
FOIA ..... Freedom of Information Act
The Forum ..... Intelligence Community Inspectors General Forum
FY ..... Fiscal Year
GAO ..... Government Accountability Office
HPSCI ..... House Permanent Select Committee on Intelligence
I&E ..... Inspections and Evaluations
IC ..... Intelligence Community
ICD ..... Intelligence Community Directive
ICFLP ..... Intelligence Community Foreign Language Program
ICIG ..... Inspector General of the Intelligence Community
ICWPA ..... Intelligence Community Whistleblower Protection Act
IG ..... Inspector General
INSA ..... Intelligence and National Security Alliance
IPERA ..... Improper Payments Elimination and Recovery Act
IT ..... Information Technology
NARA ..... National Archives and Records Administration
NGA ..... National Geospatial-Intelligence Agency

NRO ..... National Reconnaissance Office
NSA..... National Security Agency
ODNI..... Office of the Director of National Intelligence
OGC ..... Office of the General Counsel
OIG..... Office of the Inspector General
PPD ..... Presidential Policy Directive
SORN ..... System of Record Notices
SSCI ..... Senate Select Committee on Intelligence
U.S..... United States
U.S.C. ..... United States Code

Office of the Inspector General of the Intelligence Community

571-204-8149 open; 939-9200 secure