Office of the Inspector General
National Security Agency

Semi-Annual Report to Congress

1 April 2018 to 30 September 2018

Office of the Inspector General

Pursuant to the Inspector General Act of 1978, as amended, and in accordance with NSA/CSS Policy 1-60, the NSA Office of the Inspector General (OIG) conducts audits, inspections, intelligence oversight, and investigations. The OIG's mission is to detect and deter waste, fraud, abuse, and misconduct within the Agency and its programs, to promote the economy, efficiency, and effectiveness of NSA operations, and to conduct intelligence oversight ensuring that NSA activities comply with the law and are consistent with civil rights and civil liberties.

Audits

The audit function provides independent assessments of Agency programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls – Mission and Mission Support audits examine a wide range of Agency programs and operations, and Technology and Cybersecurity audits focus on information technology programs, systems, and capabilities. Financial audits determine whether Agency financial statements are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles, and conduct other required financial audits. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

Inspections

Inspections are organizational reviews that assess the efficiency and effectiveness of Agency components. The Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

Intelligence Oversight

Intelligence oversight (IO) works to ensure that NSA intelligence and intelligence-related functions comply with federal law, executive orders, and DoD and NSA policies, and that Agency activities are conducted consistently with civil liberties and U.S. person privacy protection. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

Investigations

The OIG investigates a wide variety of allegations of waste, fraud, abuse, and misconduct involving NSA programs, operations, and personnel. The OIG initiates investigations based upon information from a variety of sources, including complaints made to the OIG Hotline; information uncovered during its inspections, audits, and reviews; and referrals from other Agency organizations. Complaints can be made to the OIG Hotline online, by email, regular mail, telephone, or in person, and individuals can do so anonymously or identify themselves but indicate that they wish to maintain their confidentiality.

NOTE: A classified version of the Semi-Annual Report (SAR) to Congress formed the basis of this unclassified version. The National Security Agency (NSA) Office of the Inspector General (OIG) has endeavored to make this unclassified version of the SAR as complete and transparent as possible. However, where appropriate, the NSA OIG has rephrased or redacted information to avoid disclosure of classified information and as required to protect NSA sources and methods. In that regard, the classified version of this report contained descriptions of additional completed and ongoing work that could not be included in the public version of this report.

A Message from the Inspector General

I am very pleased to submit the semi-annual report (SAR) of the National Security Agency/Central Security Service (NSA) Office of the Inspector General (OIG) for the period 1 April through 30 September 2018. The report reflects a large and diverse body of independent oversight work conducted by the OIG over the past six months, and it is my honor to present it and to work with the dedicated men and women of the OIG whose outstanding efforts it reflects.

Transparency is a bedrock principle for OIGs, and during the past several months we have taken a number of significant steps in this regard at the NSA OIG. In July, for the first-time ever, we publicly released an unclassified version of our SAR from the prior reporting period. The OIG has prepared and provided to the Agency and Congress highly classified versions of its SARs for some time, but the public release of the unclassified version during this reporting period enabled us to inform the public more generally about the nature and scope of our oversight work. The unclassified version of the SAR initially was posted on https://oversight.gov, the aggregator site for federal Inspectors General maintained by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). It remains available on that important site, and also now is available on the NSA OIG's own new public internet site, https://oig.nsa.gov. This independent website provides the public with a great deal of information about the OIG, its structure and operations, and the nature of its oversight activities. We are very excited about both of these developments, and I encourage those who are interested in more information to view the introductory video on our site discussing why we believe it was important to enhance the transparency of our oversight work so that, even if the public cannot know everything about every Agency program or operation, it knows that there is effective independent oversight going on here. That oversight helps to ensure that taxpayer dollars are being spent wisely and that Agency programs are conducted in conformance with the law and civil rights and U.S. person privacy protections. In the latter regard, during this reporting period, I also was pleased to meet with representatives of non-governmental organizations active in the area of civil liberties and privacy rights, so that I could talk with them about our efforts and hear from them about the issues with which they are concerned. I am grateful to them for sharing their viewpoints and their expertise, and I am excited by all of the steps we have taken to enhance the transparency of our office's work.

We at the NSA OIG continue to champion whistleblower rights and protections. There is nothing more fundamental to the work of an OIG than the basic proposition that people should feel comfortable coming forward to this office or other designated recipients when they see something they reasonably believe is wrong, and they never should suffer reprisal for doing so. During this reporting period, we continued our efforts to inform Agency employees and affiliates about their rights and protections in this critical area, preparing and distributing informational cards to individuals and both electronic and hard copies of posters at facilities throughout the NSA enterprise. Our new public website follows our internal site here at the NSA in having a separate page that contains a variety of information about whistleblower rights and protections for both Agency employees and employees of contractors and others to whom general whistleblower protections were extended earlier this year. We also publicized National Whistleblower

Appreciation Day within the Agency this July, and I was pleased to attend a related event at the Dirksen Senate Office Building as well. I have continued and will continue to speak about the importance of these issues before groups large and small within and outside the Agency.

That brings us to the oversight work of the NSA OIG itself – the myriad investigations, audits, inspections, and special studies described in this report that cover a wide range of the programs and operations of the Agency and the conduct of its employees and others. During this reporting period, we took additional steps to ensure that our oversight work is as impactful as possible, including putting in place additional requirements intended to increase the timeliness of agency responses to the OIG and its resolution of outstanding recommendations. Agency management agreed with all OIG recommendations made during this period.

As detailed in the pages that follow, the OIG issued a total of 21 reports and oversight memoranda during this reporting period, making 620 recommendations to assist the NSA in addressing the findings and deficiencies that we identified and, thereby, improving its operations. We also found that some aspects of Agency programs and operations that we examined were working well, and we explicitly recognized a number of commendable or best practices that could be replicated across the enterprise. Our reports and oversight memoranda issued during this period were not posted publicly due to their classified nature, but they are available on the internal OIG website for access by personnel with the appropriate clearances, and copies of the reports and memoranda are enclosed with this classified version of this report provided to Congress. We also have been active in investigating diverse allegations of waste, fraud, abuse, and misconduct, processing 554 contacts that resulted in the initiation of 39 investigations and 118 inquiries during this reporting period, in which we also closed 30 investigations and 88 inquiries. OIG investigations resulted in disciplinary action being taken by the Agency against 24 employees, and the potential recoupment of a total of approximately $261,000 from employees and contractors.

All of the OIG's efforts were conducted in conformity with the Inspector General Act of 1978, as amended (the IG Act), which celebrated its 40th anniversary this year. The NSA OIG was brought within the IG Act in 2010 and, in 2014, the law was amended to call for a Presidentially appointed, Senate-confirmed (PAS) Inspector General here. It has been an honor to serve since January of this year as the NSA's first PAS IG, and to be part of a community that has grown to include 73 statutory IGs who collectively oversee operations of nearly every aspect of the Federal Government.

Pursuant to the IG Act, I am pleased to report that the OIG experienced no attempts by the Agency to interfere with our independence, and that the Agency fully cooperated with our work and did not refuse to provide or attempt to delay or restrict access to records or other information. In particular, I would like to acknowledge Agency leadership, including the Director, the Deputy Director, the heads of the Agency Directorates, and others throughout the organization who have been receptive as we have implemented the measures referenced above and conducted the work described in this report. As I traveled during this reporting period to the four NSA Cryptologic Centers and elsewhere, I have very much appreciated the input and the support for the oversight work of my office.

It continues to be an exciting time for the NSA OIG, as we endeavor to enhance the impact and the transparency of our work in promoting positive change at this agency whose work is, at its name implies, so critical for our national security.

ROBERT P. STORCH

Inspector General

DISTRIBUTION:

DIR
DDIR
ExDIR
CoS
Director, Workforce Support Activities
Director, Business Management & Acquisition
Senior Acquisition Executive
Director, Engagement & Policy
Director, Research
Director, Operations
Director, Capabilities
Director, National Security Operations Center
General Counsel

Contents

Index of Reporting Requirements

§5(a)(1)	Significant problems, abuses, and deficiencies	3
§5(a)(2)	Recommendations for corrective action	3
§5(a)(3)	Significant outstanding recommendations	27-31
§5(a)(4)	Matters referred to prosecutorial authorities	16-17
§5(a)(5)	Information or assistance refused	IV
§5(a)(6)	List of audit, inspection, and evaluation reports and oversight memoranda	24-25
§5(a)(7)	Summary of significant reports	3
§5(a)(8)	Audit reports with questioned costs	26
§5(a)(9)	Audit reports with funds that could be put to better use	26
§5(a)(10)	Summary of reports for which no management decision was made	3
§5(a)(11)	Significant revised management decisions	3
§5(a)(12)	Management decision disagreements	3
§5(a)(13)	Information described under Section 804(b) of FFMIA of 1996	N/A
§5(a)(14)	Results of peer review conducted of NSA OIG	22
§5(a)(15)	List of outstanding recommendations from peer review of NSA OIG	N/A
§5(a)(16)	List of peer reviews and outstanding recommendations conducted by NSA OIG	22
§5(a)(17)	Statistical tables of investigations	20-21
§5(a)(18)	Description of metrics used in statistical tables of investigations	24-25
§5(a)(19)	Reports concerning investigations of Seniors	17-18
§5(a)(20)	Whistleblower Retaliation	18
§5(a)(21)	Agency interference with IG independence	IV
§5(a)(22)	Disclosure to the public	IV
§5(a)(note)	P.L. 110-181 §845, Final completed contract audit reports	
§5(a)(note)	P.L. 103-355 (as amended), Outstanding recommendations past 12 months	27
* IG Act of 1978, as amended, including the IG Empowerment Act of 2016.		

This page intentionally left blank.

OIG Executive Summary

This has been a busy and productive reporting period for the OIG. Among the Division and program highlights are:

Audit Division

During the 6-month reporting period, the Audit Division issued a total of 6 reports and oversight memoranda containing 34 recommendations to improve Agency operations. These audit products, consisting of three audit reports, one quick reaction report, a review arising from a hotline complaint, and an oversight review, were performed as a result of OIG- and Agency- identified risks as well as congressional mandates. The Audit Division is divided into three branches – Technology and Cybersecurity, Mission and Mission Support, and Financial Audit.

The Technology and Cybersecurity branch performed a review to determine whether individuals were designated to fill certain System Security Plan (SSP) critical roles (Information System Owner (ISO), Information System Security Officer (ISSO), and System Administrator (SA)) for 10 operational Agency systems. We found that several Agency systems examined are operating without one or more critical security roles assigned as required. As a result, the Agency does not have reasonable assurance that some systems have requisite security oversight.

The Mission and Mission Support branch focused two audits on the health and safety of the Agency workforce. While performing an ongoing audit related to the Agency's handling of weapons and ammunition, we observed a concern that required prompt attention and issued a Quick Reaction Report related to loading barrels being located on a conference room shelf within Security space, which posed a potential critical life safety risk to passersby or unsuspecting personnel in their vicinity. The Audit of the Emergency Management Program reviewed the process to prepare and respond to emergencies at NSA's Washington-area facilities.

The Financial Audits branch conducted a congressionally mandated audit concerning NSA's Compliance with the Improper Payments Elimination and Recovery Improvement Act (IPERIA).

Inspections Division

The OIG issued six inspection reports and conducted five new inspections, all on field sites. There were no attempts to impede our inspection activities, and the Agency and all sites fully cooperated with our work, which resulted in a wide range of recommendations for improvements in operations.

Intelligence Oversight

The OIG's Intelligence Oversight Division issued a total of nine special studies and oversight memoranda during this reporting period. These consisted of three special studies, three, advisory memoranda, two quick reaction reports, and an annually required report, which were performed as a result of OIG identified risks; new civil liberties and privacy protections training requirements

imposed by DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 August 2016, and DoD Directive 5148.13, *Intelligence Oversight*, 26 April 2017; as a part of the OIG's series of studies on special authorities; and in response to requirements levied on the OIG in the Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act of 2008; a complaint to the OIG hotline; and a U.S. House Permanent Select Committee on Intelligence request to the Inspector General of the Intelligence Community. In total, 95 recommendations were made in these Intelligence Oversight special studies and oversight memoranda to assist the Agency in improving its operations and increase compliance with requirements for protecting civil liberties and U.S. Person privacy.

Investigations

During this reporting period, the Investigations Division received and processed 554 contacts, which resulted in the initiation of 39 investigations and 118 inquiries. Three new investigations involve allegations of whistleblower reprisal, and two involve allegations of nepotism. Thirty investigations and 88 inquiries were closed during the reporting period, resulting in the proposed recoupment to the Agency of approximately $125,000 from employees and approximately $136,000 from contractors. As a result of OIG investigations, disciplinary actions ranging from termination to reprimands were taken against 24 employees. A case referred to the U.S. Attorney for the District of Maryland in 2017 resulted in a guilty plea, and another involving a contractor company resulted in a settlement with the government calling for payment of over $1.5 million. One other case was accepted for consideration of prosecution by the U.S. Attorney for the District of Maryland, and another case is under review.

Whistleblower Program

The OIG's guiding principle in this area remains clear: Whistleblowers perform an important service to the NSA and the public when they come forward with what they reasonably believe to be evidence of wrongdoing. They should never suffer retaliation or reprisal for doing so. During this period, the OIG opened three new reprisal investigations, and closed one reprisal investigation in which the OIG did not substantiate the allegations. Additionally, the OIG has expanded its efforts to inform Agency employees and others regarding whistleblower rights and protections, including making additional informational materials available on the OIG's internal website and the OIG's new external website, preparing information cards for distribution to new employees and others, and disseminating posters for electronic and other display throughout the Agency enterprise.

Significant Problems, Abuses, and Deficiencies and Other Significant Reports

OIG projects during the reporting period did not reveal serious or flagrant problems or abuses related to the administration of Agency programs or operations that would require immediate reporting to the DIRNSA and Congress pursuant to Section 5(d) of the Inspector General Act. However, the OIG's *Special Study of Data Sharing with Third Party Partners* revealed significant problems and deficiencies, as detailed below.

Report on the Special Study of Data Sharing with Third Party Partners

The OIG conducted this study to follow up on problems identified in an earlier special study, and because of the increase in the amount of data shared with Third Party Partners (certain foreign countries, hereafter referred to as "Partners") since then. An area of emphasis in the study was the protection of the privacy rights of U.S. persons (USPs). The OIG made 22 recommendations to assist the Agency in addressing the findings of the study, which included the following:

- Governing documentation, including relevant U.S. SIGINT Directives and other policies and documents, is outdated, inaccurate, and/or incomplete;
- Inadequate Agency documentation of data flows risks potentially unauthorized or delayed sharing of data with Partners;
- Sampling documentation and processes used by the Agency to identify and mitigate potential compliance incidents require improvement;
- Partner personnel who access certain data may lack required training; and
- Intelligence Oversight Officers are not clearly identified and not all personnel who represent NSA to the Partner have been properly trained.

Summary of Reports for Which No Management Decision Was Made

No reports without management decisions were published.

Significant Revised Management Decisions

No reports with significant revised management decisions were published.

Management Decision Disagreements

No reports with management disagreements were published.

Audits

Audit Reports and Memoranda Completed in the Reporting Period

Audit of the NSA's Emergency Management Program

The Department of Defense requires that Agencies establish policy, assign responsibilities, and develop procedures to sustain an all-hazards emergency management (EM) program. In response, the Agency developed Policy 1-65, *National Security Agency EM Program*, and the *Emergency Operation Center Procedure Manual* to establish the Agency's process to prepare and respond to emergencies at NSA's Washington-area (NSAW) facilities. The audit found that emergency preparedness needs improvement, emergencies were not managed as described, and EM program structure was lacking. The report resulted in 19 recommendations to assist the Agency in improving the Emergency Management Program.

Audit of NSA's FY2017 Compliance with the Improper Payments Elimination and Recovery Improvement Act

The objective of the audit was to determine whether the Agency complied with the Improper Payments Information Act, as amended by the Improper Payments Elimination and Recovery Act of 2010 and IPERIA. The audit found that in FY2017, the Agency complied with IPERIA. However, the Agency can improve the effectiveness of its payroll improper payment review process. In addition, NSA's FY2017 Agency's Financial Report identified three programs susceptible to improper payments: transactions by others, grants, and payroll. The report resulted in two recommendations to update the IPERIA payroll SOP and to clarify Agency policy for recording hours worked that exceed approved scheduled overtime.

Quick Reaction Report arising from the Audit of NSA's Accountability of Weapons, Ammunition, and Other Sensitive Assets

The NSA OIG is conducting an audit to assess NSA's control over weapons, ammunition, and other sensitive assets, such as deployment gear, police land mobile radios, defensive gear, and badges. During the course of the audit, the auditors observed health and safety concerns that required prompt attention; auditors found that loading barrels were located in areas within Security space in a NSA facility that posed a potential critical life safety risk. The report resulted in two recommendations to relocate loading barrels and to implement guidance on the proper location of loading barrels in NSA facilities.

Audit of Nuclear Command and Control Systems

The OIG conducted this audit of Agency Nuclear Command and Control (NC2) systems security controls to determine whether system security controls were implemented to sufficiently protect the program data and to assess NSA compliance with NSA/CSS Policy 6-3, *Information System Security Authorization Using the Risk Management Framework*, 13 June 2016, revised 24 May 2017, and Intelligence Community Directive (ICD) 503, *Practitioner Manual*, 29 January 2013.

Due to the classification of the OIG's findings and recommendations, they cannot be further described in the unclassified version of this report.

Oversight Review of the Audit of the NSA Restaurant Fund and the NSA Civilian Welfare Fund

The overall objective of the oversight review was to ensure that the audits performed by an independent public accounting (IPA) firm of the financial statements of the NSA Restaurant Fund and the NSA Civilian Welfare Fund as of and for the fiscal years ended 30 September 2017 and 2016 were performed in accordance with U.S. generally accepted government auditing standards. In its audit, the IPA firm reported: the financial statements were fairly presented, in all material respects, in accordance with U.S. generally accepted accounting principles; no material weaknesses in internal control over financial reporting; and no reportable noncompliance with provisions of laws tested or other matters. The NSA OIG reviewed the IPA firm's report and related documentation, and inquired of its representatives, which disclosed no instances in which the IPA firm did not comply, in all material respects, with U.S. generally accepted government auditing standards.

Review of the Designation of Individuals to Fill System Security Plan (SSP) Critical Roles

In December 2017, the NSA OIG received an anonymous complaint that individuals were not designated to fill certain System Security Plan (SSP) critical roles (Information System Owner (ISO), Information System Security Officer (ISSO), and System Administrator (SA)) for a number of operational Agency systems. As a result of this allegation, the OIG initiated a review, which revealed that the Agency does not have reasonable assurance regarding the requisite security oversight of some of the systems and that Security Engineering Services was not following its own guidance regarding procedures if a critical role is not assigned to a system. The report resulted in three recommendations to assist NSA in addressing the issues identified.

Ongoing Audits

Audit of Nuclear Command and Control Program II

The overall objective of the audit is to assess mission critical aspects, of the NC2 program, including systems security controls, governance, mission assurance, personnel, and facilities. The OIG is issuing two reports to address this topic, one focused on systems, which was issued during this reporting period (see above), and the other on the remaining issues.

Audit of Award Fee Contracts

The overall objective of the audit is to evaluate whether governance of the award fee process complies with applicable laws and policies and is conducted economically and efficiently. The OIG is examining 54 such contracts in effect during Fiscal Years 2016 and 2017, with a total reported value of several billion over the life of the contracts.

Audit of the Post Publication of Serialized SIGINT Reports

The overall objective of the audit is to determine whether comprehensive, consistent, and effective processes for Post-Publication of Serialized SIGINT Reports exist at the Agency. The NSA's

Post-Publication of Serialized SIGINT Reports Service offers consumers of NSA serialized reporting the ability to request approval to share appropriate report intelligence, notwithstanding the original report classification or dissemination control markings, with certain other government customers or partners. Specific processes and associated policies and procedures related to Identity Releases are not in the scope of this audit.

Audit of NSA's CIO Authorities

The overall objective of the audit is to determine whether the Agency's CIO is compliant with the requirements of the Clinger-Cohen Act of 1996 and Office of Management and Budget (OMB) M-11-29, *Chief Information Officer Authorities*, 8 August 2011, in providing oversight and management of information technology.

Audit of NSA's Travel Program

The overall objective of the audit is to determine if the Agency's travel program has adequate internal controls to ensure travel entitlements are paid efficiently and in accordance with applicable policy and procedures.

FY2018 Review of the Compliance with the Federal Information Security Management Act at NSA

The overall objective of the review is to evaluate the Agency's information security program and practices. In accordance with Office of Management and Budget guidance, the OIG is assessing the overall effectiveness of the Agency's information security policies, procedures, and practices.

Audit of NSA Corporate Authorization Service (CASPORT)

The overall objective of the audit is to determine, through review of configuration and operating procedures, whether CASPORT, which provides authorization attributes and access control services to NSA Enterprise programs and projects, is secure, resilient, and operationally effective.

Audit of NSA's FY2018 Financial Statements

The objective is to provide an opinion on whether the Agency's financial statements are presented fairly, in all material respects, in accordance with U.S. Generally Accepted Accounting Principles and to assess the Agency's internal controls over financial reporting and compliance with applicable laws and regulations.

Audit of NSA's Internal Controls Over Second Party Integrees

The overall objective of this audit is to determine whether the internal controls over the integration of Second Party (certain foreign countries) personnel into the NSA workforce are operating effectively and efficiently.

FY2018 Statement of Standards for Attestation Engagement 18, "NSA's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Controls"

The OIG contracted with an independent public accounting firm to conduct a Type II Service Organization Controls 1 examination and prepare an opinion on whether (1) NSA management's description of systems fairly presents the systems designed throughout the period 1 October 2017 through 30 June 2018; (2) controls related to the control objectives identified in management's system description were suitably designed throughout the specified period; and (3) controls selected for testing operated effectively to provide reasonable assurance that the control objectives in NSA management's system description were achieved through the specified period.

Joint Audit of Intragovernmental Transactions

The objectives of the audit are to determine whether processes for recording and monitoring intragovernmental transactions are effective and in compliance with federal requirements and whether intragovernmental account balances are accurate and properly supported.

Audit of NSA's Accountability for Weapons, Ammunition, and Other Sensitive Assets

The overall objective of the audit is to assess NSA's controls over weapons, ammunition, and other sensitive assets, such as deployment gear, police land mobile radios, defensive equipment, and badges.

Audit of NSA's Information System Decommissioning Process

The overall objective of the audit is to determine whether the Agency is effectively decommissioning information systems, including doing so consistently, securely, and efficiently.

Audit of NSA's Facilities and Logistics Service Contract

The overall objective of the audit is to determine whether the contract, which has a maximum ceiling of several hundred million dollars over a 5-year period, was awarded properly and is being administered effectively and in accordance with applicable policies.

Audit of NSA's Temporary Medical Leave Assistance Program (Leave Bank)

The overall objective of the audit is to determine whether NSA is administering the Leave Bank in accordance with applicable laws and Agency regulations. The audit also will determine whether internal controls within the program are effective in preventing fraud, waste, and abuse.

Inspections

Inspection Reports and Memoranda Completed in the Reporting Period

Limited Scope Inspection of the Laboratory for Analytic Sciences (LAS)

The OIG conducted a limited-scope inspection of the cryptologic activities performed at the LAS on the campus of North Carolina State University in Raleigh, NC, from 31 July through 2 August 2017. The inspectors also reviewed the cryptologic activities of a contractor facility associated with LAS' research and analytic activities, from 22-23 August 2017. Inspectors interviewed members of the workforce, site leaders, and key customers, and reviewed site documentation. This was the first inspection of LAS-associated facilities.

The OIG found the LAS workforce to be professional, friendly, innovative, and collaborative, and that the leadership team was organized, supportive, and communicates clearly and often. The OIG identified a number of deficiencies that should be addressed, making 20 recommendations to assist the Agency in addressing the issues identified in the report.

Limited Scope Inspection of Human Language Technologies (HLT) Contractor Locations

The OIG conducted limited scope inspections of the cryptologic activities performed at two separate HLT contractor locations, from 12 through 28 September 2017. This was the first inspection of these sites.

The OIG did not identify any negative findings in a number of areas, including Mission Operations, Program Management, and Training and Knowledge. However, the OIG identified a number of deficiencies that should be addressed involving Agency IT systems, making 11 recommendations to assist the Agency in addressing the findings identified in its report.

Joint Inspectors General Inspection Report - NSA Georgia (NSAG), 23 October to 3 November 2017

A joint NSA, Army Intelligence Security Command (INSCOM), U.S. Navy Fleet Cyber Command (FCC), and 25th Air Force Offices of the Inspector General Inspection team evaluated the overall compliance, effectiveness, and efficiency of NSAG during an inspection from 23 October through 3 November 2017. The last inspection of NSAG was in March 2014.

Overall, NSAG personnel expressed a high level of job satisfaction, but struggled with non-mission concerns such as the Field Tour Policy (which impacts the amount of time employees can remain at a site without rotating elsewhere), unfilled billets following the Agency-wide restructuring under NSA21, space allocation, and insufficient seating issues. The OIG team identified a number of deficiencies that should be addressed, many of which were commensurate with what the OIG has seen at many field sites. The OIG found that special attention should be

paid to integrees and contractors performing certain missions without appropriate authorization; training issues associated with a lack of adequate billets and personnel; and mission challenges faced due to a lack of enough well-trained linguists.

The OIG team noted a number of commendable practices at NSAG it believed other NSA sites should consider for adoption:

- a council to target employee assistance strategies toward key events affecting the workforce;
- a cross-organizational effort to highlight workforce safety concerns and requirements to senior leadership;
- an Organizational Safety and Health Representative (OSHRep) inspector program requiring OSHReps to inspect areas other than their own workspace, to learn new skills, and to be exposed to different environments; and
- a data center management team providing a comprehensive training program for all personnel accessing the machine rooms of NSAG.

The OIG made a total of 291 recommendations and 27 observations to assist NSAG and the Agency in addressing the findings identified during the inspection.

Field Inspection of NSA/CSS Representative to Defense (NCR DEF) and NSA/CSS Representative to Defense Intelligence Agency (NCR DIA): 26 to 27 February 2018

The OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the NCR DEF and NCR DIA during a 26 to 27 February 2018 inspection. The OIG team reviewed pertinent documents, support agreements, policies, regulations, and intelligence oversight data. Inspectors conducted interviews with members of both the NCR DEF and NCR DIA workforce, including off-site interviews with outgoing and incoming leadership.

Overall, the OIG uncovered relatively few issues of concern at NCR DEF and NCR DIA. Although the quality and functionality of information technology and systems were commensurate with what the OIG has seen at most field sites, the OIG found that attention should be paid to some issues, including restricting physical access to certain equipment at the Pentagon- and DIA Headquarters-hosted locations. In addition to some property accountability discrepancies, several support agreements for both offices need to be updated. The OIG made 42 recommendations to assist the Agency in addressing the issues identified in the report.

Ongoing Inspection Work

- ***Inspection of NSA Kent Island: 4 to 5 June 2018***
- ***Joint Inspectors General Inspection Report - Alaska Mission Operations Center: 16 to 20 July 2018***
- ***Joint Inspectors General Inspection Report - NSA Hawaii: 4 to 14 September 2018***
- ***Inspection of NSA/CSS Representative Pacific Command: 12 to 18 September 2018***

Intelligence Oversight

Special Studies and Oversight Memoranda Completed in the Reporting Period

Quick Reaction Report arising from the Review of NSA Analyst Compliance with Intelligence Community Directive on Dissemination of Congressional Identities

While conducting a review of NSA compliance with Intelligence Community Directive (ICD) 112, 29 June 2017, *Congressional Notification*, Annex A, "Dissemination of Congressional Identity Information," 19 January 2017, the OIG discovered three NSA serialized reports in which it appeared that the handling of U.S. Person information, including congressional identity information, did not comply with NSA policy/guidance.

The OIG issued a Quick Reaction Report in which it recommended that NSA review the identified reports and implement corrective actions as appropriate. NSA Directorate of Operations confirmed the OIG findings and took the appropriate corrective actions.

Advisory Memorandum on NSA's Implementation of Department of Defense (DoD) Training Requirements: Civil Liberties and Privacy Protections and Intelligence Oversight

The OIG found that, although new civil liberties and privacy protections training requirements imposed by DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 August 2016, and DoD Directive 5148.13, *Intelligence Oversight*, 26 April 2017, had been in effect for more than a year, NSA had not yet fully determined the content, audience, and periodicity of the required training. The OIG made 13 recommendations to address these concerns, 5 of which were completed and closed by the time of report publication.

In addition, as a result of this advisory, the NSA determined that the exemption to the DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 7 December 1982, IO training requirement, authorized by the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) [ATSD(IO) is now the DoD Senior Intelligence Oversight Official (DSIOO)] in 2008 for certain categories of NSA contractors, does not carry forward to the new requirements. The OIG made another five recommendations on the topic of contractor exemptions to required DoD training; four of the five recommendations were completed and closed at the time of report publication.

Quick Reaction Report on the Review of the Ingest Filter of an NSA Data System

The OIG is currently conducting a Limited Scope Study of NSA Data Tagging Controls to Comply with the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) Sections 704 and 705(b) Minimization Procedures. As part of the study, the OIG reviewed NSA's filtering control implemented in December 2017 to prevent data objects that contain selectors associated with Section 704 and 705(b) authorized targets from being ingested into an NSA data system integrating data from multiple intelligence platforms. The system is not approved for FISA data because it is accessible by certain foreign government partners who are not authorized to have such access and

provides limited data to a system accessible by other foreign government partners. During testing performed on 4 June 2018 and 18 July 2018 (each covering data ingested during the prior 10-day period), the OIG found that NSA's filtering control did not prevent a significant number of data objects containing selectors associated with several Section 704 or 705(b) authorized targets from being ingested into the data system. The OIG issued a Quick Reaction Report in which it made six recommendations to assist the Agency in addressing these deficiencies.

Annual FAA Section 702 Report to Congress

The OIG completed its report for 2017 in accordance with the Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act of 2008 subsection 702(m)(2). The OIG reviewed the data reported by NSA with respect to the number of disseminated intelligence reports containing one or more references to U.S. person identities; the number of U.S. person identities subsequently disseminated by NSA in response to requests for identities that were not referred to by name or title in the original reporting (*i.e.*, pursuant to unmasking requests); and the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed. With respect to the latter category, the OIG was not able to independently ascertain how many such communications were actually reviewed. The OIG must provide each such review annually to the Attorney General, the DNI, the Congressional intelligence committees, and the Committees on the Judiciary of the House of Representatives and the Senate.

Advisory Memorandum on the Routine Practice of Emailing Data Inconsistently with Agency Procedures

The OIG reviewed and substantiated an allegation that it received that analysts within an NSAW Directorate of Operations organization routinely email data via the Agency's classified email system in a manner not consistent with applicable Agency procedures. The OIG also determined through previous studies, inspections, and reviews that this practice occurs throughout the enterprise.

The OIG assessed that the practice of emailing data is the result of fast-paced operations that demand quick collaboration, ambiguous and hard-to-find guidance, and the lack of an enforcement mechanism to ensure compliance with current guidance. Previous OIG reports recommended that the Agency: 1) develop formal guidance, 2) clarify the requirements for compliantly emailing data, and 3) develop an enforcement mechanism. However, those recommendations remain open and were more than 22 months overdue as of the issuance of this Advisory Memorandum. Given the recurring nature of this problem, the OIG believes it is important that the Agency re-evaluate the effectiveness of current controls and take action consistent with the OIG's prior recommendations.

Advisory Memorandum on Policies Identifying and Documenting Intelligence Oversight Functions and Responsibilities

While conducting inspections of intelligence oversight programs at NSA field elements, the OIG observed sites using different titles for personnel who oversee the intelligence oversight program at various locations. The OIG, therefore, reviewed NSA policies to identify the responsibilities

and qualifications for personnel who oversee the intelligence oversight program at a particular location and found that NSA policies did not fully define the responsibilities or qualifications for this role. The OIG identified additional intelligence oversight roles that either are not fully defined or are used inconsistently in NSA policies and guidance. These deficiencies place NSA at risk of ineffective intelligence oversight. Thus, the OIG made three recommendations to NSA to address these concerns by defining and applying consistent usage of these roles in NSA policies and guidance.

Special Study of Data Sharing with Third Party Partners

See the "Significant Problems, Abuses, and Deficiencies and Other Significant Reports in the Reporting Period" section of this report.

Special Study of NSA Compliance with Requirements for SIGINT Mission Documentation

The OIG conducted this study to examine deficiencies in SIGINT mission documentation noted during OIG intelligence oversight inspections and to make recommendations to address these deficiencies. The review revealed a number of deficiencies that have resulted in unauthorized accesses to data. In addition, internal controls for a system that manages access to SIGINT data, compliance training for intelligence oversight officers, and guidance on the timeline to report compliance incidents all need improvement so NSA management has reasonable assurance that the SIGINT mission is conducted in accordance with its authorities and policies. The OIG made 34 recommendations to assist the Agency in addressing the deficiencies identified in this report.

Special Study of Compliance with Signals Intelligence Policies in Two Programs

In response to a U.S. House Permanent Select Committee on Intelligence request to the Intelligence Community Inspector General, the OIG conducted this study to determine whether the intelligence oversight (IO) policies and procedures implemented in two programs comply with applicable laws, regulations, and policies. The review revealed several deficiencies that increase the risk for improper handling of mission data and that have the potential to impact the protection of U.S. person privacy rights. The OIG made 11 recommendations that it believes will facilitate compliance with IO and security regulations and policies and improve management and administration of the two programs.

Ongoing Special Studies

Special Study of Certain Internet Capabilities, Part II

This study expands upon the OIG's earlier study, *Special Study of Certain Internet Capabilities,* which determined whether controls for certain internet capabilities that provide access to publicly available information on the internet are adequate to ensure compliance with Department of Defense and NSA policies to protect the civil liberties and privacy of U.S. persons. This second study examines management oversight, policy, training, and roles and responsibilities for such internet capabilities.

Review of NSA Compliance with Intelligence Community Directive on Dissemination of Congressional Identities

The objective of this review is to evaluate NSA's compliance with Intelligence Community Directive 112, 29 June 2017, *Congressional Notification*, and its Annex A, "Dissemination of Congressional Identity Information," 19 January 2017. The OIG review is focused on NSA analysts' compliance with the requirements regarding the dissemination of congressional identity information in intelligence reporting.

Limited Scope Study of NSA Data Tagging Controls to Comply with the FISA Amendments Act (FAA) Sections 704 and 705(b) Minimization Procedures

The objective of this review is to determine to what extent NSA controls ensure that data labels are applied accurately and completely to FAA Sections 704 and 705(b) SIGINT data.

Special Study of NSA's System Compliance Certification Process

The objective of this review is to assess the efficiency and effectiveness of NSA's system compliance certification process. The purpose of NSA's certification process is to ensure that, at the time of certification, SIGINT systems are operating in accordance with the legal authorities, directives, and policies that protect U.S. person privacy.

Special Study of a Targeting System's Control Framework to Ensure Targeting Complies with NSA's SIGINT Authorities to Protect U.S. Person Privacy

The objective of this review is to evaluate the accuracy, reliability, and effectiveness of a targeting system's control framework to ensure targeting complies with NSA's SIGINT authorities to protect U.S. person privacy.

Special Study of the Endpoint and Forensics Mission

In this review, the OIG is evaluating the efficiency and effectiveness of NSA's procedures used to ensure that the endpoint and forensics mission complies with legal authorities, directives, and policies that protect U.S. person privacy.

Special Study of the Process to Purge Signals Intelligence Data from NSA Source Systems of Record

The objective of this review is to assess the effectiveness and efficiency of NSA's process to find, and quarantine or remove, unauthorized or otherwise noncompliant SIGINT data completely, reliably, and in a timely manner in accordance with legal and policy requirements.

Special Study of NSA's Systems-Related Compliance Incident Management Process

The objective of this review is to determine the effectiveness and efficiency of NSA's incident management process for systems-related compliance matters.

Verification of NSA's Deletion of Certain USA Freedom Act Data

The objective of this activity is to independently verify that NSA has deleted all USA Freedom Act data ingested prior to 23 May 2018 from NSA repositories identified by the Agency following its receipt from telecommunications service providers of call dialing records that the NSA was not authorized to receive.

Special Study of NSA Controls to Comply with Signals Intelligence Retention Requirements

The objective of this review is to determine whether select NSA controls are adequate to ensure compliance with SIGINT retention requirements.

Investigations

Prosecutions

An OIG investigation reviewing allegations that a contractor provided unqualified labor in support of an Agency contract resulted in a referral to the U.S. Attorney for the District of Maryland. In July 2018, the Department of Justice and the contractor, CACI Technologies LLC signed an agreement in which CACI agreed to pay more than $1,500,000 to settle the allegation that it breached its contract with the Agency by billing and accepting payment for work performed by certain employees who did not meet the required contractual qualifications. The settlement was neither an admission of liability by CACI, which cooperated in the investigation and took remedial action in the wake of the investigation, nor a concession by the United States that its claims were not well founded.

A case referred to the U.S. Attorney for the District of Maryland in October 2017 involving allegations that a contractor employee fraudulently charged the Agency for hours not worked is pending resolution.

A case referred to the U.S. Attorney for the District of Maryland in July 2018 was accepted for consideration of criminal prosecution. In this case, the OIG received allegations that a contractor employee fraudulently charged the Agency for hours not worked. Based upon current information, the contractor may have fraudulently charged the Agency more than 1,700 hours, resulting in a shortfall to the Agency of approximately $220,000. The contractor employee's actions were potentially in violation of various statutes, including 18 U.S.C. §§ 287 and 1001, and 31 U.S.C. § 3802.

The U.S. Attorney for the District of Maryland is reviewing a case referred by the OIG in September 2018. The case involves allegations that a contractor employee fraudulently charged the Agency for hours not worked. Based upon current information, the contractor may have fraudulently charged the Agency more than 1,600 hours, resulting in a shortfall to the Agency of approximately $152,000. The contractor employee's actions were potentially in violation of various statutes, including 18 U.S.C. §§ 287 and 1001, and 31 U.S.C. § 3802.

Agency Referrals

In addition to the cases discussed above and as required by section 4(d) of the Inspector General Act of 1978 (as amended), 5 U.S.C. appendix, the Investigations Division reported eight other cases to the Department of Justice during the reporting period. In each case, the OIG had reasonable grounds to believe that a violation of federal criminal law had occurred. The allegations referred included employees representing a private company back to the federal government, making false statements, and submitting false timesheets, and contractors submitting false labor charges. The OIG anticipates at this time that the government is likely to handle them administratively, rather than criminally.

The Investigations Division referred 27 cases involving Agency personnel to NSA Employee Relations (ER) for potential disciplinary action. During the reporting period, the OIG received notification from the Agency of disciplinary decisions regarding 29 employees. Two employees were removed from employment, eight employees resigned in lieu of termination, and three employees resigned before disciplinary action was taken. Five employees received suspensions ranging from 10 to 30 days. Six employees received written reprimands, and in five cases, ER took no action.

Five cases substantiating contractor misconduct were referred to the Maryland Procurement Office for action, resulting in the proposed recoupment of approximately $136,000.

OIG Hotline Activity

The Investigations Division fielded 554 contacts through the OIG hotline.

Significant Investigations

Senior Military Officer: Hostile Work Environment, Preferential Treatment

An OIG investigation determined that a Senior Military Officer failed to take action to correct a subordinate's inappropriate behavior enabling the creation of a hostile work environment. The officer's failure to promote a positive and professional work environment was in violation of DoD 5500.7-R, JER, Chapter 12, Section 4, Paragraph 12-401 (b) & (d) through (g), and Military Service regulations. The OIG also determined that the officer had created the appearance of violating ethical standards pertaining to impartiality and preferential treatment toward the subordinate, in violation of 5 CFR § 2635.101 (b)(14). Finally, the OIG found that the officer's failure to be candid during sworn testimony was in violation of Agency policy and 5500.7-R, JER, Chapter 12, Section 4, Paragraph 12-401 (a) & (b).

The investigative findings were forwarded to the Department of Defense Office of the Inspector General, the Military Service Inspector General, and the Office of Personnel Security.

The case did not meet the requirements for reporting to the Department of Justice.

Senior Executive: Hostile Work Environment, Preferential Treatment

An OIG investigation determined that a Senior Executive employee engaged in conduct that created a hostile work environment and interfered with individuals' work performance in violation of Agency policy. The investigation also determined that the employee had engaged in activities that created the appearance of violating ethical standards pertaining to impartiality and preferential treatment, in violation of 5 CFR § 2635.101 (b)(14).

The investigative findings were forwarded to the Office of Personnel Security. The employee retired before disciplinary action was taken.

The case did not meet the requirements for reporting to the Department of Justice.

Senior Executive: Misuse of Subordinates' Time, Unnecessary Official Travel

An OIG investigation determined that a Senior Executive employee requested that subordinates use official time to perform activities other than those required in the performance of official duties or authorized in accordance with law or regulation, in violation of 5 CFR § 2635.705(b). Additionally, the OIG determined that the employee conducted an unnecessary government-funded TDY travel when other means to meet mission requirements were available, in violation of JTR, Chapter 1, paragraph 010202. The employee also used Government property for other than authorized purposes, in violation of 5 CFR §2635.704 and Agent policy; and failed to avoid actions that created the appearance of violation of the law or ethical standards, in violation of 5 CFR §2635.101(b)(14) and Agency policy.

The investigative findings were forwarded to Employee Relations (ER), the Office of Personnel Security, and the Agency Chief of Staff. Disciplinary action against the employee is pending.

The case did not meet the requirements for reporting to the Department of Justice.

GG-15: Time and Attendance

An OIG investigation determined that a GG-15 employee had submitted false and inaccurate timesheets for a shortfall to the Government of 540 hours. The employee's actions violated various Agency policies.

The investigative findings were forwarded to ER, the Office of Personnel Security, and Payroll Entitlements for review and any action deemed appropriate. The employee retired before disciplinary action could be taken.

This case was reported to the Department of Justice in January 2018, because of the possible violations of 18 USC §§ 287 and 1001. The case was not accepted for prosecution.

Whistleblower Reprisal

An OIG investigation found that that three civilian employees and a military officer did not reprise against a subordinate for making protected communications to supervisors and the OIG. The investigation determined that the complainant had made four protected disclosures and thereafter suffered two adverse personnel actions, but there was clear and convincing evidence that the Agency would have taken the adverse actions absent the complainant's protected disclosures. To give full consideration to whether Agency personnel acted improperly, the OIG also considered whether under the circumstances the subjects' actions constituted an "abuse of authority." The OIG did not find sufficient evidence to conclude that conduct by any of the subjects rose to the level of an abuse of authority.

The case did not meet the requirements for reporting to the Department of Justice.

Summary of Additional Investigations

NSA OIG opened 39 investigations and 118 inquiries while closing 30 investigations and 88 inquiries during the reporting period. The new investigations are reviewing various allegations including whistleblower reprisal, ethics violations, misuse of Government resources, and violations of time and attendance and contract billing policies.

Contractor Labor Mischarging

NSA OIG opened three contractor labor mischarging investigations and substantiated three cases that had been opened previously. The substantiated cases resulted in the proposed recoupment of approximately $136,000. Seven investigations remain open.

Time and Attendance Fraud

NSA OIG opened three new investigations into employee time and attendance fraud during the reporting period. Eight investigations that had been opened previously were substantiated during the reporting period, which resulted in the proposed recoupment of approximately $125,000. Two of these employees were terminated from employment, four employees resigned or retired, and action against the remaining two employees is pending. Four investigations remain open.

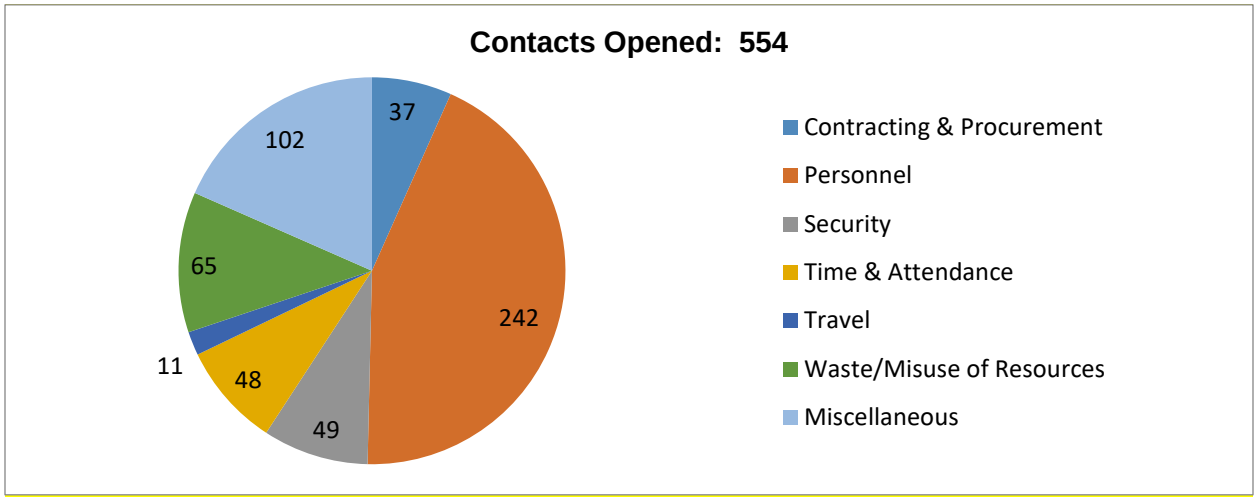
Computer Misuse

NSA OIG opened six new investigations involving allegations of computer misuse. The OIG substantiated two existing cases. The substantiated cases involved employees and were referred to ER for disciplinary action. One case resulted in suspension of the employee's security clearance, pending further action. Disciplinary action against the other employee is pending. Five investigations remain open.

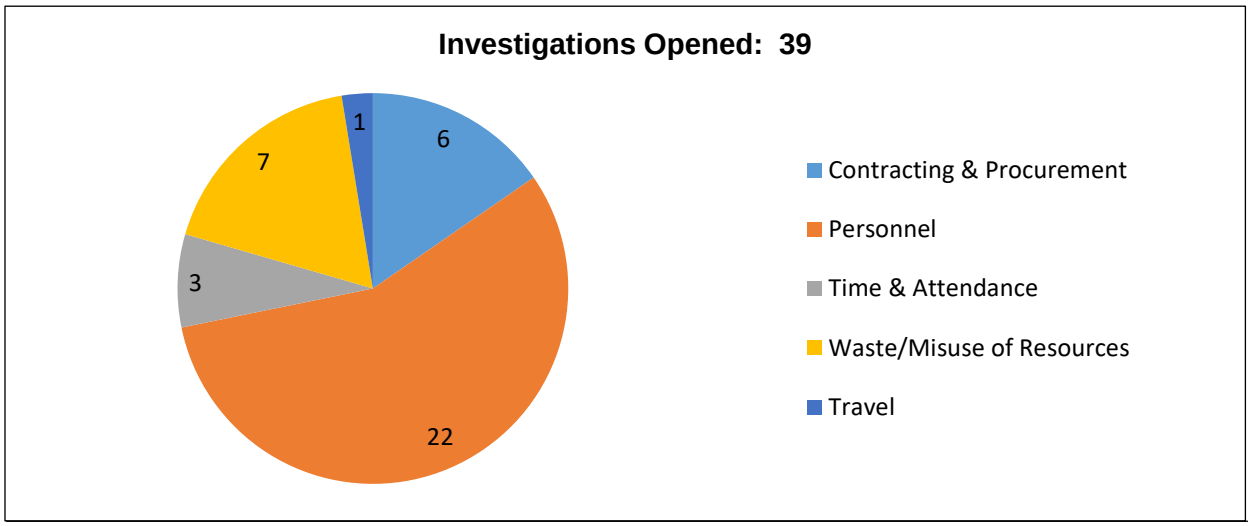
Investigations Summary

Total number of investigative reports issued	30
Total number of persons reported to DOJ for criminal prosecution	10
Total Number of Persons Referred to State and Local Authorities for Criminal Prosecution	0
Total Number of Indictments	0
Data contained in this report and table were obtained from NSA OIG Electronic Information Data Management System (eIDMS))	

Total Hotline Contacts Received



Investigations Opened



Peer Review

The Defense Intelligence Agency (DIA) peer reviewed the NSA OIG Audits Division and issued a report on 25 September 2018 for the 3-year period ended 31 March 2018. DIA issued a rating of "pass", the highest rating possible. The NSA OIG did not peer review another OIG in the reporting period, but is preparing for a peer review of its Inspections Division in February 2019.

Whistleblower Program

Whistleblowers perform an important service to the NSA and the public when they come forward with what they reasonably believe to be evidence of wrongdoing. They should never suffer retaliation or reprisal for doing so. The NSA OIG considers whistleblowers a vital source of information that helps the OIG accomplish its mission of fighting waste, fraud, abuse, and misconduct within the Agency and its programs.

The NSA OIG operates a Hotline, staffed by experienced and knowledgeable managers, to receive and process complaints from inside and outside of the Agency. Individuals may submit complaints anonymously; if the complainant elects to identify him/herself, the OIG will maintain his/her confidentiality unless the complainant consents or disclosure is unavoidable.

The OIG's Investigations Division examines all credible claims of reprisal. Between 1 April 2018 and 30 September 2018, the OIG opened three new reprisal investigations; it also closed one reprisal investigation in which it did not substantiate the reprisal allegations.

Given the importance of whistleblowers to the Agency and the OIG, the OIG has taken steps to help ensure that Agency employees and others are fully informed about whistleblower rights and protections, to include providing guidance to the Agency about the content of the mandatory online training related to whistleblowers. In the prior reporting period, the OIG added to its internal NSA website a prominent whistleblower tab that allows the viewer to access a detailed presentation and FAQs on whistleblower rights and protections. During this period, the OIG added a robust whistleblower rights and protections page to its new public-facing website. It also prepared and disseminated informational cards and posters and notices to employees and locations throughout the enterprise on whistleblower rights and protections, with guidance about how to contact the OIG for additional information. The OIG continues to staff a Whistleblower Coordinator position, which has served as a resource by which Agency employees and others obtain further information about their rights and protections.

Finally, the OIG continues to reach out to non-governmental organizations that are active on whistleblower issues and encourage dialogue so that the OIG can continue to benefit from their important perspective and experience. The IG attended the event at the Capitol Visitors Center in Washington, D.C., in recognition of National Whistleblower Appreciation Day in July 2018, and continues to speak publicly about the importance of whistleblower rights and protections.

Appendix A: Audits, Inspections, Special Studies, and Oversight Memoranda Completed in the Reporting Period

Audits

Mission and Mission Support

- *Audit of the NSA's Emergency Management Program*
- *Quick Reaction Report arising from the Audit of NSA's Accountability of Weapons, Ammunition, and Other Sensitive Assets*

Technology and Cybersecurity

- *Audit of Nuclear Command and Control Systems*
- *Review of the Designation of Individuals to Fill System Security Plan (SSP) Critical Roles*

Financial Audit

- *Audit of NSA's FY2017 Compliance with the Improper Payments Elimination and Recovery Improvement Act*
- *Oversight Review of the Audit of the NSA Restaurant Fund and the NSA Civilian Welfare Fund*

Inspections

Enterprise Inspections

- *Limited Scope Inspection of the Laboratory for Analytic Sciences (LAS)*
- *Limited Scope Inspection of Human Language Technologies (HLT) Contractor Locations*
- *Field Inspection of NSA/CSS Representative to Defense (NCR DEF) and NSA/CSS Representative to Defense Intelligence Agency (NCR DIA), 26 to 27 February 2018*

Joint Inspections

- *Joint Inspectors General Report - NSA Georgia (NSAG), 23 October to 3 November 2017*

Intelligence Oversight

- *Quick Reaction Report arising from the Review of NSA Analyst Compliance with Intelligence Community Directive on Dissemination of Congressional Identities*
- *Advisory Memorandum on NSA's Implementation of Department of Defense (DoD) Training Requirements: Civil Liberties and Privacy Protections and Intelligence Oversight*
- *Quick Reaction Report on the Review of the Ingest Filter of an NSA Data System*
- *Annual FAA Section 702 Report to Congress*
- *Advisory Memorandum on the Routine Practice of Emailing Data Inconsistently with Agency Procedures*
- *Advisory Memorandum on Policies Identifying and Documenting Intelligence Oversight Functions and Responsibilities*
- *Special Study of Data Sharing with Third Party Partners*
- *Special Study of NSA Compliance with Requirements for SIGINT Mission Documentation*
- *Special Study of Compliance with Signals Intelligence Policies in Two Programs*

Appendix B: Audit Reports with Questioned Costs and Funds That Could Be Put to Better Use

Audit Reports with Questioned Costs[1]

Report	No. of Reports	Questioned Costs	Unsupported Costs
For which no management decision had been made by start of reporting period	0	0	0
Issued during reporting period	0	0	0
For which management decision was made during reporting period	0	0	0
Costs disallowed	0	0	0
Costs not disallowed	0	0	0
For which no management decision was made by end of reporting period	0	0	0

Audit Reports with Funds that Could Be Put to Better Use[2]

Report	No. of Reports	Amount
For which no management decision had been made by start of reporting period	0	0
Issued during reporting period	0	0
For which management decision was made during reporting period	0	0
Value of recommendations agreed to by management	0	0
Value of recommendations not agreed to by management	0	0
For which no management decision was made by end of reporting period	0	0

[1] Because OIG recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.

[2] Because OIG recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.

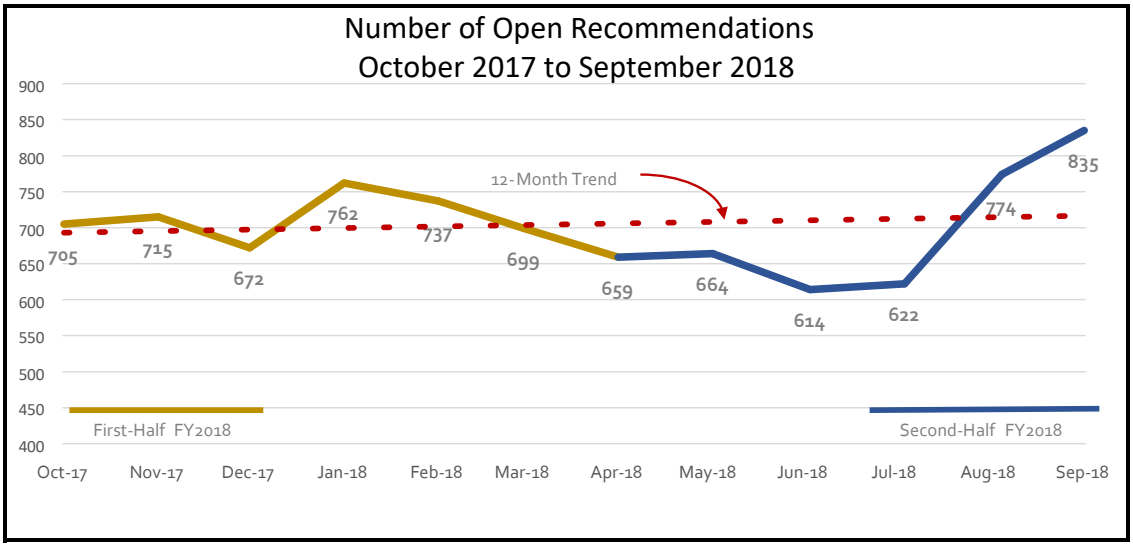
Appendix C: Recommendations Overview

Recommendations Summary

The OIG made 620 recommendations to NSA management in reports and oversight memoranda issued in the second half of FY2018. The Agency closed 257 of these new recommendations, and a total of 415 recommendations during the reporting period.

Outstanding Recommendations[3]

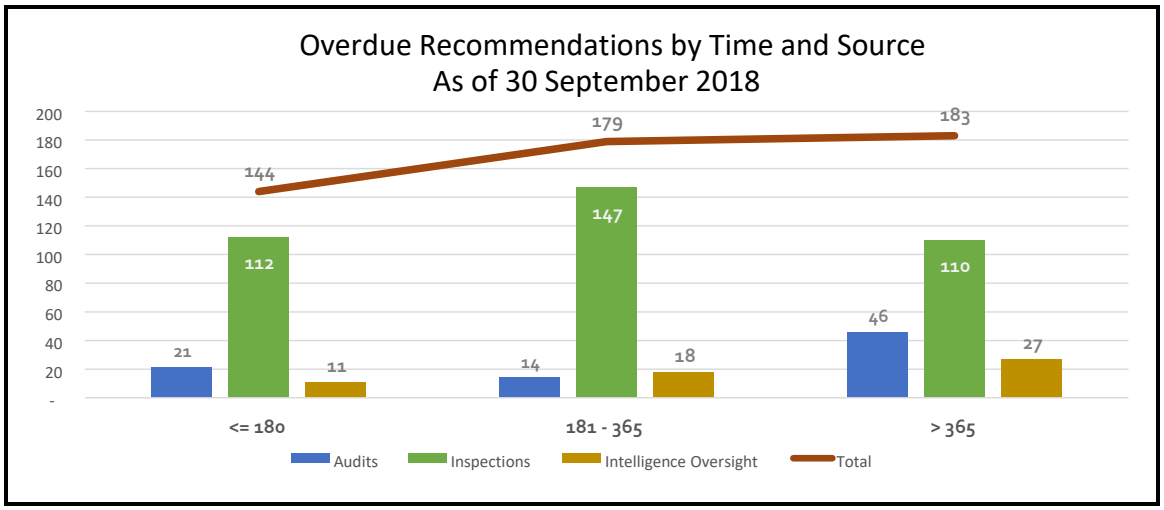
	Audits	Inspections	Intelligence Oversight	Total
Open reports	33	41	24	98
Open recommendations	128	569	138	835
Overdue recommendations	81	369	56	506
Overdue recommendation as % of total open	**63%**	**65%**	**41%**	**61%**



[3] The number of outstanding recommendations increased significantly in the last 2 months of the reporting period following the release of a large inspection report in August and a number of other reports in September 2018. This also resulted in a corresponding decrease in the percentage of outstanding recommendations that were overdue as of the end of the reporting period. A recommendation is overdue when the Agency has not taken action sufficient to warrant closure of the recommendation by the target completion date to which the Agency agreed at the time the report was completed.

Overdue Recommendations Breakdown

Days Past Target Completion Date	Audits	Inspections	Intelligence Oversight	Total	Percent
<= 180	21	112	11	144	29%
181 - 365	14	147	18	179	35%
> 365	46	110	27	183	36%
Totals	**81**	**369**	**56**	**506**	



Significant Outstanding Recommendations - Audits

Audit of NSA Enterprise Solution and Baseline Exception Request Processes

The OIG found in 2011 that Agency organizations and contractors were able to purchase IT items without requisite approvals and recommended that the Agency implement automated compliance controls to address the issue. Although the Agency has now implemented such a solution for software acquisitions, they have not yet funded their identified strategy for implementing automated compliance controls for hardware acquisitions.

The OIG also recommended that the Agency develop contract provisions to require contractors to comply with approved processes, as NSA/CSS Policy 6-1, *Management of NSA/CSS Global Enterprise IT Assets*, 8 September 2008, requires. This recommendation depends on implementation of the previous recommendation before mandatory contract provisions or language for hardware purchases and the processes can be developed and included in applicable contracts.

NSA Export Controls

The U.S. government has a number of programs to protect technologies critical to U.S. national security interests. The OIG found in 2013 that the export control process is ineffective and

recommended that the Agency formally review all Agency export guidance to deconflict guidance and policies, assign a hierarchy to guidance, establish logical links that support hierarchy, and consolidate all responsibilities into NSA/CSS Policy 1-7. The Office of Policy has adjudicated comments received and is awaiting confirmation from the Office of General Counsel that their comments were adjudicated to their satisfaction. The policy office anticipated that the new policy could be completed by 30 September 2018. The OIG will require evidence of a thorough review of all export guidance prior to closing the recommendation.

The OIG also recommended that the Agency track exports authorized to contractors in an automated centralized database. At a minimum, it should include origin and destination, type of export (defense article, service, or technical data), U.S. munitions list category, estimated dollar value, authority, dates of issue and expiration, and contract number. According to NSA's Office of Policy, unique systems must be developed supporting top secret, secret, and unclassified export activities. The Engagement and Policy Directorate has requested a revised completion date of 1 December 2020.

Audit of the Information Assurance Workforce Improvement Program (IAWIP)

DoDD 8570.01-M requires that personnel who perform Information Assurance (IA) duties, regardless of job series or occupational specialty or whether full time or as a collateral duty, maintain a certification corresponding to the highest functions required by their positions. The OIG found in 2014 that NSA's IAWIP should improve the designation and tracking of IAWIP positions within the Agency and recommended that the Agency designate specific positions that meet the IAWIP criteria as outlined in NSA/CSS Policy 6-34, *NSA/CSS Cyberspace Workforce Improvement Program* (CWIP). The action to identify CWIP (formerly IAWIP) positions was recently closed; however, a second recommendation to load CWIP position designations into the Agency's PeopleSoft system remains open at this time.

Significant Outstanding Recommendations – Inspections

Secure the Net / Secure the Enterprise / Insider Threat

Inspection teams find many instances of non-compliance with rules and regulations designed to protect computer networks, systems, and data. Significant outstanding inspection findings include:

- System Security Plans are often inaccurate and/or incomplete;
- Two-person access (TPA) controls not properly implemented for data centers and equipment rooms; and,
- Removable media not properly scanned for viruses.

Continuity of Operations Planning (COOP)

There are significant outstanding recommendations regarding the Agency's continuity of operations planning (COOP). Deficiencies in this area could result in significant impact on mission support to the warfighters and policy makers that rely on NSA intelligence.

Emergency Management Plan

Many subordinate organizations inspected do not have a mature, well exercised Emergency Management Plan or Emergency Action Plan for the protection of personnel and the site. These plans encompass situations such as an active shooter, natural disaster, and terrorist threat.

Significant Outstanding Recommendations – Intelligence Oversight

Special Study Assessing Management Controls over FAA §702

Obligation to Review (OTR) alerts are part of NSA's system of controls designed to provide reasonable assurance of compliance with Section 702 of the FISA Amendments Act of 2008 and the targeting and minimization procedures that establish requirements for the Agency's use of the authority. OTR alerts support compliance with targeting requirements and are generated when target communications are not reviewed with the frequency required by NSA internal guidance. As reported during the 2012 study, the OTR system is operational for some FAA §702 selectors. However, the OIG's recommendation to implement OTR for certain FAA §702 selectors will not be resolved until NSA's system receives the associated data. The current Agency estimate to implement the required corrective actions is November 2018.

Special Study of the Protection of U.S. Person Information during Analytic Processing

The Agency has a collection source system of record authorized to store unevaluated and unminimized SIGINT data from multiple sources. Although this system is scheduled to be decommissioned, guidance on the disposition of retained data in the system is needed before the data can be transitioned to the new mission data repository. The OIG recommended that steps be taken to bring the system into full compliance with all retention authorities. To do so, the OIG further recommended that the NSA Office of General Counsel must provide guidance on legal considerations needed to identify data from this system that must be retained pursuant to preservation orders, and the Operations Directorate must provide guidance on mission considerations needed to identify the system data that must be retained for mission purposes. To date, NSA management has not resolved these recommendations.

Report on the Special Study of an Office of Oversight and Compliance Mission Compliance Program

The OIG reviewed an Office of Oversight and Compliance that is responsible for implementing guidelines, regulations, and directives that govern the United States SIGINT System's (USSS) acquisition, processing, retention, and dissemination of SIGINT. The OIG found that, in certain respects, the office does not fully perform its oversight responsibilities over the entire USSS and does not fully execute its mission to perform proactive and comprehensive verification of USSS activities. The OIG recommended that the office:

- publish its authority to establish SIGINT compliance procedures and priorities for the entire USSS and its oversight role of SIGINT activities across the entire USSS;
- implement a process to periodically review the Intelligent Oversight programs of organizations and agencies that access unevaluated and unminimized SIGINT or conduct mission under DIRNSA authority to ensure that their activities conform to SIGINT policies and procedures;
- develop a strategy for executing periodic verification of E.O. 12333 procedures that comprehensively addresses all stages of the SIGINT production cycle;
- develop and publish consistent and clear incident reporting criteria in accordance with the SIGINT Director's oversight responsibilities to ensure completeness, accuracy, and timeliness of USSS incident reporting;
- analyze all USSS compliance incidents to identify trends and evaluate compliance risk; and
- recommend corrective actions to resolve all SIGINT compliance incidents, including cross-mission and cross-agency incidents, and ensure implementation of these recommendations.

Management agreed to complete these actions prior to NSA21, but has requested extensions to complete these actions by 31 December 2018.

Report on a Certain Integrated Network

The OIG conducted a study to assess the handling and protection of SIGINT data in a network owned and maintained by another U.S. Government entity (USG) that was used, among other things, to transfer SIGINT data for software design and testing. The OIG found that NSA had no formal process for documenting approvals for government sites and laboratories to connect to or disconnect from the network. To address this concern, as well as similar cases, the OIG recommended that NSA implement a formal process for timely notification to the other USG entity of changes that affect a site's authority to connect to data flows of raw SIGINT on the USG entity's networks. The target completion date was February 2013. To date, NSA management, unable to identify ownership for the recommendation, has not resolved this recommendation.