

---

**(U) OFFICE OF THE INSPECTOR GENERAL OF THE  
INTELLIGENCE COMMUNITY**



**(U) Annual Work Plan  
Fiscal Year 2020**

Michael K. Atkinson

Inspector General of the Intelligence Community

## (U) INSPECTOR GENERAL FOREWORD

(U) On behalf of the Office of the Inspector General of the Intelligence Community (ICIG), I am pleased to present the ICIG's Fiscal Year 2020 Work Plan. The Work Plan identifies the congressionally mandated reports that align with the ICIG's statutory requirements. The Work Plan also identifies the discretionary projects the ICIG intends to undertake to review the efficiency and effectiveness of programs or activities within the responsibility and authority of the Director of National Intelligence.

(U) To prepare for the selection of projects for Fiscal Year 2020, senior ICIG management officials held discussions with leaders across the Intelligence Community, the congressional intelligence committees, and other stakeholders to address areas that would benefit from an Inspector General review. The ICIG also discussed potential topics and joint projects with the Intelligence Community Inspectors General Forum, which consists of the twelve statutory or administrative Inspectors General with oversight responsibility for an element of the Intelligence Community.

(U) To help identify and select the projects, the ICIG also reviewed the Strategic Priorities outlined in the 2019 *National Intelligence Strategy*, the Office of the Director of National Intelligence's *IC2025 Vision and Foundational Priorities*, and the 2018 *Management and Performance Challenges for the Office of the Director of National Intelligence*. Those documents, coupled with assessments of emerging threats and topics, led to our decisions on projects we plan to pursue. The Work Plan for Fiscal Year 2020 includes, among others, projects related to Artificial Intelligence and Machine Learning, Cybersecurity, Information Security Continuous Monitoring, Management of Office of the Director of National Intelligence Service Agreements, and Security Clearance Reform.

(U) Not included in this Work Plan are potential directives issued by Congress that may be identified with the enactment of the *Intelligence Authorization Act* (IAA). Changes in the law that require the ICIG to conduct additional projects may also require the ICIG to adjust the Work Plan, and, as a result, reduce the number of discretionary projects. In addition, the ICIG may also need to revise, add, or remove discretionary projects based on unforeseen events or constraints to the ICIG's workforce due to limited personnel resources, budgets, or operational challenges.

(U) The Office of the Inspector General of the Intelligence Community looks forward to continuing our steadfast commitment to integrity, independence, diversity, and transparency.



Michael K. Atkinson  
Inspector General

**(U) Table of Contents**

**(U) INSPECTOR GENERAL FOREWORD..... 1**

**(U) INTRODUCTION ..... 3**

**(U) AUTHORITY ..... 3**

**(U) MISSION ..... 3**

**(U) ICIG STRATEGIC GOAL ..... 3**

**(U) ICIG CORE VALUES..... 3**

**(U) FISCAL YEAR 2020 PLANNED PROJECT DESCRIPTIONS..... 4**

**1. (U) REQUIRED PROJECTS..... 4**

**2. (U) DISCRETIONARY PROJECTS ..... 5**

**(U) FISCAL YEAR 2020 PEER REVIEWS ..... 9**

**(U) APPENDIX A: THE AUDIT PROCESS ..... 10**

**(U) APPENDIX B: THE INSPECTIONS AND EVALUATIONS PROCESS ..... 12**

**(U) APPENDIX C: THE INVESTIGATIONS PROCESS ..... 13**

**(U) APPENDIX D: THE CENTER FOR PROTECTED DISCLOSURES ..... 15**

**(U) APPENDIX E: ACRONYM LIST ..... 17**

## **(U) INTRODUCTION**

### **(U) AUTHORITY**

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

### **(U) MISSION**

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

### **(U) ICIG STRATEGIC GOAL**

(U) 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.

### **(U) ICIG CORE VALUES**

**INTEGRITY**  
**INDEPENDENCE**  
**COMMITMENT**  
**DIVERSITY**  
**TRANSPARENCY**

## **(U) FISCAL YEAR 2020 PLANNED PROJECT DESCRIPTIONS**

### **1. (U) REQUIRED PROJECTS**

#### **(U) Fiscal Year 2020 Risk Assessment of the Office of the Director of National Intelligence's Government Charge Card Program**

(U) *The Government Charge Card Abuse Prevention Act* requires inspectors general to conduct periodic risk assessments of agency charge card programs to analyze the risk of illegal, improper, or erroneous purchases. The assessment will examine the ODNI's implementation of the internal control requirements set forth in the *Government Charge Card Abuse Prevention Act* and Office of Management and Budget guidance.

#### **(U) Fiscal Year 2020 Independent Evaluation of the Office of the Director of National Intelligence's Information Security Program and Practices Required by the *Federal Information Security Modernization Act of 2014***

(U) *The Federal Information Security Modernization Act* prescribes an annual process of self-assessment and independent evaluation of federal agencies' information security programs and practices. The ICIG will perform the independent evaluation of the ODNI's information security program and practices. The evaluation will assess whether the ODNI's information security policies, procedures, and practices are effective in protecting information and whether the ODNI complied with applicable laws and regulations.

#### **(U) Management Challenges Facing the Office of the Director of National Intelligence**

(U) *The Reports Consolidation Act of 2000* requires the ICIG to identify the most serious management and performance challenges facing the ODNI. The ICIG provides its findings to the Director of National Intelligence for inclusion in the Fiscal Year 2020 Agency Financial Report.

#### **(U) Review of the Office of the Director of National Intelligence's *Compliance with the Improper Payments Elimination and Recovery Act of 2010***

(U) *The Improper Payments Elimination and Recovery Act (IPERA)* requires each federal agency to perform a review of programs and activities to assess whether the risk of improper payment is significant. Each Inspector General is required to assess and submit a report on whether the agency complied with IPERA. This project will evaluate the completeness, accuracy, and validity of the ODNI's disclosures on improper payments as reported in the FY 2019 Agency Financial Report.

## 2. (U) DISCRETIONARY PROJECTS<sup>1</sup>

### **(U) Building Capacity and Expertise for Oversight of the Augmenting Intelligence Using Machines Initiative**

(U) The ICIG's *Semiannual Report October 2018 - March 2019* named "Improving Oversight of Artificial Intelligence" as a programmatic objective for future work. The report noted that Intelligence Community Offices of Inspectors General, individually or collectively, may lack the people, tools, and focus needed to effectively evaluate the vulnerabilities and operation of cognitive technologies. The ICIG will conduct a range of activities intended to build intelligence oversight capacity and expertise related to the Intelligence Community's Augmenting Intelligence using Machines (AIM) Initiative, which intends to synchronize and enable the development and rapid adoption of artificial intelligence, automation, and augmentation technologies.

### **(U) Cybersecurity Intelligence Sharing with Industry**

(U) According to a number of studies, even though a cybersecurity partnership is beneficial for both the U.S. government and the private sector, some private companies are reluctant to establish partnerships with the government. Among the key concerns are issues of trust, control, and disclosure. The ICIG will examine the challenges and impediments to sharing cybersecurity intelligence with industry.

### **(U) Examination of the Efficiency and Effectiveness of Intelligence Community Directive 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community***

(U) Efficient and effective intelligence information sharing – discovery, access, and use of information – remains an important Intelligence Community priority to achieve intelligence integration, the principal mission of the ODNI. On January 21, 2009, the ODNI issued Intelligence Community Directive (ICD) 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, as the primary Intelligence Community policy to address the Director of National Intelligence information sharing mandates contained in the *Intelligence Reform and Terrorism Prevention Act* as well as Executive Order 12333, *United States Intelligence Activities*. The ICIG and the Department of Defense Office of Inspector General will examine the efficiency and effectiveness of ICD 501 and other applicable ODNI policy or guidance implementing intelligence information sharing.

---

<sup>1</sup> (U) The list of discretionary projects is not in order of priority or intended sequence.

**(U) Implementation of Intelligence Community Directive 701, *Unauthorized Disclosures of Classified National Security Information***

(U) The unauthorized disclosure of classified information threatens to cause potentially long-lasting and irreversible harm to our nation's ability to identify and respond to the many threats that face our nation. The revision to Intelligence Community Directive (ICD) 701, *Unauthorized Disclosures of Classified National Security Information*, was issued in December 2017. The revised policy redirected some responsibilities, clarified others, and created additional ones for a comprehensive approach to manage unauthorized disclosures across the Intelligence Community. The ICIG will conduct a review of the Intelligence Community's implementation of ICD 701. The purpose of this evaluation is to assess the efficiency and effectiveness of the revised policy, including execution of the revised roles and responsibilities pursuant to the Directive.

**(U) Information Security Continuous Monitoring Projects****(U) Implementation of the Office of the Director of National Intelligence's Information Security Continuous Monitoring Program**

(U) Continuous monitoring is a risk management approach to cybersecurity that maintains an accurate picture of an agency's security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status. In today's environment of widespread cyber-intrusions, advanced persistent threats, and insider threats, it is essential for agencies to have real-time accurate knowledge of their enterprise IT security posture to respond swiftly and effectively to external and internal threats. This audit will determine the reasons why the ODNI has not consistently implemented an Information Security Continuous Monitoring (ISCM) program.

**(U) Joint Project on Intelligence Community Elements' Implementation of Information Security Continuous Monitoring Programs**

(U) This project will report the consolidated results of separate audits conducted by the Offices of Inspectors General of six Intelligence Community elements – National Reconnaissance Office, National Geospatial-Intelligence Agency, National Security Agency, Defense Intelligence Agency, Central Intelligence Agency, and the Office of Director of National Intelligence – of their element's implementation of an ISCM program. Specifically, the capstone report will identify the reasons why the six Intelligence Community elements remain at a low maturity level for implementing continuous monitoring.

**(U) Security Clearance Reform****(U) Integrity of Security Clearance Data Reporting**

(U) The Director of National Intelligence, as the Security Executive Agent under Executive Order 13467, is responsible for assuring the quality, timeliness, consistency, and integrity of national security vetting practices. Data concerning security clearance processing timeliness are used to inform decisions made by the Security Executive Agent and Congress and are considered integral to overseeing the effectiveness of the security clearance process and reducing the security clearance backlog. The ICIG will assess the ability of the Intelligence Community elements and Security Executive Agent to accurately capture, document, and report required security clearance processing timeliness information and whether the Intelligence Community elements calculate processing timeliness in a consistent manner. The audit will also determine whether the Security Executive Agent accurately compiles and reports data provided by the Intelligence Community elements, as required, and uses timeliness data to address the security clearance backlog and inform security clearance-related policy decisions.

**(U) Intelligence Community Implementation of Security Clearance Reciprocity**

(U) The Director of National Intelligence, as the Security Executive Agent under Executive Order 13467, is responsible for ensuring reciprocal recognition of eligibility for access to classified information among Executive Branch agencies. This review will determine whether Intelligence Community agencies are complying with recent Director of National Intelligence reciprocity guidance.

**(U) Intelligence Community Advanced Campaign Cell**

(U) The Intelligence Community Advanced Campaign Cell was established by the Principal Deputy Director of National Intelligence in 2014 with several participating IC elements. Its mission is to develop and apply innovative analytic and collection methods, technology, and tradecraft techniques integrating multiple intelligence disciplines against the hardest problems facing the Intelligence Community. Together with the National Security Agency's Office of Inspector General, the ICIG will participate in a joint review of management and intelligence oversight at the Intelligence Community Advanced Campaign Cell.

**(U) Intelligence Advanced Research Projects Activity Contracting**

(U) Charged with providing research and technical capabilities for the Intelligence Community, the Intelligence Advanced Research Projects Activity (IARPA) invests in high-risk/high payoff research programs. This project will assess whether the ODNI administers contracts for IARPA in accordance with applicable regulations. The project will also address the management and oversight of IARPA's contractors.

**(U) The Office of the Director of National Intelligence's Management of Service Agreements**

(U) The ODNI leverages a number of service agreements with other Intelligence Community elements through which the ODNI obtains counterintelligence, security, and information technology services, among others. This project will assess the ODNI's oversight of service agreements to determine whether the ODNI is receiving the level of service for which it is paying.

## **(U) FISCAL YEAR 2020 PEER REVIEWS**

### **(U) Audit**

(U) *Generally Accepted Government Auditing Standards* (GAGAS) requires audit organizations that conduct projects in accordance with GAGAS to obtain an external peer review conducted by reviewers independent of the audit organization being reviewed. The peer review provides a basis to determine if the reviewed audit organization's system of quality control is suitably designed, and whether it complies with its quality control system. This provides reasonable assurance that it conforms to professional standards and applicable legal and regulatory requirements in all material respects.

(U) The ICIG and the Offices of Inspectors General at the Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency conduct peer reviews of each other's audit divisions once every three fiscal years on a pre-determined schedule. The Inspector General of the Intelligence Community Audit Division was externally peer reviewed in Fiscal Year 2017; the next external peer review of the Inspector General of the Intelligence Community is scheduled for Fiscal Year 2020. The external peer review schedule has been coordinated with the other Intelligence Community Offices of Inspectors General.

### **(U) Inspections and Evaluations**

(U) As adopted and approved by the majority of the Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) members, Offices of Inspectors General (OIG) with an Inspections and Evaluations organization that conduct inspections and evaluations in accordance with the *CIGIE Quality Standards for Inspection and Evaluation* (Blue Book) must undergo an external peer review every three years. The CIGIE external peer review program is designed to assure Offices of Inspectors General and their stakeholders of the Inspections & Evaluations organization's compliance with Blue Book standards. External peer reviews provide a level of objectivity and independence in making this determination.

(U) The ICIG's Inspections and Evaluations Division is scheduled to be peer reviewed in June 2020. Previous peer reviews of Inspections & Evaluations occurred in 2014 and 2017. In advance of the peer review, Inspections & Evaluations completed an update of the ICIG's Inspections Manual to ensure that it aligns with current Division practices and procedures as well as the *CIGIE Quality Standards for Inspection and Evaluation*.

(U) In 2020, the Inspections and Evaluations Division will support Inspectors General peer reviews of the Central Intelligence Agency's Inspections program, the National Geospatial-Intelligence Agency's Inspections program, and the Defense Intelligence Agency's Inspections program.

(U) The Inspector General of the Intelligence Community Assistant Inspector General for Inspections and Evaluations, as Chair of the Intelligence Community Inspectors General's Inspections Committee, will continue to serve as the peer review schedule coordinator for the Intelligence Community Offices of Inspectors General inspection programs and provide schedule updates to the CIGIE Inspections and Evaluations Committee.

## (U) APPENDIX A: THE AUDIT PROCESS

(U) The ICIG's Audit Division evaluates whether the goals and objectives of the Office of the Director of National Intelligence (ODNI) and Intelligence Community element programs are achieved; resources are used efficiently, and the programs and activities are conducted in accordance with applicable laws, regulations, and good business practices. Audits and projects may be financial or performance in nature. Audits are conducted in accordance with the generally accepted government auditing standards, as well as the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency. The audit process involves the following stages:

(U) Announcement of Audit. The Inspector General of the Intelligence Community sends a formal memorandum to the management of the organization(s) being audited or reviewed. The announcement memorandum includes the audit objectives, the start date, and a request for a point of contact.

(U) Entrance Conference. At the beginning of each audit or project, the Inspector General of the Intelligence Community team holds an entrance conference with the management organizations being audited or reviewed. The team discusses the objectives, scope, and timing; makes specific arrangements for access to records, information, and personnel; and makes plans for Inspector General of the Intelligence Community's workspace (if applicable) and access to relevant information systems. The team also discusses management's preferences for the frequency of status updates (e.g., monthly, bi-monthly, or as developments warrant).

(U) Fieldwork. An audit or project can be conducted at domestic and/or overseas locations. During the fieldwork stage, the Inspector General of the Intelligence Community's team gathers information to fully understand the entity's operations, activities, and internal controls. The information obtained may include but is not limited to, relevant laws and regulations, prior Inspector General reports, organization charts, budget data, mission statements, system data, and policies and procedures. The team interviews personnel to understand more about the organization or activity under review, performs analysis on data and information provided, and documents conclusions.

(U) Exit Conference. The team holds an exit conference to formally advise management of the results and obtain management comments on tentative findings and recommendations. At the meeting or shortly thereafter, a preliminary draft report is provided to management to ensure all relevant information was considered in the development of the findings and that information in the report is accurate. Management input is vital prior to the issuance of the draft report to ensure issues and conditions are fairly reported, any factual errors are corrected, and disagreements are resolved.

(U) Report. The ICIG's team issues a report for management's review. Management is asked to provide comments and state whether they agree with the report's recommendations within 30 days from the issuance of a draft report. Management comments on the draft report are considered in preparing the final report. The final report is issued to appropriate ODNI and/or Intelligence Community element managers. Highlights of each final report are included in the ICIG's next Semiannual Report to the Director of National Intelligence and Congress. Within 60 days of the

issuance of the final report, management must provide a report to the Audit Division Assistant Inspector General explaining the actions taken to implement the recommendations and providing a timetable for recommendations that will require longer than 60 days to implement.

(U) Audit Follow-up. For the ODNI and the Intelligence Community to realize the maximum benefit from Inspector General of the Intelligence Community audits and projects, management should ensure that adequate corrective action is taken in a timely manner on the recommendations in the report. The Inspector General of the Intelligence Community's Audit Division Assistant Inspector General closely monitors implementation of recommendations and welcomes continuing communication from management on progress and actions. The status of open recommendations is periodically conveyed to ODNI senior managers and other stakeholder points of contact. Recommendations are reported in the semiannual report to the Director of National Intelligence and Congress. The Inspector General of the Intelligence Community's Audit Division Assistant Inspector General issues a closure memorandum when he or she determines that all recommendations in a report have been addressed.

(U) For additional information about the Audit process, please visit our website at [www.dni.gov/ICIG](http://www.dni.gov/ICIG).

## (U) APPENDIX B: THE INSPECTIONS AND EVALUATIONS PROCESS

(U) The ICIG's Inspections and Evaluations Division conducts inspections, evaluations, and reviews to assist the Office of the Director of National Intelligence (ODNI) and Intelligence Community elements in improving their efficiency, effectiveness, and processes, as well as to build capacity. A variety of criteria are used as performance measures, including applicable laws, regulations, directives, and best practices. Inspections, evaluations, and reviews are conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency. The Inspections and Evaluations process involves the following stages:

(U) Planning. Inspection topics may be selected from a variety of sources, including: Executive Department Direction, Congressionally Directed Actions, ODNI leadership requests, and Inspector General of the Intelligence Community internally generated ODNI Component Inspections.

(U) The ICIG's annual work planning process prioritizes inspections, evaluations, and reviews. Once topics are selected, team leads and members are assigned and preliminary research begins. Team meetings are held to scope the inspection and set objectives. All members sign *Statements of Independence*, which identify any conflicts of interest, and Division leadership determines if any conflict mitigation methods are required.

(U) The ICIG sends a formal memorandum announcing the inspection, evaluation, or review. This memorandum is sent to the organizations involved or, depending on the topic, may be sent IC-wide. The announcement memorandum includes the objectives, start date, and request for a point of contact.

(U) Execution. The Execution Phase begins when the team issues a Data Call requesting a variety of documents and data from the participating organizations. A workforce questionnaire may be issued and results evaluated. Interviews of organizational leaders, employees, contractors, and other appropriate personnel are conducted, documented, and analyzed to support the development of Findings. Themes are developed, de-conflicted, and sourced, after which a list of Draft Findings and Recommendations is created.

(U) Reporting. Findings and Recommendations are finalized at the beginning of the Reporting Phase, and an In-Progress Review (IPR) is presented to the Inspector General of the Intelligence Community's leadership and the participating organizations. Following the IPRs, a draft report is written and issued for ICIG internal coordination, after which comments from participating organizations are solicited. After adjudicating all internal Inspector General of the Intelligence Community and participating organization comments, a final report is issued that may include subject organizational comments. Recommendations are tracked to closure. The team conducts a lessons learned session to document issues or opportunities for Inspections & Evaluations process improvement.

(U) For additional information about the inspection, evaluation, or review process, please visit our website at [www.dni.gov/ICIG](http://www.dni.gov/ICIG).

## (U) APPENDIX C: THE INVESTIGATIONS PROCESS

(U) The ICIG's Investigations Division is the principal agent for investigating potential violations of federal law or agency regulations. The Investigations Division conducts or participates in independent and objective criminal and administrative investigations pertaining to programs and activities within the Director of National Intelligence's responsibility and authority. Consistent with the ICIG's unique statutory authority, the Investigations Division coordinates cross-Intelligence Community criminal and administrative investigations. The Investigations Division fulfills the ICIG's statutory obligations by conducting investigations that detect and deter fraud and abuse in such programs and activities. In addition, investigations can provide senior managers with actionable information on critical issues that aid in their decision-making.

(U) Although investigations may be proactive, based on planned initiatives using data analytics, many investigations are reactive and initiated in response to information and allegations received by the Investigations Division. Due to the combination of unpredictability and the need to protect sources and methods of proactive investigations, the Investigations Division does not identify its planned investigations in the Annual Work Plan. However, because investigations often result from a deliberate subversion of the Office of the Director of National Intelligence's (ODNI's) procedures or controls, the details obtained from investigations may result in referrals to other ICIG Divisions and become integral to planning audits, inspections, and special projects.

(U) The Investigations Process. The Investigations Division receives information about potential violations through various sources, including the ICIG's Hotline; in-person meetings; telephone calls; emails; referrals from Intelligence Community Inspectors General Forum members; and law enforcement agencies. Examples of the types of violations the Investigations Division handles include, but are not limited to:

- conflicts of interest
- bribes and kickbacks
- unauthorized disclosures
- procurement fraud
- cost mischarging
- false official statements
- abuse of authority by government officials
- reprisal and retaliation
- misuse of government resources
- senior official misconduct

(U) The ICIG uses its independent investigative authority to gather and analyze facts associated with the information it receives to determine if potential violations have occurred, and the extent or severity of those potential violations. Cases in which violations are determined to be minor are most often referred to ODNI management for administrative action. The Investigations Division also refers complaints involving other agencies to the appropriate Inspector General office for further handling, if warranted. However, cases where violations are determined to be more serious (e.g., involving allegations of significant loss or serious violations of law) are further investigated

for possible criminal prosecution and/or civil litigation. When the ICIG's Investigations Division substantiates the allegations, one or more of the following actions, depending on the type and severity of the violation, may occur:

- criminal and/or military prosecution
- payment of restitution and/or civil settlement
- removal of personnel
- management referral
- contract value adjustment
- contract administrative action

(U) The Investigations Division engages in multiple forms of outreach to help ensure that ODNI personnel are fully aware of current and emerging issues as well as their obligation to report potential violations. For example, it regularly communicates through new employee orientation briefings and information tables to support and raise employee awareness of how to address questions, concerns, issues, and complaints. The Investigations Division also provides alerts on schemes and incidents that could adversely affect the ODNI and Intelligence Community programs. In addition, it conducts liaison activities with the Intelligence Community Inspectors General Forum members and law enforcement agencies, sharing information, generating potential investigative leads, and cultivating sources.

(U) For more additional information about the investigations process, please visit our website at [www.dni.gov/ICIG](http://www.dni.gov/ICIG).

## **(U) APPENDIX D: The Center for Protected Disclosures**

(U) 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 Intelligence Community 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.

(U) The ICIG's Center for Protected Disclosures (the Center) covers three functional areas critical for whistleblowers in the Intelligence Community: The ICIG's Hotline program; Outreach; and administering requests for review under Section C of Presidential Policy Directive 19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information*.

(U) The ICIG receives and processes Whistleblower complaints through the ICIG's Hotline program. The ICIG's Hotline program receives whistleblower complaints and concerns through public and secure telephone numbers and website addresses as well as through drop boxes and walk-in meetings at the ICIG's main office in Reston, Virginia, and its satellite offices in McLean, Virginia and Bethesda, Maryland.

(U) The Center also receives and processes allegations of "urgent concerns," disclosed pursuant to the *Intelligence Community Whistleblower Protection Act* (the ICWPA). The ICWPA established a process to ensure that the Director of National Intelligence, the Senate Select Committee on Intelligence (SSCI), and the House Permanent Select Committee on Intelligence (HPSCI) 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 involving classified information. The Center tracks all ICWPA disclosures, ensures review of materials for classified information, and coordinates disclosures with other authorities for appropriate review and disposition.

(U) The Center coordinates and harmonizes Hotline best practices with other Intelligence Community agencies through quarterly meetings of the Hotline Working Group. The Working Group shares information regarding commonalities and differences regarding the software they use, referral procedures, vetting of complaints, and referral of those complaints to other Inspectors General.

(U) The Center also 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.

(U) 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 individuals in the Intelligence Community, 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, individuals who believe they have suffered reprisal for making a protected disclosure are 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.

(U) For additional information about the whistleblower process, please visit our website at [www.dni.gov/ICIG](http://www.dni.gov/ICIG) or contact Inspector General of the Intelligence Community Hotline at 855-731-3260 (u) or 933-2800 (s).

**(U) APPENDIX E: ACRONYM LIST**

AIM	Augmenting Intelligence using Machines
The Center	Center for Protected Disclosures
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DNI	Director of National Intelligence
ERP	External Review Panel
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
HPSCI	House Permanent Select Committee on Intelligence
IARPA	Intelligence Advanced Research Projects Activity
IC	Intelligence Community
ICD	Intelligence Community Directive
ICIG	Inspector General of the Intelligence Community
ICWPA	Intelligence Community Whistleblower Protection Act
I&E	Inspections and Evaluations
IPERIA	Improper Payments Elimination and Recovery Improvements Act
IPR	In-Progress Review
ISCM	Information Security Continuous Monitoring
ODNI	Office of the Director of National Intelligence
PPD	Presidential Policy Directive
SSCI	Senate Select Committee on Intelligence
U.S.	United States

UNCLASSIFIED

THIS PAGE IS INTENTIONALLY BLANK

UNCLASSIFIED



UNCLASSIFIED