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

(U) Annual Work Plan

Fiscal Year 2019

(U) November 2018

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 our Fiscal Year 2019 Work Plan. The Plan identifies the ICIG's mandatory, as well as discretionary, assessments for the upcoming year. Each of the identified assessments supports and furthers the ICIG's statutory responsibility to promote economy, efficiency, and effectiveness in the administration and implementation of the programs and activities within the responsibility and authority of the Director of National Intelligence (DNI), and to prevent and detect fraud and abuse in such programs and activities.

(U) Prior to this year, the ICIG used its annual Work Plan as an internal coordination document and did not share it with Office of the Director of National Intelligence (ODNI) components, our Congressional oversight Committees, or the Intelligence Community Inspectors General Forum (the Forum). However, we developed this year's Work Plan intending to provide it to our colleagues and stakeholders as part of our broader effort to increase transparency and information sharing across the Intelligence Community, (IC) and to better align the ICIG's practices with other IC Inspectors General.

(U) The Work Plan identifies and details two types of assessments – mandatory and discretionary. Mandatory assessments are those required by Congressional statute. Discretionary assessments are those the ICIG selects at its discretion based on certain criteria. The ICIG uses measures such as mission impact, national security risk, cost, and information obtained through multiple sources, including the DNI, ODNI senior leadership, members of Congress and their staff, Forum members, IC employees and contractors, and other interested members of the public. Further, the ICIG planned joint discretionary assessments with other Forum members in accordance with our unique statutory responsibilities, and as part of Congress's intent for the ICIG to work across the IC to improve management, coordination, integration, and information sharing.

(U) The Work Plan is what it says it is – a plan. It is flexible and subject to change to account for the Intelligence Community's dynamic operating environment. We may need to add to our list of required assessments based on changes in the law, and as a result, reduce the number of discretionary assessments we conduct. We may also need to revise, add, or remove previously identified discretionary assessments based on unforeseen events or constraints to our workforce due to limited personnel resources, budgets, security clearance processing, or other operational challenges. Consistent with our commitment to professionalism and transparency, we will communicate any such changes to the appropriate stakeholders and notify appropriate officials regarding the timing and scope of our assessments before they begin.

(U) The ICIG looks forward to the coming year and providing the leadership, coordination, and responsiveness required and expected of us by the public, the DNI, and Congress.

Michael K. Atkinson
Inspector General of the Intelligence Community

Contents

(U) FISCAL YEAR 2019 PLANNED PROJECT DESCRIPTIONS

1. (U) REQUIRED PROJECTS

(U) FY 2019 Risk Assessment of ODNI'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 ODNI's implementation of the internal control requirements set forth in the Act and Office of Management and Budget guidance.

(U) Review of the ODNI's Compliance with the Improper Payments Elimination and Recovery Improvements Act (IPERIA) of 2012

(U) IPERIA 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 IPERIA. This project will evaluate the completeness, accuracy, and validity of the ODNI's disclosures on improper payments as reported in the FY 2018 Agency Financial Report.

(U) Review of the ODNI Implementation of the Cybersecurity Information Sharing Act of 2015, Section 107(b), *Oversight of Government Activities* for Calendar Years 2017 and 2018

(U) This review will assess ODNI's implementation of Cybersecurity Information Sharing Act requirements for Section 107(b), for calendar years 2017 and 2018, and specifically:

- The sufficiency of policies and procedures related to sharing cyber threat indicators within the federal government
- Classification of cyber threat indicators or defensive measures
- Accounting of the security clearances for sharing with the private sector
- Actions taken by the federal government based on cyber threat indicators or defensive measures shared with the federal government
- Sharing of cyber threat indicators or defensive measures with appropriate federal government entities
- Identification of barriers to sharing information about cyber threat indicators and defensive measures

(U) Joint Project on the Implementation of Cybersecurity Information Sharing Act of 2015 Section 107(b), *Oversight of Government Activities* for Calendar Years 2017 and 2018

(U) The project will report to Congress the consolidated results of the ODNI and Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury Inspector Generals' evaluations of their agencies' respective assessments of calendar year 2017 and 2018 implementation of Cybersecurity Information Sharing Act requirements for Section 107(b).

(U) FY 2019 Independent Evaluation of the Office of the Director of National Intelligence's (ODNI) Information Security Program and Practices Required by the Federal Information Security Modernization Act (FISMA) of 2014

(U) FISMA 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 information security program and practices of the ODNI. The evaluation will assess whether ODNI information security policies, procedures, and practices are effective in protecting information and whether the ODNI complied with applicable laws and regulations.

2. (U) DISCRETIONARY PROJECTS[1]

(U) Assessment of IC Foreign Language Capabilities

(U) Intelligence Community Directive (ICD) 630 introduced policies to develop and implement an integrated approach for ensuring the continuous availability of foreign language capabilities in an effort to achieve IC mission objectives. This assessment will examine ODNI's role in implementing an IC-wide strategy and achieving integration for foreign language programs and agency progress in accomplishing the goals of the *U.S. Intelligence Community Foreign Language Strategic Plan 2017-2020.*

(U) Assessment of ODNI Cybersecurity Requirements Process in the Major Systems Acquisition Life Cycle

(U) Cybersecurity is a critical component of the systems engineering process, and failure to integrate cybersecurity requirements across the entire acquisition life cycle may introduce exceptional risk to systems and users. The ICIG will review the Major Systems Acquisition cybersecurity requirements process to assess the effectiveness of actions undertaken to protect IC systems.

(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) Evaluation of Intelligence Oversight Guidelines and Processes

(U) As stated in Executive Order (EO) 12333, the IC has a solemn obligation to protect U.S. person information as it conducts intelligence activities. EO 13470 also establishes the need for guidelines for IC elements on access to and dissemination of all intelligence and intelligence-

[1] (U) The list of discretionary assessments is not in order of priority or intended sequence.

related information in addition to the requirements. This joint IC Office of Inspector General (OIG) evaluation will assess the IC intelligence oversight guidelines and their implementation.

(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 ability to identify and respond to the many threats that face our nation. The revision to ICD 701, *Unauthorized Disclosures of Classified National Security Information*, was issued December 22, 2017. The revised policy redirected some responsibilities, clarified others, and created additional ones for a comprehensive approach to managing unauthorized disclosures across the IC. 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) Implementation of Security Executive Agent Governing Policies for the Security Clearance Process

(U) Executive Order 13467 assigns DNI responsibility, as the Security Executive Agent (SecEA), 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 eligibility to hold a sensitive position. The ICIG, in collaboration with other IC OIGs, intends to examine the authorities, policies, and procedures vested in the SecEA to determine their adequacy, and review organizations' efficiency and effectiveness in the implementation of SecEA requirements, with a particular focus on the management of the current security clearance backlog.

(U) The Intelligence Advanced Research Projects Activity (IARPA) Contracting

(U) Charged with providing research and technical capabilities for the IC, IARPA invests in high-risk/high payoff research programs. This project will assess whether ODNI administers contracts for IARPA in accordance with applicable regulations. The project will also address whether contractors receive adequate oversight.

(U) Management of Privileged Users of ODNI Systems

(U) The ODNI relies on privileged users to develop, maintain, and operate IT solutions that enable the ODNI mission. Due to their elevated access to IT systems, these privileged users present a greater security risk. This project will assess whether internal controls are sufficient to mitigate the risk that such privileged users could cause serious harm to national security by compromising the confidentiality, integrity, and availability of ODNI information systems.

(U) ODNI's Assessment and Authorization (A&A) Program

(U) This project will evaluate ODNI's A&A program to determine its effectiveness in managing security risks to ODNI information systems. It will also assess whether the A&A program meets the objectives of ICD 503, *Intelligence Community Information Technology Systems Security Risk Management*; Committee on National Security Systems Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*; and other relevant ODNI requirements.

(U) ODNI Crisis Management Process and Procedures

(U) The Arab Spring, high-profile terrorist attacks, and other crises have impacted ODNI operations, particularly at the National Intelligence Management Council level. Crisis management is a core government function, including how the IC operates in a crisis, primarily focusing on National Intelligence Manager roles. Intelligence Community Policy Guidance (ICPG) 900.2, *Intelligence Community Crisis Management*, which was signed December 23, 2016, provides criteria and standards for this review. This project will assess the efficiency and effectiveness of ODNI's ability to engage in accordance with current proposed criteria and standards for IC crisis management.

(U) ODNI's Management of Service Agreements

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

(U) Support to Joint National Security Agency (NSA)-National Reconnaissance Office (NRO) OIG Facility Inspection

(U) This project plans to provide ICIG support to a joint NSA-NRO OIG inspection of an IC facility that will assess the overall efficiency and effectiveness of operations and determine levels of cooperation and collaboration among the mission partners. The ICIG's participation will provide another perspective and assist other members of the team in the identifying and examining issues discovered during the inspection.

(U) Support to NRO/Department of Energy (DOE) Intergovernmental Transfers

(U) The ICIG will support an audit NRO is conducting in coordination with DOE OIG. The project will examine whether NRO's activities in managing funds provided to DOE ensure accurate account balances to properly support and meet NRO's requirements.

(U) Terrorist Identities Datamart Environment (TIDE)

(U) ODNI's Directorate of Terrorist Identities (DTI) within the National Counterterrorism Center maintains the central repository of information on known or suspected terrorists. DTI is responsible for TIDE, which is the U.S. government's central repository of information on international terrorist identities, their contacts, and their support networks. The project will assess TIDE, including information system security controls; information sharing among IC elements; acquisition, integration, and development of identity information; compliance with policies and procedures governing TIDE operations, including intake and redress of identities and associated information; and protection of U.S. Person information in accordance with applicable laws and policies.

(U) Travel, Training, and Conference Spending

(U) This project will evaluate whether reimbursement claims for training, travel, and expenses for conferences were submitted and approved in accordance with applicable federal laws, regulations, and ODNI policy.

(U) Use and Impact of the Annual Functional Manager Assessment Report (AFMAR)

(U) The Intelligence Authorization Act for FY 2014 directs the DNI, in consultation with the IC Functional Managers (FMs), to submit the “Annual Functional Management Assessment Report” (AFMAR), to Congress’ intelligence oversight committees. The AMFAR empowers FMs, particularly in the area of critical budgetary control over their domains. Both Congress and the DNI have expressed their intent to link AFMAR to the National Intelligence Strategy. There have been three AFMAR reporting cycles since its inception. The ICIG will assess how effectively AFMAR has informed integrated management and mission execution, continues to empower FMs, and provides visibility to Congress.

(U) Validating the Claims of Higher Education by ODNI Cadre Employees

(U) Individuals with degrees from institutions that are not adequately accredited pose a potential risk to the integrity of the IC and a danger to the public. The recent attention on insider threat in the IC and continuous monitoring emphasizes the need to analyze data on the educational claims of ODNI cadre and contractors. This project will assess ODNI’s policy and processes designed to identify and authenticate claims of higher-level education made by cadre employees after the employees have on-boarded.

(U) FISCAL YEAR 2019 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 Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and ICIG conduct peer reviews of each other's audit divisions once every three fiscal years on a pre-determined schedule. The ICIG audit division was externally peer reviewed in FY2017; the next external peer review of the ICIG is scheduled for FY2020. The external peer review schedule is currently being revised and coordinated with the other IC OIGs.

(U) Inspections

(U) As adopted and approved by the majority of the Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) members, OIGs with an Inspections and Evaluations (I&E) 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 OIGs and their stakeholders of the I&E organization's compliance with covered Blue Book standards. External peer reviews provide a level of objectivity and independence in making this determination.

(U) ICIG I&E will support a multi-agency OIG peer review of the National Security Agency Inspections program in February 2019, and the NRO Inspections program during May-June 2019.

(U) The ICIG AIG for I&E, as Chair of the ICIG Inspections Committee, will continue to serve as the peer review schedule coordinator for the IC OIG inspection programs and provide schedule updates to the CIGIE I&E Committee.

(U) The I&E Division is scheduled to be peer reviewed in June 2020. Previous peer reviews of I&E occurred in 2014 and 2017.

(U) APPENDIX A: THE AUDIT PROCESS

(U) The ICIG Audit Division evaluates whether the goals and objectives of ODNI and IC 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 CIGIE. The audit process involves the following stages:

(U) **Announcement of Audit**. The ICIG 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 ICIG 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 ICIG 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 ICIG team gathers information to fully understand the entity's operations, activities, and internal controls. The information obtained may include relevant laws and regulations, prior IG 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 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 IC 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 IC to realize the maximum benefit from ICIG audits and projects, management should ensure that adequate corrective action is taken in a timely manner on the recommendations in the report. The ICIG 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 DNI and Congress. The ICIG Audit Division Assistant Inspector General issues a closure memorandum when he or she determines that all recommendations in a report have been addressed.

(U) Questions about the Audit process or component responsibilities in responding to draft and final reports may be addressed to Patti M., Assistant Inspector General for Audits, at 571-204-8149.

(U) APPENDIX B: THE INSPECTIONS PROCESS

(U) The ICIG Inspections and Evaluations Division conducts inspections, evaluations, and reviews to assist ODNI and IC 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 CIGIE. The Inspections and Evaluations process involves the following stages:

(U) **Planning**.

(U) Selection of inspection topics – Inspection topics may come from a variety of sources, including: Executive Department Direction, Congressionally Directed Actions, ODNI leadership requests, and ICIG internally generated ODNI Component Inspections.

(U) The ICIG annual work planning process selects and 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 organizations involved or, depending on the topic, it may be sent IC-wide. The announcement memorandum includes the objectives, start date, and request for a point of contact.

(U) Entrance Conference.

(U) The team will hold an Entrance Conference with the organizations involved in the inspection, evaluation, or review, and Senior Leaders from the organizations are interviewed. Information from the entrance conference and interviews are used to finalize a workforce questionnaire and data call.

(U) **Execution**.

(U) 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 is issued and results are 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**.

(U) Findings and Recommendations are finalized at the beginning of the Reporting Phase, and an In-Progress Review (IPR) is presented to ICIG 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 ICIG 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 I&E process improvement.

(U) Questions about the inspection, evaluation, or review process, or component responsibilities in responding to draft and final reports, may be addressed to Daniel S., Assistant Inspector General for Inspections & Evaluations at 571-204-8149.

(U) APPENDIX C: THE INVESTIGATIONS PROCESS

(U) The Investigations Division is the principal agent for investigating potential violations of federal law or agency regulations. The Division conducts independent and objective criminal and administrative investigations pertaining to programs and activities within the DNI's responsibility and authority. Consistent with the ICIG's unique statutory authority, the Division coordinates cross-IC criminal and administrative investigations. The 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 initiatives in the Annual Work Plan. However, because investigations often result from a deliberate subversion of ODNI procedures or controls, the details obtained from investigations may become integral to planning audits, inspections, and special projects.

(U) The Investigations Process

(U) The Investigations Division receives information about potential violations from ODNI and other IC personnel through various sources, including the ICIG Hotline; in-person meetings; telephone; emails; referrals from Intelligence Community Inspectors General Forum members; and law enforcement agencies. Examples of the types of violations the Investigations Division addresses 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 Division also refers complaints involving other agencies to the appropriate IG 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 investigation 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 ODNI and IC 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) APPENDIX D: ACRONYMS LIST

A&A	Assessment and Authorization Program
AFMAR	Annual Functional Manager Assessment Report
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CNSSI	Committee on National Security Systems Instruction
DNI	Director of National Intelligence
DOE	Department of Energy
DTI	Directorate of Terrorist Identities
EO	Executive Order
FISMA	Federal Information Security Modernization Act
FM	Functional Managers
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IARPA	Intelligence Advanced Research Projects Activity
IC	Intelligence Community
ICIG	Office of the Inspector General of the Intelligence Community
ICD	Intelligence Community Directive
ICPG	Intelligence Community Policy Guidance
I&E	Inspections and Evaluations
IPERIA	Improper Payments Elimination and Recovery Improvements Act
IPR	In-Progress Review
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
SecEA	Security Executive Agent
TIDE	Terrorist Identities Datamart Environment

THIS PAGE IS INTENTIONALLY BLANK