Office of the Inspector General
National Security Agency

Semi-Annual Report to Congress

1 April 2019 to 30 September 2019

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/CSS Office of the Inspector General (OIG) conducts independent oversight that promotes Agency respect for Constitutional rights, adherence to laws, rules, and regulations, and the wise use of public resources. Through investigations and reviews, we detect and deter waste, fraud, abuse, and misconduct and promote the economy, the efficiency, and the effectiveness of Agency operations.

AUDIT

The Audit Division comprises three sections: Cybersecurity and Technology, Financial Audits, and Mission and Mission Support. The Division's audits and evaluations examine the economy, the efficiency, and the effectiveness of NSA programs and operations; assess Agency compliance with laws, policies, and regulations; review the operation of internal information technology and controls; and determine whether the Agency's financial statements and other fiscal reporting are fairly and accurately presented. Audits are conducted in accordance with auditing standards established by the Comptroller General of the United States.

INSPECTIONS

The Inspections Division performs organizational inspections and functional evaluations to assess adherence to regulations and policies and to promote the effective, efficient, and economical management of an organization, site, or function. OIG inspection reports recommend improvements and identify best practices across a broad range of topics, to include mission operations, security, facilities, and information technology systems. The Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other Intelligence Community (IC) entities to jointly inspect consolidated cryptologic facilities. Inspections and evaluations are conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) "Quality Standards for Inspection and Evaluation."

INTELLIGENCE OVERSIGHT

The Intelligence Oversight (IO) Division conducts evaluations that examine a wide range of NSA intelligence and intelligence-related programs and activities to assess if they are conducted efficiently and effectively, and are in compliance with federal law, executive orders and directives, and IC, DoD, and NSA policies, and appropriately protect civil liberties and individual privacy. The IO function is grounded in Executive Order 12333, which establishes broad principles for IC activities. IO evaluations are conducted in accordance with the CIGIE "Quality Standards for Inspection and Evaluation."

INVESTIGATIONS

The Investigations Division examines allegations of waste, fraud, abuse, and misconduct by NSA affiliates or involving NSA programs or operations. The investigations are based on submissions made through the classified or unclassified OIG Hotline, as well as information uncovered during OIG audits, inspections, and evaluations, and referrals from other internal and external entities. Investigations are conducted in accordance with the CIGIE "Quality Standards for Investigations."

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 and ensure the fairness and accuracy of the unclassified version of the report. 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 pleased to present the Semiannual Report to Congress (SAR) of the National Security Agency/Central Security Service (NSA) Office of the Inspector General (OIG) for the period 1 April 2019 through 30 September 2019. The SAR describes a wide range of audits, evaluations, inspections, and investigations completed and ongoing during this reporting period that relate to many aspects of the work of the NSA, all with the core purpose of furthering the integrity and the efficiency of the critical operations that are conducted here.

During the reporting period, the OIG issued 14 reports or other oversight memoranda containing a total of 232 recommendations for improvement. A number of these recommendations were closed by the Agency by the time the report or memorandum was issued, while actions in response to many others will take more time to complete. During this period, the Agency revised its procedures and structures to help ensure appropriate coordination among Agency stakeholders in responding to OIG reports and recommendations. The total number of open recommendations decreased 14 percent from 596 at the beginning of the reporting period to 513 at the end, while the number of those recommendations that were overdue (in that Agency action had extended beyond the target completion date) went down 29 percent from 427 to 303. Those overdue recommendations represented 59 percent of the total number of open recommendations as of 30 September 2019, reflecting the lowest percentage of open recommendations that were overdue over the past four SARs. This reflects significant progress, but there is still substantial work to be done, including on the 173 recommendations that were overdue by more than a year at the end of the reporting period. The NSA Director has emphasized the importance of taking action to address the issues identified by the OIG, and my office will continue to make every effort to promote such efforts in order to make our work as impactful as possible in furthering the economy, the efficiency, and the effectiveness of Agency operations.

The reports and reviews issued by the OIG during this reporting period address a broad spectrum of Agency programs and operations. These include reviews in which we identified significant issues and made recommendations for improvement in areas ranging from the Agency's controls to ensure proper integration of personnel from Second Party, or "Five Eyes," countries to the Agency's management of its weapons and other sensitive assets, to its compliance with the rules related to the handling of Congressional identity information in its intelligence reporting. The OIG's oversight also includes inquiries and investigations into misconduct by Agency affiliates and related to its programs and operations. During the 6 months covered by this SAR, the OIG Investigations Division fielded 558 new contacts (an increase of over a hundred from the prior reporting period), resulting in the initiation of 75 inquiries and 37 investigations (both substantially increased from the prior period as well). We also referred 33 cases involving Agency personnel to NSA Employee Relations for potential disciplinary action, and the Agency took such actions against 29 individuals during this period based on misconduct substantiated by the OIG. During this period, we saw two Agency contractors enter guilty pleas in federal court to criminal conduct in cases investigated by the OIG, and we have several other criminal matters pending with the U.S. Attorney's Office. And during the reporting period, we substantially expanded our assessment of the Top Management and Performance Challenges faced by the Agency that is statutorily required to be included in the Agency Financial Report, working to draw lessons from the past and look

forward to the issues that we believe the Agency must address in the future. It has been a busy 6 months at the OIG.

One area I want to highlight that remains of critical importance for this OIG, and all OIGs, is whistleblower rights and protections. As I have often said, whistleblowers perform a valuable service to the Agency and the public by coming forward when they see something they believe is wrong, and they should never suffer reprisal for doing so. Here at the NSA OIG, we have continued to emphasize the importance of whistleblower rights and protections as essential to our ability to obtain information necessary to conduct informed oversight. On a daily basis, we receive valuable information from people on the front lines throughout the extended enterprise who come forward with information that they reasonably believe evidences waste, fraud, abuse, or misconduct of all types. We depend on this input to initiate many of our investigations, and it also often is valuable in informing our audits, evaluations, and other oversight work. Because of the importance of whistleblower protection, my office continues to prioritize investigations into allegations of reprisal against whistleblowers, and we have enhanced our procedures to ensure the accuracy of our conclusions and to make sure that people who come forward know that they have every opportunity to seek relief through this office. We continue to expand the information about whistleblower rights and protections on both our internal and our external website, https://oig.nsa.gov, including a video that we posted this summer with the NSA Director in which we join together to encourage NSA employees and affiliates to come forward and "make the call."

The NSA OIG functions as part of the larger IG Community, and in that regard, we are active in the operations of the Council of the Inspectors General on Integrity and Efficiency (CIGIE). During the reporting period, I was pleased to assume the position of Vice Chair of the CIGIE Technology Committee, and am particularly excited to Chair the newly created Emerging Technologies Subcommittee that is exploring the use of artificial intelligence and other new and developing technologies across the government, how OIGs can best provide meaningful oversight over such activities, and how we can employ such capabilities to further our own oversight efforts. Our office also is active in a number of other important CIGIE Committees, as well as the collaborative efforts of the Intelligence Community Inspectors General Forum, and we will continue to look for opportunities to partner with our fellow OIGs to address cross-cutting issues and develop best practices to further our oversight work.

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. Agency management agreed with all OIG recommendations during the reporting period.

In sum, this is a complicated, multi-faceted Agency doing important, complex work, and we at the OIG have a dedicated team of investigators, inspectors, evaluators, and auditors working together to provide independent oversight that is impactful in promoting positive change.

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, Cybersecurity
Director, National Security Operations Center
Director, Office of Civil Liberties, Privacy, and Transparency
General Counsel

Contents

A Message from the Inspector General ..... **iii**
Index of Reporting Requirements ..... **vii**
OIG Executive Summary **1**
Significant Problems, Abuses, and Deficiencies and Other Significant Reports **3**
Summary of Reports for Which No Management Decision Was Made 5
Significant Revised Management Decisions 5
Management Decision Disagreements 5
Audits **6**
Completed Audits 6
Ongoing Audits 8
Inspections **10**
Completed Inspection Reports 10
Ongoing Inspection Reports 12
Intelligence Oversight **13**
Completed Special Studies 13
Ongoing Special Studies 14
Investigations **16**
Prosecutions 16
Agency Referrals 16
OIG Hotline Activity 17
Significant Investigations 17
Summary of Additional Investigations 20
Peer Review **23**
Whistleblower Program **24**
Appendix A: Audits, Inspections, Special Studies, and Oversight Memoranda **25**
Appendix B: Questioned Costs and Funds That Could Be Put to Better Use **27**
Appendix C: Recommendations Overview **28**

Index of Reporting Requirements

§5(a)(1)	Significant problems, abuses, and deficiencies	3–5
§5(a)(2)	Recommendations for corrective action	3–5
§5(a)(3)	Significant outstanding recommendations	29-31
§5(a)(4)	Matters referred to prosecutorial authorities	16
§5(a)(5)	Information or assistance refused	iv
§5(a)(6)	List of audit, inspection, and evaluation reports	25-26
§5(a)(7)	Summary of particularly significant reports	1–2
§5(a)(8)	Audit reports with questioned costs	27
§5(a)(9)	Audit reports with funds that could be put to better use	27
§5(a)(10)	Summary of reports for which no management decision was made	5
§5(a)(11)	Significant revised management decisions	5
§5(a)(12)	Management decision disagreements	5
§5(a)(13)	Information described under 05(b) of FFMIA of 1996	N/A
§5(a)(14)	Results of peer review conducted of NSA OIG	23
§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	23
§5(a)(17)	Statistical tables of investigations	21-22
§5(a)(18)	Description of Metrics used in statistical tables of investigations	22
§5(a)(19)	Reports concerning investigations of Seniors	17-19
§5(a)(20)	Whistleblower Retaliation	19-20
§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	28-29
* IG Act of 1978, as amended, including the IG Empowerment Act of 2016.		

This page intentionally left blank.

OIG Executive Summary

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

Audit Division

The Audit Division of the NSA OIG is divided into three branches – Mission and Mission Support, Cybersecurity and Technology, and Financial Audit. During this reporting period, the Audit Division issued a total of 8 reports containing 67 recommendations to improve Agency operations.

The Mission and Mission Support Branch performed an audit of *NSA's Internal Controls Over Second Party Integrees*. In this audit, we identified what the OIG determined to be a risk of improperly integrating Second Party, or Five Eyes personnel into the workforce, and potentially impacting relationships with these critical partners. We also issued a report on the *Agency's Temporary Medical Leave Assistance Program,* which plays a critical role in offering leave assistance to NSA/CSS employees during a time of medical crisis. Our audit identified the risk of ineffective management potentially impacting the overall Leave Bank balance and inconsistent decisions for approving and disapproving cases. Additionally, we completed an audit of *NSA's Accountability for Weapons, Ammunition, and Other Sensitive Assets*. The audit revealed that NSA did not properly report that since 2012 deployers to or from hostile areas lost 5 and misplaced but subsequently recovered 7 firearms. We also identified other issues with inventory, facilities, and insufficient controls to protect tactical gear. The OIG made 27 recommendations in this audit to the Agency to assist it in improving its operations in this critical area.

The Cybersecurity and Technology Branch performed an audit to determine whether the NSA's Corporate Authorization Service (CASPORT), which provides authorization attributes and access control services across the Agency, is secure, resilient, and operationally effective. We made multiple recommendations, all of which were completed by the Agency. We also issued a report on *CIO Authorities*, which contained a detailed high-level assessment of Chief Information Officer (CIO) responsibilities established by Congress and the Office of Management and Budget. Our audit revealed that the Agency did not have an integrated strategy for implementing CIO responsibilities, and that the CIO here lacked clearly defined and communicated authorities and responsibilities.

Inspections Division

The OIG issued four inspection reports during this reporting period, and conducted 7 new inspections, all at field sites. The Agency and all sites fully cooperated with our work, which resulted in a wide range of recommendations for improvements in operations. We also identified a number of commendable or best practices being utilized at the inspected sites that we believe could be replicated elsewhere. During this period, the Inspections Division received and responded to the results of the Peer Review conducted of our work in the prior reporting period by the NGA, DIA, CIA and IC IGs.

Intelligence Oversight Division

During this reporting period, the OIG's Intelligence Oversight Division issued one advisory memorandum and one report on a special study. The advisory memorandum assessed NSA analysts' adherence to Intelligence Community Directive (ICD) 112, *Congressional Notification*, 29 June 2017, and its Annex A, "Dissemination of Congressional Identity Information," 19 January 2017, specifically including testing that identified a number of compliance issues with the requirements regarding dissemination of congressional identity information in the Agency's intelligence reporting. The special study evaluated the efficiency and effectiveness of NSA's procedures used to ensure that the Agency's Endpoint & Forensics (E&F) mission complies with legal authorities, directives, and policies that protect U.S. person privacy. In total, we made 14 recommendations in these two reports to assist the Agency in improving its operations and to increase compliance with requirements for protecting civil liberties and individual privacy in its intelligence activities.

Investigations Division

During this reporting period, the Investigations Division received and processed 558 contacts, which resulted in the initiation of 75 inquiries and 37 investigations. Four new investigations involved allegations of whistleblower reprisal, one involved allegations of ethics violations, one involved allegations of sexual harassment, and one involved allegations of nepotism. We closed 27 investigations and 72 inquiries during the reporting period, resulting in the proposed recoupment to the Agency of over $63,000 from employees and more than $540,000 from contractors. As a result of OIG investigations, disciplinary actions ranging from reprimands to termination were taken against 29 employees. Two individuals entered guilty pleas in federal court based on investigations conducted by the OIG, and several other cases that we referred to the U.S. Attorney for the District of Maryland are pending resolution.

Whistleblower Program

Whistleblower rights and protections continue to be a seminal priority for our office. During this period, we enhanced our procedures for handling reprisal cases, released a new video in which the Director joins with the IG to encourage the reporting of suspected wrongdoing, and completed our work on a new on-line training program that we anticipate will be released in the coming reporting period.

Significant Problems, Abuses, and Deficiencies and Other Particularly 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 Director, NSA, and Congress pursuant to Section 5(d) of the Inspector General Act. However, the following reviews revealed significant problems, abuses, or deficiencies, or were otherwise particularly significant reports as provided in Section 5(a) of the Act:

Review of National Security Agency/Central Security Service Analyst Compliance with Intelligence Community Directive on Dissemination of Congressional Identities

The OIG conducted this review to assess NSA analysts' adherence to Intelligence Community Directive (ICD) 112, *Congressional Notification*, 29 June 2017, and its Annex A, "Dissemination of Congressional Identity Information," 19 January 2017. The OIG's testing revealed deficiencies in the handing of congressional identity information in NSA reports. The key findings are as follows:

- The failure to follow NSA guidance and minimization procedures, and errors in the application of NSA guidance and procedures were contributing factors for NSA reports being noncompliant or potentially noncompliant, in some instances, with ICD 112, Annex A, requirements for disseminating Congressional identity information.
- In some instances, NSA policy, guidance, and procedures do not provide adequate direction for analysts to properly minimize congressional identity information per ICD 112, Annex A. The failure to address the ICD 112, Annex A, minimization requirements unique to congressional identity information in NSA policy, guidance, and procedures may result in identities being mishandled and/or NSA being noncompliant with ICD 112, Annex A. Additionally, inconsistency among NSA policy, guidance and procedures as well as with ICD 112, Annex A may result in NSA reports being noncompliant with ICD 112, Annex A.
- There were only nominal references to ICD 112, Annex A, and analysts' responsibilities for dissemination of congressional identity information in available training materials, and no training materials specifically addressed ICD 112, Annex A.

This Advisory Memorandum followed a Quick Reaction Report that the OIG previously issued and reported on in a prior SAR regarding 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, and procedures. Those findings were promptly addressed by the Agency and, in the current report, the OIG made eight additional recommendations to address the issues that we identified in this area.

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

Weapons, ammunition, and other sensitive assets are necessary to ensuring the health and safety of NSA affiliates throughout the Enterprise. The audit revealed the following primary concerns:

- Since 2012, NSA deployers to or from hostile areas have lost five firearms, and misplaced but subsequently recovered seven additional firearms while traveling. However, NSA did not report these instances internally or externally, as required, including not disclosing them to the OIG in a timely fashion during the audit.
- NSA's accountability for weapons is inaccurate and inefficient. Databases maintained to account for weapons were not up to date, and we found that more than 100 firearms had inaccurate locations in the system of record for 11 months.
- The types of weapons storage facilities across the enterprise were not well defined and, therefore, it is unclear which should comply with Department of Defense (DoD) regulations and NSA policies for administrative and physical controls over firearms.
- NSA does not have sufficient controls in place to protect tactical gear from unauthorized use, theft, or loss. We found that the Agency has not conducted an inventory of tactical gear since March 2016, and could not explain inventory discrepancies between physical counts and inventory records.

The findings identified by the OIG in this review highlight a risk that weapons or other sensitive assets could be misused, which could cause or facilitate a potentially dangerous situation. The OIG made 27 recommendations to assist NSA in addressing the risks identified in this audit report.

Audit of CIO Authorities

The OIG conducted this audit to determine whether the Chief Information Officer (CIO) function has been implemented at the NSA in compliance with the requirements of the Clinger-Cohen Act of 1996 (CCA) and Office of Management and Budget (OMB) M-11-29, *Chief Information Officer Authorities,* 8 August 2011, for providing oversight and management of information technology (IT). Specifically, the OIG completed high-level assessments of three main areas: Governance/IT Investment and Budget Management; Program Management, including Program Workforce Management; and Information Security. We also evaluated the Agency's establishment and implementation of an Enterprise IT Architecture program, as well as the CIO's placement within NSA's organizational and management structure.

The OIG found that the Agency and CIO have made substantial progress in establishing and implementing the full scope of CIO authorities, but that additional actions are required for the CIO to more effectively meet CCA and OMB M-11-29 obligations and ensure the CIO has the requisite oversight of and decision rights for all Agency IT. To address this, the OIG recommended that the CIO develop and implement an integrated strategy to address each of these highly interrelated component areas of IT. The OIG also found that the Agency's CIO role is ambiguous, without clearly defined authorities and responsibilities. The OIG attributed this to a number of factors, including dual hatting the functions of the CIO with those of an NSA Directorate, a lack of documentation for the delegation of authorities, failure to include the CIO role in Agency

organization charts, and Agency communications that reinforced the CIO's authorities primarily for the information security component of CCA and OMB M-11-29.

The issues identified in this audit increase the risk that the Agency may continue to not fully meet the obligations of CCA and OMB M-11-29 and, therefore, may not be maximizing its effectiveness and efficiency in designing, investing in, acquiring, managing, and maintaining the full range of its IT. The OIG made a total of four recommendations to improve Agency governance in this area -- the Agency has taken action sufficient to close one, and additional actions planned by management meet the intent of the remaining three recommendations.

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 decisions disagreements were published.

Audits

Audit Reports and Oversight Memoranda Completed in the Reporting Period

Audit of NSA's Internal Controls Over Second Party Integrees

The concept of exchanging personnel and information with NSA's Five Eyes (FVEY) partners dates back to a 1946 United Kingdom – United States Agreement. According to NSA policy, Second Party integration should be beneficial to the United States Cryptologic System mission, strengthen relationships with Second Party Nations, and be consistent with U.S. Government law, policy, strategy, and interest. The OIG conducted this audit to determine whether the internal controls over the integration of Second Party personnel into the NSA workforce are operating effectively and efficiently. Our audit revealed that because NSA policy did not assign overall responsibility to one organization, there were no standard processes in place to establish and staff Integree positions, and the Agency cannot account for all Integree positions or all Integrees across the enterprise. Additionally, we found that not all Agency personnel had an understanding of Second Party Partner relationships; as a result, some Integrees reported having experiences that are not beneficial to the mission or the Second Party relationship. The Agency agreed with the OIG's findings and recommendations, but not with the OIG's assessment of the resulting risk of improper integration. The OIG made 13 recommendations to assist NSA in addressing the deficiencies identified in this audit.

Audit of NSA's Fiscal Year 2018 Compliance with the Improper Payments Elimination and Recovery Improvement Act of 2012

The objective of the audit was to determine whether the Agency complied with the Improper Payments Elimination and Recovery Improvement Act using the OIG procedures in the Office of Management and Budget Circular A-123 Appendix C, *Requirements for Payment Integrity Improvement*, 26 June 2018. The audit found that in FY2018 the Agency complied with IPERIA. However, we found that the Agency can improve its processes and procedures for estimating its improper payment rate and for reporting its IPERIA results. The report resulted in five recommendations to improve procedures related to documentation requirements, testing reconciliations, and the Agency Financial Report (AFR) review process.

Audit of NSA's Corporate Authorization Service (CASPORT)

The overall objective of the audit was 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. We found that the Agency has widely implemented CASPORT as a mandated authorization service, and we made 12 recommendations to assist NSA in ensuring that CASPORT functions as intended and required to support timely and reliable access to Agency systems. All recommendations have been closed based on Agency action sufficient to address their intent.

Audit of the Temporary Medical Leave Assistance Program (TMLAP)

The Temporary Medical Leave Assistance Program plays a critical role in offering leave assistance to NSA/CSS employees during a time of medical crisis. The Agency has an obligation to employees for ensuring that Leave Bank hours are adequately monitored and appropriate controls

are in place so that participants can use the program when needed. The OIG conducted this audit because of the important role of this program at the Agency. Our audit revealed the program generally is successful in providing needed support to employees, but the findings identified the risk of ineffective management of the Leave Bank Program. We found that the program did not have finalized documented Standard Operating Procedures, which has led to unreliable data, Leave Bank cases not being closed promptly, and the absence of approved guidance for determining annual dues. Additionally, the OIG found an increased risk because Leave Bank decisions generally are not subject to an independent review. Finally, we found the Leave Bank balance was not reconciled; therefore, the Agency cannot be certain the reported balance is correct. The OIG made four recommendations to assist NSA in addressing the risks identified.

FY2019 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

We contracted with an independent public accounting firm to perform an examination of NSA's description of its system supporting the performance of financial processing services on behalf of another U.S. Government organization for the period of October 1, 2018, through June 30, 2019, and the suitability of the design and the operating effectiveness of controls to achieve the related control objectives stated in the description. The examination noted certain exceptions, including with the design and operating effectiveness of controls, which resulted in a qualified opinion.

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

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

Review of the Agency's Nuclear Weapons Personnel Reliability Program

The purpose of the Nuclear Weapons Personnel Reliability Program (NWPRP) is to ensure that all NSA personnel who perform duties associated with nuclear weapons meet the highest possible standards of individual reliability in accordance with Department of Defense guidance and NSA Policy. The OIG conducted this review to determine whether NWPRP complied with the DoD guidance and Agency policies and to determine whether corrective actions had been implemented to satisfy recommendations from previous audits. Our review revealed that the Agency's NWPRP has a strong control environment and continues to improve operations. The OIG made two recommendations to improve administration of the program. The Agency agreed and took action to close the recommendations.

Audit of CIO Authorities

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

Ongoing Audits

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 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 Enterprise-wide Space Utilization

The overall objective of the audit is to assess whether effective, efficient, and economical processes and controls for issuing, managing, and accounting for space exist across the NSA Enterprise.

Audit of NSA's FY2019 Financial Statements

The overall objective of the audit is to determine whether the Agency's financial statements are free from material misstatement. The audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. It also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. The audit will consider and report on internal control over financial reporting and compliance with certain laws, regulations and other matters for the fiscal year ending 30 September 2019.

Evaluation of the NSA/CSS Implementation of the Federal Information Security Modernization Act of 2014 (FISMA)

The overall objective of the evaluation is to review the Agency's information security program and practices. In accordance with the 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 the Agency's Retention Incentive Program

The overall objective of the audit is to assess the economy and effectiveness of the NSA's retention incentive program, and to determine whether the Agency has adequate internal controls to ensure that retention incentives are awarded in accordance with applicable policy and procedures.

Audit of the Agency's Management of Fit-Up Costs and Allocation of Shared Operating Expenses

The overall objective of the audit is to assess the economy and effectiveness of the NSA's fit-up process, and to determine whether shared operating expenses are properly allocated to other agencies occupying NSA buildings. "Fit-up" is defined by the Agency as the phase in which a complete and usable facility is tailored to specific occupant needs. It occurs after construction completion, but prior to occupancy.

Audit of Cost-Reimbursement Contracts

The overall objective of the audit is to determine whether the Agency has effective and efficient internal controls over cost-reimbursement contract expenses.

Audit of Tactical Serialized Reporting

In this audit, the OIG is examining whether the Agency's tactical serialized reporting is being used effectively and efficiently and is in compliance with applicable laws, regulations, policies, and best practices. Tactical serialized reporting is an optional reporting mechanism that may be used to disseminate SIGINT in support of tactical operations.

Oversight Review of NSA's Restaurant Fund and Civilian Welfare Fund

The overall objective of the oversight review is to determine whether the audits performed by an independent public accounting firm of the financial statements of the Restaurant Fund and Civilian Welfare Fund for the years ended 30 September 2017 and 2018 were performed in accordance with Government Auditing Standards and the terms of the contract for nonappropriated fund instrumentalities audit services.

Audit of the Agency's Parking and Transportation Initiatives

The purpose of this audit is to assess the economy, efficiency, and effectiveness of NSA parking and transportation initiatives, and to determine if they are in compliance with applicable laws, regulations, policies, and best practices.

Inspections

Inspection Reports and Memoranda Completed in the Reporting Period

Special Study on the Assignment of Military Affiliates to NSA

The Inspections Division performed this study in an effort to identify possible root causes for concerns raised during OIG inspections of NSA Georgia, NSA Texas, AMOC, and NSA Hawaii. During each of these inspections, the OIG heard about the number of military affiliates "outside the fence" and the perception at those sites that there was a significant delay between when assigned military affiliates arrived at NSA facilities and when they were granted access to those facilities and NSA information and mission, resulting in substantial inefficiencies for the Agency.

The OIG identified three primary impediments to military affiliates obtaining access to NSA:

- The military services are assigning some military affiliates to NSA before they have a favorably adjudicated single-scope background investigation and polygraph examination as required by Department of Defense Instruction 5210.45.
- The process for providing security paperwork to NSA is manual and time consuming.
- Military affiliates who transfer from one NSA site to another often experience challenges in obtaining access to facilities and information at their new site.

The OIG made three recommendations to assist the Agency in addressing these issues and enabling more efficient utilization of these critical personnel.

Quick Reaction Report Arising from the Inspection of an Overseas Location

While conducting an inspection at an overseas location, the OIG discovered that certain information technology (IT) equipment in use there had not been properly certified for use as required in their Interim Certification Letter, potentially putting NSA mission and information at risk.

The OIG issued a Quick Reaction Report in which it recommended that NSA conduct a survey of other sites and promptly replace any other improperly certified equipment as well as establishing and promulgating new processes to ensure this type of equipment is acquired only from properly certified vendors and only after acquisition security fully vets the required purchase.

Inspection of NSA/CSS Representative (NCR) and Cryptologic Services Group (CSG) to U.S. Pacific Command (USPACOM)

The OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the NCR to U.S. Pacific Command (USPACOM, now known as USINDOPACOM). The OIG reviewed pertinent documents, support agreements, policies, regulations, and intelligence oversight data. Inspectors conducted interviews with members of the NCR USPACOM workforce, as well as off-site interviews with outgoing and incoming leadership.

Although successful in accomplishing its mission and recognized by external customers for excellent support on regional issues, NCR USPACOM faces numerous challenges. The OIG made

48 recommendations and 7 observations to assist the NCR USPACOM and the Agency in addressing the findings identified during the inspection. These included concerns with a lack of standardized, definitive guidance on how military members should balance their time between NSA mission and service component requirements, the need for updates to several intelligence oversight documents, poor information technology support, and safety and security risks posed by issues related to facilities and other matters addressed in the report.

Joint Inspectors General Inspection Report – National Security Agency Hawaii (NSAH)

The NSA, Army Intelligence and Security Command, U.S. Fleet Cyber Command, and 25th Air Force OIGs Joint Inspection team evaluated the overall climate and the compliance, effectiveness, and efficiency of the National Security Agency Hawaii (NSAH) Cryptologic Center. The inspection included 21 focus groups, participants of which represented all segments of the military and civilian government workforce at the NSAH. In addition, the OIG team reviewed pertinent documents, support agreements, policies, and regulations. Further input came from NSAH employee responses to the May 2017 and 2018 Intelligence Community Employee Climate Surveys. The OIG interviewed members of the workforce and observed site operations and functions in mission operations; intelligence oversight; infrastructure technology and systems; resource programs; safety, security, facilities, continuity of operations and emergency management; and training. The OIG also interviewed senior site leaders and senior NSA leaders responsible for NSAH missions.

Overall, we found site personnel were encouraged by the efforts of the recently arrived senior leaders, and we noted best practices in welcoming new arrivals to site and physical and account security practices implemented to mitigate unintended exposure to sensitive information. However, the OIG also identified a number of concerns for NSAH, including property control concerns, issues related to facility safety and security, and issues with configuration management. The OIG made a total of 90 recommendations to assist the NSAH and the Agency in addressing the findings identified during the inspection. In addition, the OIG provided three observations and noted four commendable practices identified during this inspection.

Ongoing Inspection Work

The NSA, Army Intelligence and Security Command, U.S. Fleet Cyber Command, and 25th Air Force OIGs jointly conducted an inspection at RAF Menwith Hill (RAFMH) that evaluated the overall climate and the compliance, effectiveness, and efficiency of the organization.

The NSA OIG conducted three inspections during this reporting period that evaluated the overall climate and the compliance, effectiveness, and efficiency of the following organizations:

- Special United States Liaison Office, London (SUSLOL)
- NSA Cryptologic Representative, US AFRICOM
- NSA Cryptologic Representative, US EUCOM

During each inspection, the OIG reviewed pertinent documents, support agreements, policies, regulations, and intelligence oversight data. Inspectors conducted interviews with members of the respective organization's workforce and mission leaders, and where appropriate, with representatives from their customers.

Intelligence Oversight

Special Studies and Oversight Memoranda Completed in the Reporting Period

Review of National Security Agency/Central Security Service Analyst Compliance with Intelligence Community Directive on Dissemination of Congressional Identities

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

Special Study of the Endpoint and Forensics Mission

The objective of this study was to evaluate the efficiency and effectiveness of NSA's procedures used to ensure the Endpoint & Forensics (E&F) mission complies with legal authorities, directives, and policies that protect U.S. person privacy.

While a comprehensive analysis of E&F's output and the overall effectiveness of its work was beyond the scope of this review, information obtained by the OIG through interviews reflects that E&F has been a positive contributor in both the document and media exploitation (DOMEX) community and internal to NSA. However, the OIG's study revealed the following deficiencies that have the potential to impact the efficiency and effectiveness of the E&F mission:

A lack of clear delineation of E&F's roles and responsibilities relative to the handling of DOMEX within the IC and across the U.S. Government has resulted in duplication of effort in some instances. Moreover, E&F does not have a process to obtain documented data owner approval for inclusion of customer-owned data in SIGINT reports, and our testing of a sample of serialized reports revealed a lack of related documentation. The E&F organization also does not maintain a log to track what results produced by cryptanalytic sources and methods are shared with customers, as required by its service level agreement with another NSA organization. Lastly, E&F's operational SOPs are outdated or non-existent, and the organization does not have a documented process for updating them.

The OIG made six recommendations to assist the Agency in addressing these issues and, thereby, to improve the efficiency and effectiveness of its E&F efforts. In addition, the OIG will share its findings with the Inspector General for the Intelligence Community particularly related to duplication of effort within the IC.

Ongoing Special Studies and Evaluations

Limited Scope Study of NSA Data Tagging Controls to Comply with 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 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 internet capabilities.

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.

Review of Overcollect Compliance Incidents by Overhead Satellite Systems

The OIG reviewed reported overcollect compliance incidents by overhead satellite systems. According to incident reports reviewed by the OIG, these incidents are usually addressed by reinforcing training of documented procedures; however, the recurrence of these incidents suggests that this remedy has proven insufficient to fully address the problem.

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.

Joint Review of Overhead SIGINT Compliance at a Joint Facility

The objectives of this joint review are to assess the application of SIGINT compliance policies and procedures at a joint facility; assess the processes or mechanisms for raising questions and resolving disagreements regarding programs or operations as they relate to SIGINT compliance; and identify any hurdles that may keep SIGINT compliance policies from keeping pace with applicable technological advances.

NSA's Dissemination of FISA Section 702 Collection to Certain Partners

The overall objectives of the study are to assess whether the procedures for disseminating Section 702 counterterrorism collection to certain partners are sufficient to ensure compliance with the current legal and policy framework, including the protection of U.S. person privacy, and whether the dissemination of this data to the partners is efficient and effective.

Limited Scope Evaluation of United States Person (USP) Identifiers Used to Query against FAA Section 702 Data

The objective of this evaluation is to assess the effectiveness of the internal controls used to protect USP privacy rights by determining whether NSA analysts are appropriately documenting the foreign intelligence purpose and using approved USP identifiers as query terms against FAA Section 702 data, in accordance with FAA Section 702 query procedures.

Limited-Scope Evaluation of Mission Correlation Table Data

The objective of the evaluation is to test the effectiveness of controls for Mission Correlation Table (MCT) data, including, for example, assigning mission authorities, location, and members to an MCT; managing MCT and mission member entitlements; granting mission members access to signals intelligence data in NSA repositories; and administering MCT roles and responsibilities

Investigations

Prosecutions

One case referred to the U.S. Attorney for the District of Maryland in October 2017 resulted in a contractor pleading guilty to one count of making false statements in violation of 18 U.S.C. § 1001. The case involved the contractor fraudulently billing the Agency for over 1,500 hours at a cost of over $411,000 for time that was not worked. Sentencing is scheduled for later this year.

One case referred to the U.S. Attorney for the District of Maryland in July 2018 resulted in a contractor pleading guilty to one count of making false claims in violation of 18 U.S.C. §§ 287 2(b). The case involved the contractor fraudulently billing the Agency for over 1700 hours at a cost of over $220,000 for time that was not worked. Sentencing is scheduled for later this year.

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 June 2017 involving allegations that a contractor company provided unqualified labor in support of an agency contract is pending resolution.

A case referred to the U.S. Attorney for the District of Maryland in July 2018 involving allegations that an Agency employee colluded with an Agency contractor to overbill the government is ongoing.

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 16 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 ethics violations, making false statements, submitting false timesheets, and contractors submitting false labor charges. The OIG anticipates at this time that the government is likely to handle all of these cases administratively, rather than criminally.

The Investigations Division referred 33 cases involving Agency personnel to NSA Employee Relations (ER) for potential disciplinary action. During the reporting period, the OIG also received notification from the Agency of disciplinary decisions regarding 23 employees in grades GG-14 and below. One employee was terminated from employment; three employees retired or resigned in lieu of removal; four employees resigned before ER took disciplinary action; four employees received suspensions of greater than 14 days; one employee received a suspension of 14 days or fewer; nine employees received letters of reprimand or counseling; and one employee received no penalty. Twenty-three cases referred by the OIG to ER from this and prior reporting periods are pending action.

Employee Relations took disciplinary action against five GG-15s and one Senior Executive during the reporting period for misconduct reported in a previous SAR. The Senior Executive entered into an Alternative Discipline Agreement in which the Senior Executive agreed to accept a reduction in grade, assignment to a non-supervisory position, and a 15-day suspension from pay and duty. The disciplinary actions for the GG-15s consisted of two employees that resigned in lieu of removal; one employee was reduced in grade and suspended from pay and duty for 30 days; one employee received a 7-day suspension from pay and duty; and one employee that received no penalty.

Seven cases substantiating contractor misconduct were referred to the Agency's Contracting Office for action, resulting in the recoupment of a total of $549,319. Fourteen cases substantiating employee timecard fraud were referred to the Agency's Payroll Office resulting in the recoupment of $63,764.

OIG Hotline Activity

The Investigations Division fielded 558 contacts through the OIG hotline.

Significant Investigations

Senior Executive: Misuse of Position and Misuse of Government Vehicle

An OIG investigation determined that a Senior Executive misused his position when he permitted his subordinates to obtain coffee and meals for him on multiple occasions. He also permitted his subordinates to drive him to and from the airport in their personally owned vehicles and visit his home to perform a personal task for other than official purposes in violation of 5 C.F.R. § 2635. The Senior Executive also misused a government owned vehicle when he allowed a subordinate to pick him up from the airport and be driven to his domicile in violation of DoD and Agency policies.

The investigative findings were forwarded to DoD IG, ER, the Office of Personnel Security, and the subject's supervisor.

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

Senior Executive: Misuse of Parking Pass and False Statements

An OIG investigation determined that a Senior Executive employee misused his senior executive parking permit by sharing it with his spouse in violation of Agency policy. The OIG concluded that the Senior Executive knowingly provided false statements to Agency officials and OIG personnel regarding this matter, and that he failed to give full and complete cooperation to the OIG in that he lacked candor in testimony during the OIG investigation.

The investigative findings were forwarded to DoD IG, ER, the Office of Personnel Security, and the subject's supervisor.

The case was referred to the U.S. Attorney for the District of Maryland on 9 May 2019 and declined for consideration of prosecution.

GG-15: Time and Attendance

An OIG investigation determined that a GG-15 employee knowingly submitted false and inaccurate timesheets in violation of Agency policy.

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor.

The case was referred to the U.S. Attorney for the District of Maryland on 5 June 2019 and declined for consideration of prosecution.

GG-15: Use of Public Office for Private Gain

An OIG investigation determined that a GG-15 employee created the appearance of a personal services contract by treating contractors as government employees in violation of FAR 37.104. The OIG also determined that the employee provided preferential treatment to the contractor who was a personal friend. The OIG substantiated that the employee used their public office for private gain, a violation of 5 CFR § 2635.702.

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor.

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

GG-15: Use of Public Office for Private Gain

An OIG investigation determined that a GG-15 employee did not create the appearance of establishing a personal services contract in violation of FAR 37.104. The OIG also determined that the employee did not provide preferential treatment to specific contractors in violation of 5 CFR § 2635.702 and Agency policy.

GG-15: Computer Misuse

An OIG investigation determined that a GG-15 employee misused the Agency information system to conduct private business activities in violation of Agency policy and the DoD Joint Ethics Regulation (JER) 5500.7-R.

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor.

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

GG-15: Conflict of Interest

An OIG investigation determined that a GG-15 employee violated a mandatory one-year "cooling off" period when he began working as a government program manager approximately one month after he had previously worked on the same program as a contractor affiliate. The OIG also determined that the employee held financial interests that conflicted with his official duties in violation of 5 C.F.R. § 2635.502 and Agency policy.

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor.

The case was referred to the U.S. Attorney for the District of Maryland on 4 March 2019 and declined for consideration of prosecution.

Whistleblower Reprisal

An OIG investigation reviewing reprisal allegations against two Senior Executive employees found that one Senior Executive employee reprised against a subordinate, but the other Senior Executive employee did not after the subordinate made protected communications to the chain of command and the OIG. The investigation determined that the complainant had made five protected disclosures and thereafter suffered an adverse personnel action. The investigation found that the Senior Executive who was the employee's direct supervisor reprised against the subordinate when he lowered the ratings on a performance evaluation. The investigation also found that the Senior Executive who reviewed and approved the subordinate's performance evaluation did not engage in reprisal based on clear and convincing evidence that he would have taken the same action absent the protected disclosures and the absence of a motive to retaliate on his part.

The investigative findings were forwarded to DoD IG, the Office of Personnel Security, and Human Resources. This case was not referred to ER because the Senior Executive who engaged in reprisal resigned before the investigation was completed.

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

Whistleblower Reprisal

An OIG investigation found that a GG-14 employee did not reprise against a subordinate for making protected communications to the Office of Dispute, Resolution, and Grievances (DRG). The investigation determined that the complainant did not establish a *prima facie* case of reprisal. We determined that the protected disclosure was not a contributing factor in the adverse personnel action.

The investigative findings were forwarded to the DoD IG.

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

Whistleblower Reprisal

An OIG investigation found that two GG-15 and two GG-14 employees did not reprise against a subordinate for making protected communications to the chain of command and the OIG. The investigation determined that the complainant had made two protected disclosures and thereafter suffered an adverse personnel action. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel action absent the protected disclosures.

The investigative findings were forwarded to the DoD IG.

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

Whistleblower Reprisal

An OIG investigation found that a GG-15 employee did not reprise against a subordinate for making protected communications to his chain of command. The investigation determined that the complainant had made six protected disclosures and thereafter suffered an adverse personnel action. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel action absent the protected disclosures.

The investigative findings were forwarded to the DoD IG.

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

Whistleblower Reprisal

An OIG investigation found that a GG-15 employee did not reprise against a subordinate for making protected communications to his chain of command and the Agency's Anti-Harassment Coordinator. The investigation determined that the complainant did not establish a *prima facie* case of reprisal. We determined that the protected disclosure was not a contributing factor in the subject personnel action.

The investigative findings were forwarded to the DoD IG.

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

Whistleblower Reprisal

An OIG investigation found that a GG-15 and a GG-14 employee did not reprise against a subordinate for making protected communications to the chain of command. The investigation determined that the complainant had made three protected disclosures and thereafter suffered an adverse personnel action. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel action absent the protected disclosures. However, the OIG did find that the GG-15 employee restricted the complainant from making protected disclosures in violation of NSA Policy 1-62, and created a hostile work environment by failing to take corrective actions against the GG-14. Further, we found that the GG-14 employee created a hostile working environment by denigrating others, using profanity, making offensive and disruptive comments, and engaging in other rude and disrespectful conduct in the workplace.

The investigative findings were forwarded to DoD IG, ER, the Office of Personnel Security, and the subject's supervisor.

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

Summary of Additional Investigations

NSA OIG opened 37 investigations and 75 inquiries while closing 27 investigations and 72 inquiries during the reporting period. The new investigations involve 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 six contractor labor mischarging investigations and substantiated four cases that had been opened previously. The substantiated cases closed during the reporting period resulted in the proposed recoupment of approximately $511,277. Ten investigations remain open.

Time and Attendance Fraud

NSA OIG opened five new investigations into employee time and attendance fraud during the reporting period. Four investigations that had been opened previously were substantiated during the reporting period. The substantiated cases closed during the reporting period resulted in the proposed recoupment of $44,259. Disciplinary action against three employees is pending. Six investigations remain open.

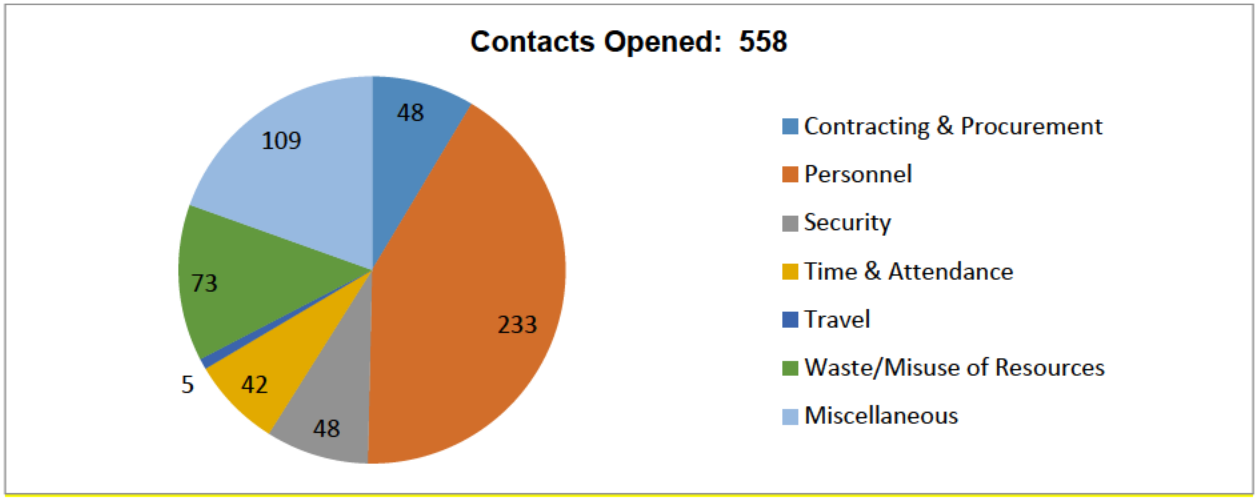
Computer Misuse

NSA OIG opened four new investigations involving allegations of computer misuse. The OIG substantiated three existing cases. The substantiated cases involved employees and the results were referred to ER for disciplinary action. Four investigations remain open.

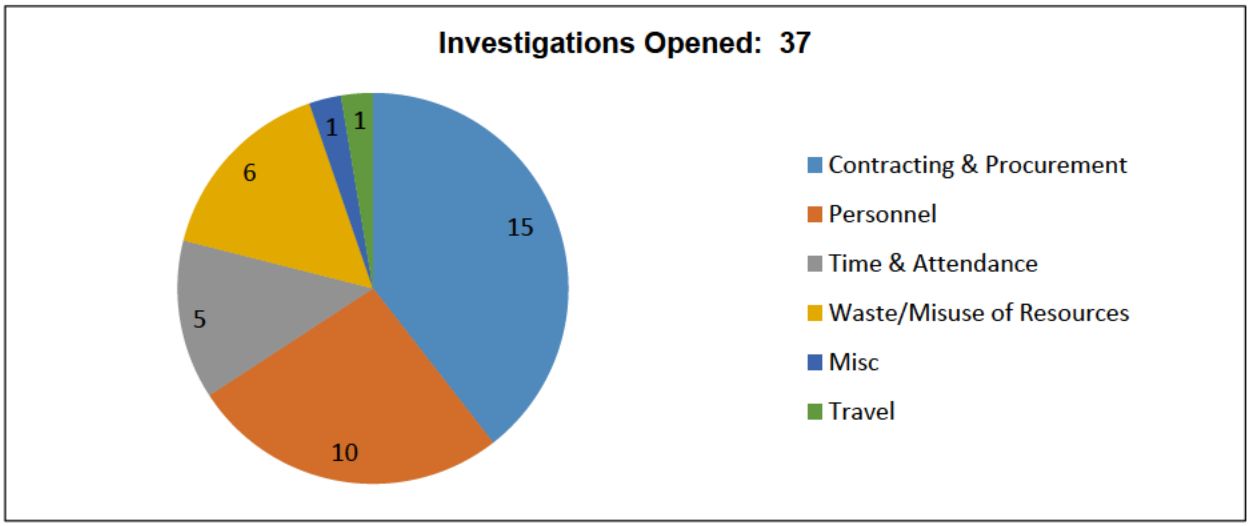
Investigations Summary

Total number of investigative reports issued	27
Total number of persons reported to DOJ for criminal prosecution	16
Total Number of Persons Referred to State and Local Authorities for Criminal Prosecution	0
Total Number of Indictments/ Waiver of Indictments and Guilty Pleas	2
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

As reported in our SAR for the period ending 31 March 2019, the OIG Inspection Division previously was subject to a peer review conducted by the NGA, DIA, CIA, and IC IGs. During the current reporting period, we received and responded to the report of that review, which found that we met all applicable standards, and we are implementing the suggestions for improvements in our practices. The OIG supported a peer review conducted of another OIG Inspections Division during the current reporting period.

Whistleblower Program

As we have stated in the past, the OIG recognizes that 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. We consider whistleblowers to be a vital source of information that helps the OIG accomplish its mission by providing information that is critical to our ability to detect and deter waste, fraud, abuse, and misconduct throughout this extensive Agency and related to its diverse programs and operations.

The NSA OIG operates a Hotline, staffed by experienced and knowledgeable investigators, 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 2019 and 30 September 2019, the OIG opened four new reprisal investigations and closed six other reprisal investigations. One of the closed investigations substantiated allegations of reprisal and was referred to the proper organization and/or Agency for further action. We also refined our procedures for handling reprisal allegations to ensure the accuracy of our determinations and to make sure that people who come forward know that they have every opportunity to seek relief through this office.

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. During this period, the OIG continued to disseminate informational cards and posters 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 serves as a resource by which Agency employees and others can obtain further information about their rights and protections. We also continue to work on additional outreach and training materials for the workforce in this important area, releasing a video on both the internal and external websites in which the Director and the IG join to encourage reporting of suspected wrongdoing and finalizing a new training module that we hope to roll out shortly.

In July, the OIG disseminated information regarding National Whistleblower Appreciation Day across the Enterprise, and the IG personally participated in a program recognizing this important event on Capitol Hill. We also are committed to continuing our relationship with non-governmental organizations (NGOs) that are active on whistleblower issues so that the OIG can continue to benefit from their important perspective and experience.

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

Audits

Mission and Mission Support

Audit of NSA's Internal Controls Over Second Party Integrees

Audit of NSA's Fiscal Year 2018 Compliance with the Improper Payments Elimination and Recovery Improvement Act of 2012

Audit of the Temporary Medical Leave Assistance Program (TMLAP)

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

Review of the Agency's Nuclear Weapons Personnel Reliability Program

Technology and Cybersecurity

Audit of NSA's Corporate Authorization Service (CASPORT)

Audit of CIO Authorities

Financial Audit

FY2019 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

Inspections

Enterprise Inspections

Inspection of NSA/CSS Representative (NCR) and Cryptologic Services Group (CSG) to U.S. Pacific Command (USPACOM)

Joint Inspections

Joint Inspectors General Inspection Report – National Security Agency Hawaii (NSAH)

Oversight Memoranda

Special Study on the Assignment of Military Affiliates to NSA

Quick Reaction Report arising from the Inspection of an Overseas Location

Intelligence Oversight

Review of National Security Agency/Central Security Service Analyst Compliance with Intelligence Community Directive on Dissemination of Congressional Identities

Special Study of the Endpoint and Forensics Mission

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

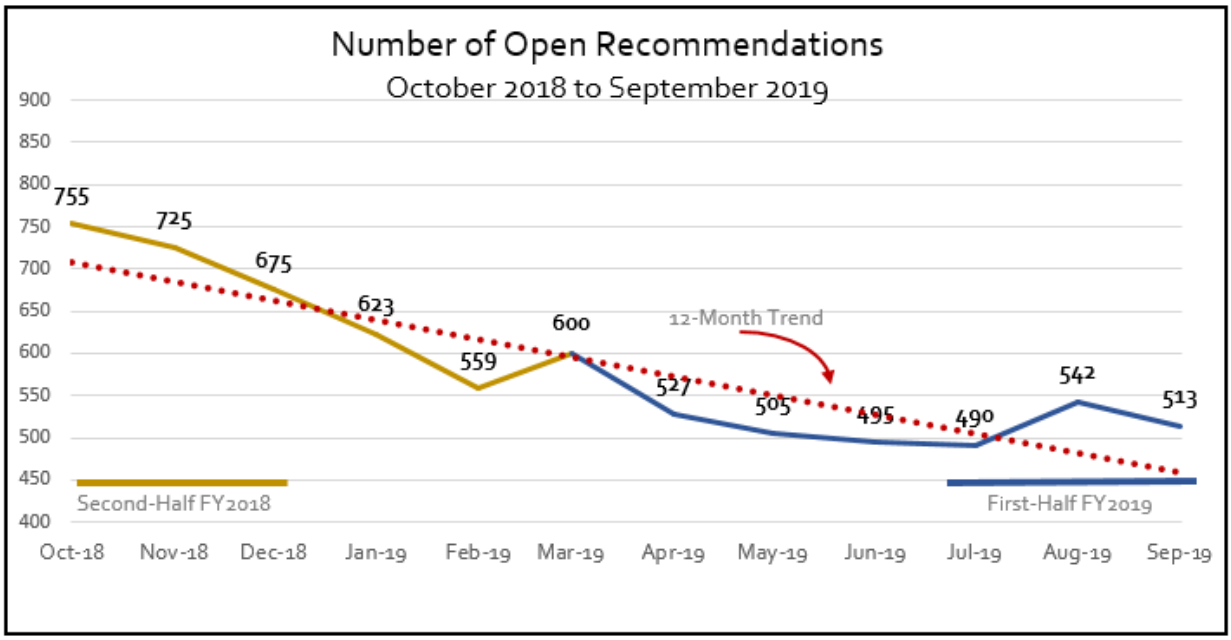
The OIG made 232 recommendations to NSA management in reports and oversight memoranda issued during this reporting period. The Agency closed 86 of the newly published recommendations, and a total of 319 recommendations during the reporting period.

Outstanding Recommendations

The OIG considers a report open when there are one or more recommendations contained in the report that have not been closed. The number of open recommendations is the total for all reports that remain open. Recommendations are considered overdue when they remain open beyond the target completion date that was reflected in the report for action sufficient to meet the intent of the recommendation to be completed.

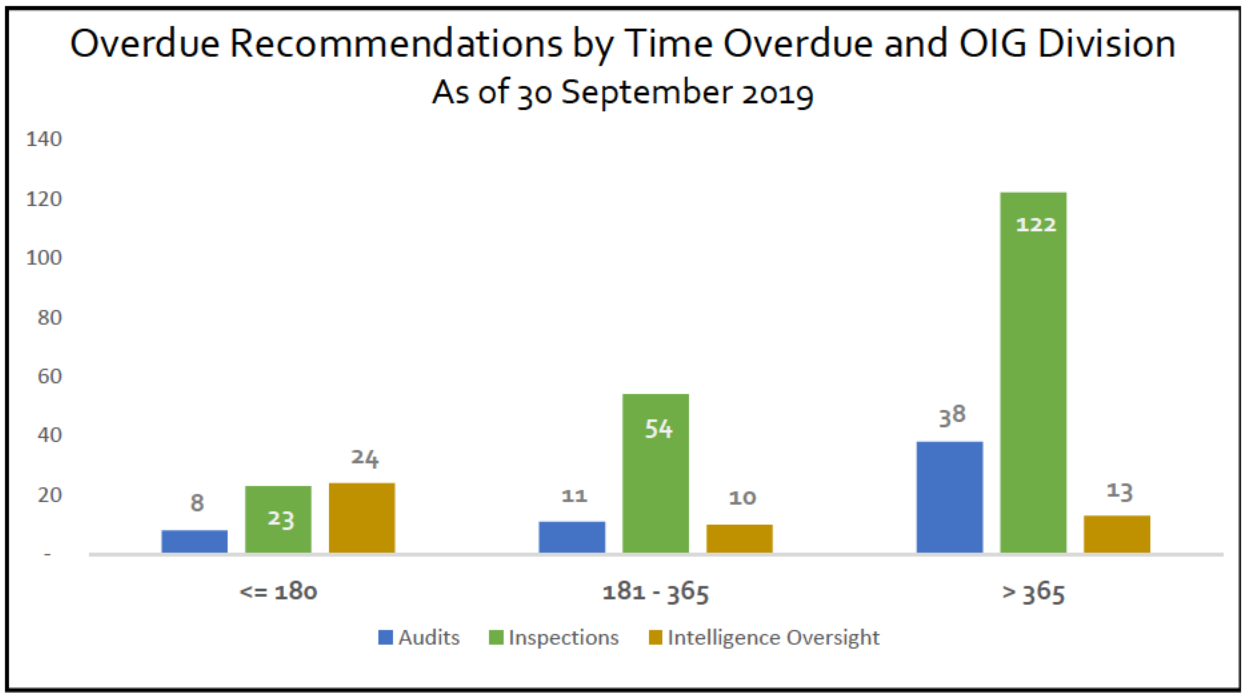
Outstanding Recommendations

	Audits	Inspections	Intelligence Oversight	Total
Open reports	33	38	18	89
Open recommendations	129	313	71	513
Overdue recommendations	57	199	47	303
Overdue recommendation as % of total open	**44%**	**64%**	**66%**	**59%**



Overdue Recommendations Breakdown

Days Past Target Completion Date	Audits	Inspections	Intelligence Oversight	Total	Percent Overdue
<= 180	8	23	24	55	18%
181 - 365	11	54	10	75	25%
> 365	38	122	13	173	57%
Totals	**57**	**199**	**47**	**303**	



Management Policy Referrals

In addition to the recommendations arising from audits, inspections, evaluations, and reviews detailed above, the OIG has issued seven referrals to Agency management involving policy issues since August 2018, including two issued during this reporting period – one relating to the release of applicant disciplinary history to internal hiring organizations and the other related to data transfer procedures. Of the seven management referrals, four are closed based upon Agency action, and three remain open as of the end of the reporting period.

Significant Outstanding Recommendations – Audits

Audit of NSA Enterprise Solution and Baseline Exception Request Processes

The OIG found in 2011 that Agency organizations and contractors are 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.

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 are not properly implemented for data centers and equipment rooms; and
- Removable media are not properly scanned for viruses.

Continuity of Operations Planning

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 who rely on NSA intelligence.

Emergency Management Plan

Many sites inspected do not have a mature, well-exercised Emergency Management Plan or Emergency Action Plan for the protection of personnel and the site. This encompasses situations such as an active shooter, natural disaster, and terrorist threat.

Significant Outstanding Recommendations – Intelligence Oversight

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 Intelligence 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 requested extensions as challenges in standing up a new compliance organization delayed resolution. Substantial progress has been made recently toward resolving the outstanding recommendations and, in several cases, all that remains is the publication of finalized documentation.

Special Study of NSA Controls to Comply with the FISA Amendments Act §702 Targeting and Minimization Procedures

The OIG conducted this study to determine whether select NSA controls are adequate to ensure compliance with the Foreign Intelligence Surveillance Act of 1978 FAA Section 702 targeting and minimization procedures. As part of this study, the OIG tested NSA's controls that ensure that data is queried in compliance with the FAA Section 702 targeting and minimization procedures. The OIG found that NSA did not have a necessary system control. The Agency had previously identified this as a concern and has been working to implement a new system control. In the review, the OIG assessed that, until this system control is implemented, the Agency will be at risk for performing queries that do not comply with NSA's FAA §702 authority. The Agency has indicated that until the recommended system control is available, it has in place multiple processes to aid in ensuring query compliance. The target completion date for this recommendation was December 2017. The current Agency estimate is to develop a prototype and implement a pre-query compliance control by December 2020.