Office of the Inspector General
National Security Agency

Semiannual Report to Congress

1 October 2019 to 31 March 2020

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 revised 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

These are difficult times. As I write this Message, the United States and, indeed, the entire world are in the midst of a global pandemic – the greatest public health emergency in more than a century. Many of our families, friends, and fellow citizens have fallen ill or fallen victim to COVID-19. Until it is defeated – and it will be defeated – we all are having to find new ways to live and work in what is frequently described as our "new normal."

As our government continues to perform critical functions and provide essential services to and for the public during this period, so should and must oversight continue in order to ensure the integrity and efficiency of those government programs and operations. Throughout our country's robust public discourse, questions have long been raised about the efficacy of government programs and the conduct of those who are entrusted to carry them out. In this context, the role of nonpartisan, independent oversight is as critical as ever. The federal Inspector General system, borne in a climate of diminished public confidence following Watergate and other scandals now almost a half-century old, remains an essential part of the oversight mosaic. Offices such as the National Security Agency/Central Security Service (NSA) Office of the Inspector General (OIG) are actively engaged in a wide range of audits, inspections, evaluations, and investigations that detect and deter waste, fraud, abuse, and corruption, and promote the economy, efficiency, and effectiveness of Agency operations. These aren't just platitudes taken from the Inspector General Act – they are the underpinnings of a system that exists to ensure that the government is performing its critical functions well, and that every American's tax dollars are spent wisely. It is because of the independence of Inspectors General's Offices in carrying out their work and the transparency that they bring to those efforts that they are able to conduct oversight that is credible and, therefore, impactful within their agencies, in the halls of Congress, and ultimately with the American people.

Against this backdrop, and in this difficult time, I am particularly pleased to present the Semiannual Report to Congress (SAR) of the NSA OIG for the period 1 October 2019 through 31 March 2020. The SAR describes the audits, evaluations, inspections, and investigations that were completed and ongoing during that reporting period. And, while the number of oversight reports issued during the period was limited by the impact of the pandemic, two things stand out for me as emblematic of the vitality and importance of our work.

First, in December 2019, the OIG publicly issued an unclassified version of its report on *NSA Controls to Comply with Signals Intelligence Retention Requirements*. This report addressed an issue of significant public importance, that is, whether the Agency was complying with the requirements for aging-off signals intelligence (SIGINT) data collected pursuant to Executive Order (E.O.) 12333 and the Foreign Intelligence Surveillance Act (FISA). We made a number of findings related to the Agency's retention of SIGINT data and, as with all our reports, specific recommendations to the NSA to assist it in addressing those issues. Coming in the wake of our now-regular preparation and public release of unclassified versions of our SARs and two of our underlying audit reports, the preparation and posting an unclassified version of this intelligence oversight report on the NSA OIG's independent public website, https://oig.nsa.gov, as well as on the site of the Council of the Inspectors General on Integrity and Efficiency (CIGIE), www.oversight.gov, represented an important step forward in this office's efforts to enhance the transparency of our oversight work in areas of significant importance to the public. The

preparation of such unclassified reports can take a good deal of additional time and effort, and we cannot do a lot of them without detracting from our other important oversight work. But the OIG will continue to look for opportunities to prepare and release such unclassified reports on issues of significant public interest where it is possible to provide more information to the public than we can reasonably include in our periodic SARs covering all our oversight work for a given reporting period.

The second development that I want to highlight is the completion and roll out earlier this year of a new training program on whistleblower rights and protections, for which the OIG provided the content as the Agency's subject matter expert. Given the seminal importance of encouraging people to come forward with what they reasonably believe to be evidence of wrongdoing, I was very pleased that the Director of the NSA agreed to make this training mandatory on an annual basis for all Agency employees. Ensuring that people on the front lines have the information they need to feel comfortable coming forward has been and will continue to be among this office's highest priorities; the agencies where OIGs work are just too big and their operations too diverse for us to know everything that is going on without people being willing to come forward when they see something they believe is wrong. As I and many others in the IG Community have said, such individuals perform a difficult, but invaluable service when they come forward, and they should never suffer reprisal for doing so.

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.

This is a difficult time, but we will find our new normal, and the women and men of the NSA OIG will continue our work conducting independent, transparent, impactful oversight for and on behalf of the American people.

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

Index of Reporting Requirements

§5(a)(1)	Significant problems, abuses, and deficiencies	3–5
§5(a)(2)	Recommendations for corrective action re: §5(a)(1)	3–5
§5(a)(3)	Significant outstanding recommendations	29-30
§5(a)(4)	Matters referred to prosecutorial authorities	17-18
§5(a)(5)	Information or assistance refused	iii
§5(a)(6)	List of audit, inspection, and evaluation reports	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	N/A
§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	24
§5(a)(17)	Statistical tables of investigations	22-23
§5(a)(18)	Description of Metrics used in statistical tables of investigations	23
§5(a)(19)	Reports concerning investigations of Seniors	18-20
§5(a)(20)	Whistleblower Retaliation	20-21
§5(a)(21)	Agency interference with IG Independence	iii
§5(a)(22)	Disclosure to the public	iii-iv
§5(a)(note)	P.L. 110-181 §845, Final completed contract audit reports	N/A
§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

Despite the impact of the global pandemic on OIG operations at the end of the reporting period, this has been another busy and productive time 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 four reports containing six recommendations to improve Agency operations.

The Cybersecurity and Technology Branch performed an audit to determine whether the Agency effectively decommissions its information systems. We found among other things that the Agency had not yet established a comprehensive decommissioning policy or program, and that it did not consistently complete, retain, or validate system decommissioning documentation. We also performed the annual evaluation of the *NSA's Implementation of the Federal Information Security Modernization of 2014 (FISMA)*. Specifically, we evaluated eight information technology (IT) security areas against applicable metrics, and determined that there was room for improvement in all areas: risk management, configuration management, identity and access management, data protection and privacy, security training, continuous monitoring, incident response, and contingency planning.

The Financial Audits branch focused during this reporting period on the congressionally mandated *Audit of NSA's Financial Statements*. In addition, the Financial Audits branch oversaw a service organization control examination related to the Agency's performance of certain financial processing services on behalf of another U.S. Government entity.

Inspections Division

The OIG issued four inspection reports during this reporting period, and conducted one new joint inspection at a field site. The Agency and all participants 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 also completed an evaluation of the NSA's personnel accountability program.

Intelligence Oversight Division

During this reporting period, the OIG's Intelligence Oversight Division issued one report on a special study that determined to what extent NSA controls ensure that data labels are assigned accurately and completely to SIGINT data acquired pursuant to the FISA Amendments Act (FAA) §§704 and 705(b). In the report, we made seven recommendations, six to assist NSA in strengthening its corporate data tagging controls and governance, and a seventh to help ensure that NSA's FISA §§704 and 705(b) data tagging legal and policy determinations are consistent with NSA representations made to the Foreign Intelligence Surveillance Court (FISC) and other external overseers regarding how NSA handles such data, and that these tagging requirements are

fully documented and promulgated to the NSA workforce. We also released an unclassified version of the previously issued *Special Study of NSA Controls to Comply with Signals Intelligence Retention Requirements*, in which the OIG made a number of findings related to the Agency's retention of SIGINT data and a total of 11 recommendations to address them.

Investigations Division

During this reporting period, the Investigations Division received and processed 524 contacts, which resulted in the initiation of 22 investigations and 69 inquiries. Three new investigations involved allegations of whistleblower reprisal, two involved allegations of ethics violations, two involved allegations of misuse of position, and one involved allegations of government owned vehicle misuse. Twenty-seven investigations and 63 inquiries were closed during the reporting period, resulting in the proposed recoupment to the Agency of approximately $706,000 from contractors and $41,000 from employees. As a result of OIG investigations, disciplinary actions ranging from termination to reprimands were taken against 21 employees. Two individuals were criminally sentenced in federal court and a whistleblower civil settlement was entered based on investigations conducted by the OIG, and several other cases we previously referred to the U.S. Attorney for the District of Maryland and the Department of Justice are pending resolution.

Whistleblower Program

Whistleblower rights and protections continue to be a primary focus for our office. During this period, we continued our efforts in this area, including completing our work as the subject matter expert on a new on-line training program that the Agency agreed to make mandatory on an annual basis for all Agency employees.

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:

Quick Reaction Report on the Personnel Accountability Concerns Found During the Joint Inspection of an Overseas Field Site

During the inspection of an overseas field site, the OIG identified two concerns related to health and safety that we believed required immediate attention by site leadership. The OIG issued a Quick Reaction Report after the site failed to contact a significant number of its personnel during an OIG-requested recall exercise. In addition, a failure to maintain accurate listings of affiliated personnel in the country could result in a failure to fully support its personnel in a crisis. The failure to follow established processes resulted in many site military members not being properly recorded in the appropriate human resources management system (HRMS).

The OIG made three recommendations to address these concerns. These included developing, documenting, and implementing a process to ensure that the site can account for all its affiliated personnel within the site; implementing periodic tests of the recall process to include generating after action results aimed at improving results; and revising the site's standard operating procedure regarding the assignment of its military personnel in HRMS, conducting a review of its military personnel at site locations, and updating HRMS accordingly. The site accepted the OIG's recommendations, and we found that management's planned actions met the intent of those recommendations.

Audit of NSA's FY2019 Financial Statements

The objective of the audit was 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. Because NSA could not provide sufficient appropriate evidence to support certain material account balances, the external accounting firm that the OIG retained did not express an opinion on the financial statements.

In FY2019, we found that material weaknesses exist in the Agency's ability to provide documentation to support the financial statement assertions. While there has been progress in a number of important respects, four of these areas - General Property, Plant & Equipment, Procurement Activity and Accounts Payable Accrual, Budgetary Activity, and Fund Balance with Treasury - continue from the FY2018 financial statement audit.

1. **General Property, Plant and Equipment (PP&E)** NSA did not have effective policies, processes, procedures, or controls to identify, accumulate, and report its General PP&E, to include Equipment, Communications Security assets, Integrated Hardware and Software assets, Leasehold Improvements, Construction-in-Progress, and Software. For equipment,

NSA did not maintain historical documentation to support equipment balances and, therefore, has developed a number of estimation methodologies to value its equipment based on equipment attributes and assumptions. However, the assigned value of a significant number of equipment assets could not be validated because the assigned values were not supported by information provided and recorded attributes, such as manufacture make and model, were not supported or were incorrect. In addition, weaknesses in the Agency's wall-to-wall inventory process were identified. A significant number of assets were not included in the Agency's property system or the Agency did not have sufficient documentation to support whether assets should have been included in the property system.

2. **Procurement Activity and Accounts Payable Accrual** NSA did not effectively design and implement policies, procedures, or controls to ensure the reliability and consistency of source documentation as it relates to both Federal and non-Federal procurement activity as well as the key source of critical data inputs and assumptions used in its accounts payable methodology. In addition, the Economy Act Order (EAO) manager control, used to verify receipts and acceptance of goods and services provided by trading partners, was not designed and implemented effectively such that EAO managers were required to review transactions timely or that the appointed EAO managers were required to certify the transaction in NSA's accounting system. Further, the review was not designed and implemented effectively so that the EAO manager could link invoiced activity to the timing of delivery of specific goods or services.

3. **Budgetary Activity** NSA's processes, procedures, and controls impacted its ability to provide sufficient documentation to support the validity of its undelivered orders. Additionally, the Agency did not design and implement control activities to effectively monitor, identify, and deobligate invalid obligations in a timely manner. Finally, the current functionality in the Agency's accounting systems is such that recoveries of prior year obligations are only recorded if adjustments pertain to an expired appropriation. NSA had been unable to obtain from its systems vendor the necessary systems changes to conform to the U.S. Standard General Ledger at the transaction level, as required by the Federal Financial Management Improvement Act of 1996.

4. **Fund Balance with Treasury (FBwT) and Deposit Funds** NSA did not fully implement effective controls to demonstrate that, working through the Defense Finance and Accounting Service, all NSA related activities were appropriately routed to NSA through the Cash Management Report process, and that NSA's FBwT was completed and accurately reconciled with Treasury. In addition, NSA's processes, controls, and associated documentation were not sufficient to ensure accurate reporting of its activity with foreign trading partners and, therefore, could not ensure that all internally generated documentation related to Deposit Funds was reconcilable to external documentation.

5. **Entity Level Controls** A material control weakness was identified in NSA's entity level controls related to control environment, risk assessment and monitoring, and information and communication. Specifically, resource constraints may have required NSA managers to prioritize certain internal controls, and reduce the number of personnel assigned to other internal controls. NSA did not complete a robust risk assessment throughout its business processes to identify and analyze risks related to the achievement of its defined reporting objectives. Further, NSA did not fully design or implement controls to evaluate the segregation of duty justifications to ensure that mitigating controls were designed and

operating effectively throughout FY 2019. Finally, NSA did not obtain reliable data from internal and external sources needed to adequately support the amounts recorded with its financial statements.

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

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

In accordance with U.S. Office of Management and Budget guidance, the OIG is required annually to assess the effectiveness of information security programs on a maturity model spectrum, which ranges from Level 1 (ad hoc) to Level 5 (optimized). Our assessment of eight IT security areas revealed that while progress was made in some areas from FY2018 to FY2019, there continues to be room for improvement in all eight IT security areas.

Table 1. Overall Maturity Levels

Security Area	FY2018 Maturity Level for Security Area	FY2019 Maturity Level for Security Area
Risk Management	2 – Defined	2 – Defined
Configuration Management	2 – Defined	2 – Defined
Identity and Access Management	3 – Consistently Implemented	3 – Consistently Implemented
Data Protection and Privacy	2 – Defined	2 – Defined
Security Training	3 – Consistently Implemented	2 – Defined
Continuous Monitoring	2 – Defined	2 – Defined
Incident Response	2 – Defined	2 – Defined
Contingency Planning	1 – Ad Hoc	1 – Ad Hoc

For the second consecutive year, Identity and Access Management was deemed the strongest security area with an overall maturity level of 3, consistently implemented. The Agency's challenges in Security Training dropped the maturity level from 3, consistently implemented, to 2, defined. For the second consecutive year, Contingency Planning was assessed at an overall maturity level of ad hoc; although the Agency has made some improvements to the program, additional improvements need to be made.

Audit of NSA's FY2019 Financial Statements

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

Audit of the Agency's Information System Decommissioning Process

The overall objective of the audit was to determine whether the Agency was effectively decommissioning information systems, including doing so consistently, securely, and efficiently. The audit revealed that the Agency had not yet established a comprehensive decommissioning policy or program. Specifically, a review of two separate Agency system decommissioning processes found that several decommissioning actions were required by one process and not the other. Further, we found that the Agency relied on decommissioned system data from two minimally integrated repositories that are used for different purposes. In addition, the Agency did not consistently complete, retain, or validate system decommissioning documentation. The OIG found that the lack of a comprehensive, consistently implemented system decommissioning program creates an increased risk that systems selected for decommissioning could continue to operate on Agency networks for an extended period of time without the Agency's knowledge. The OIG made six recommendations to assist the Agency to address the issues identified in the report, and we found that management's planned actions met the intent of those recommendations.

Oversight Review 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 2018 and 2017 were performed in accordance with U.S. generally accepted government auditing standards and the terms of the contract for non-appropriated fund instrumentalities audit services. 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, there were no material weaknesses in internal control over financial reporting and there was no reportable noncompliance with provision 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.

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 intragovernmental account balances are accurate and properly supported.

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 the Agency's Retention Incentive Program

The purpose of this audit is to assess the economy and effectiveness of 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 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.

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.

Audit of Enclaves with Distributed Monitoring Oversight

The overall objective of the audit is to determine whether Agency network enclaves with distributed monitoring oversight are secured in accordance with Agency, Department of Defense (DoD), and Federal policies.

Audit of NSA's FY2020 Financial Statements

The purpose of the audit is to express an opinion on whether the financial statements are presented fairly and in conformity with U.S. generally accepted accounting principles. The audit will consider and report on internal control over financial reporting and compliance with certain laws, regulation, and other matters.

Audit of NSA's Fiscal Year 2019 Compliance with the Improper Payments Elimination and Recovery Improvement Act of 2012

In this audit, the OIG will determine whether the Agency is compliant with the Improper Payments Elimination and Recovery Improvement Act using OIG procedures in the Office of Management

and Budget Circular A-123 Appendix C, *Requirements for Payment Integrity Improvement*, 26 June 2018.

Audit of NSA's Security and Counterintelligence Efforts to Address Insider Threats

The purpose of this Congressionally-required audit is to determine the effectiveness of the NSA Security and Counterintelligence (S&CI) posture against insider threats with an emphasis on how NSA has organized S&CI, the activities undertaken by S&CI, and the effectiveness of S&CI programs and initiatives associated with mitigating insider threats.

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, we will assess the overall effectiveness of the Agency's information security policies, procedures, and practices.

Audit of Integrity and Use of Security Clearance Data Reported to Office of the Director of National Intelligence

The NSA OIG is working with the Office of the Inspector General of the Intelligence Community (ICIG) on an audit of the integrity and use of the security clearance data reported by selected Intelligence Community elements to the Office of the Director of National Intelligence.

Evaluation of Intelligence Community Implementation of Security Clearance Reciprocity

The Office of the ICIG also is conducting an evaluation of Intelligence Community implementation of security clearance reciprocity. The NSA OIG is working with the ICIG on this effort.

Inspections

Inspection Reports and Oversight Memoranda Completed in the Reporting Period

Evaluation of NSA's Personnel Accountability Program

The Inspections Division, in coordination with the Audits Division, performed the biennial evaluation of NSA's personnel accountability program, as required by DoD Instruction (DoDI) 3001.02, *Personnel Accountability in Conjunction with Natural or Manmade Disasters*, 3 May 2010. The overall objective of the evaluation was to ensure NSA's compliance with DoDI 3001.02, which prescribes 15 responsibilities for the accounting and reporting of DoD-affiliated personnel following a natural or manmade disaster. The OIG's evaluation revealed that NSA's personnel accountability program does not comply with 4 of the 12 applicable requirements. Among these deficiencies were that procedures were contained within a draft policy that has not been finalized; NSA has not provided the necessary information and guidance to educate the workforce on their personnel accountability roles and responsibilities; and NSA has not established internal procedures to monitor compliance with DoDI 3001.02. The OIG made one recommendation to assist the Agency in addressing these deficiencies.

Quick Reaction Report on the Regional Service Center/Operations Center (ROC) Concerns Found During the Joint Inspection of an Overseas field site

During the inspection of an overseas field site, the OIG identified three concerns related to health and safety and two-person access that we believed required immediate attention by site leadership. The OIG issued a Quick Reaction Report in which it made recommendations to assist the site in addressing these concerns. Site leadership accepted the OIG's recommendations and implemented corrections within this reporting period that addresses all three concerns.

Quick Reaction Report on the Personnel Accountability Concerns Found During the Joint Inspection of an Overseas Field Site

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

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

The OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the NCR and CSG organizations assigned to USTRANSCOM. The OIG reviewed pertinent documents, support agreements, policies, regulations, and intelligence oversight data. Inspectors conducted interviews with members of the NCR TRANSCOM workforce, as well as off-site interviews with outgoing and incoming leadership.

The OIG interviewed members of the workforce and observed site operations and functions in mission operations; intelligence oversight; information technology and systems; resource programs; safety, facilities, continuity of operations, emergency management; and security. NCR USTRANSCOM's main customers within the Command consistently described the support

received as excellent, and their only concerns surrounded how to get more USTRANSCOM personnel approved for access to all of the same sensitive information USTRANSCOM leaders are authorized to see. In assessing the NCR USTRANSCOM operations and organization, the OIG identified concerns related to current and future staffing needs, customer accessibility to intelligence, and the level of engagement with USTRANSCOM customer organizations. Further, the OIG noted a need for mission owner oversight for missions delegated to NCR USTRANSCOM, as well as a desire for more operational training and a need for updated intelligence oversight documentation. Additional needs highlighted by the OIG assessment included an updated host-tenant support agreement; corrections to IT system source records; and improvements to the site's health and safety program, continuity of operations plan, and emergency action plan.

The OIG made 26 recommendations and one observation to assist NCR USTRANSCOM and the Agency in addressing the findings identified during the inspection. The OIG also noted one commendable at NCR USTRANSCOM that highlighted a best practice in the area of intelligence oversight.

Special United States Liaison Office London

The NSA OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the Special United States Liaison Office, London (SUSLOL). During the inspection, the OIG conducted focus groups, participants of which represented all segments of the civilian government workforce. The OIG also interviewed members of the SUSLOL workforce and observed SUSLOL operations and functions in mission operations; intelligence oversight; resource programs; information technology and systems; safety, facilities, and emergency management; security; and training.

Overall, the OIG found site personnel were encouraged by the communications with and restructuring efforts of site's senior leaders. The OIG noted four commendables at SUSLOL, which highlighted best practices in the areas of mission engagement with the U.K.'s Government Communications Headquarters (GCHQ) partner and intelligence oversight practices. The OIG identified a number of issues, including the following:

- Concerns related to the lack of adequate corporate knowledge management, leadership's strict application of the rotation date policy, and the governance of a separate SUSLOL site.
- Outdated governance documents, knowledge transfer issues, and lack of clarity about working under the operational authorities of the GCHQ.
- Concerns related to records management, SUSLOL's Visit Tracker tool, and property accountability. Among the recommendations was the need to identify records management officers for all SUSLOL organizations in accordance with policy requirements.
- Concerns with the use of shared printers and cell phone requirements. Only one recommendation in this area remains open.
- Issues related to safety and continuity of operations (COOP), including the need for an approved safety program and identification of an occupational safety and health representative, as well as two recommendations regarding COOP.

- Several gaps, including the lack of required standard operating procedures and knowledge management documentation, and the absence of a number of important required plans.
- Lack of a method to track the mandatory training of State Department locally employed U.K. nationals, lack of a consistent or written process to address the approval and funding of training temporary duty assignments, and issues with NSA's individual training plan (ITP) tool.

The OIG made 48 recommendations and 6 observations to assist SUSLOL and the Agency in addressing the findings identified during the inspection.

Ongoing Inspection Work

The NSA, Army Intelligence and Security Command, U.S. Fleet Cyber Command, and 16th Air Force OIGs jointly conducted one inspection during the current reporting period that evaluated the overall climate and the compliance, effectiveness, and efficiency of an overseas field site.[1]

The NSA OIG also continues to work on the reports for inspections conducted during the prior reporting period that evaluated the overall climate and the compliance, effectiveness, and efficiency of the following organizations:

- RAF Menwith Hill;
- NSA Cryptologic Representative to U.S. Africa Command; and
- NSA Cryptologic Representative to U.S. European Command.

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.

[1] On 11 October 2019, the 25th Air Force (AF) merged with the 24th AF to form a reactivated 16th AF.

Intelligence Oversight

Special Studies and Oversight Memoranda Completed in the Reporting Period

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

The objective of this study was to review select NSA data tagging controls that ensure data labels are assigned accurately and completely to SIGINT data acquired pursuant to the FISA FAA Sections 704 and 705(b). NSA implemented data labels as a means to identify the specific collection authorities under which data was acquired and the handling instructions that apply. These controls are designed to ensure the appropriate processing, retention, and dissemination of such data, and the protection of U.S. person information as required by law.

The OIG, with Agency assistance, performed system searches for a compliance purpose in NSA data fields to identify all data objects that were acquired for or in connection with FISA Sections 704 and 705(b) during a 2-day period in January 2018. Some of the control weaknesses identified by the OIG significantly limited our ability to independently determine the accuracy of data tagging assignments because of inadequate and incomplete NSA information. Nevertheless, the OIG found that:

- NSA does not have adequate and complete documentation of scenario-based data tagging rules for accurately assigning data labels to restrict access to data in accordance with legal and policy requirements, and consistently assessing data labeling errors;
- NSA has not designated a standardized field in NSA data tags to efficiently store and identify data needed to verify the accuracy of data label assignments;
- NSA does not document in its targeting tool a majority of a certain type of targeting request; and
- NSA controls do not adequately and completely verify the accuracy of data labels assigned to data prior to ingest into NSA repositories.

As a result of these findings, the OIG made seven recommendations, six to assist NSA in strengthening its corporate data tagging controls and governance, and a seventh to help ensure that NSA's FISA §§704 and 705(b) data tagging legal and policy determinations are consistent with NSA representations made to the FISC and other external overseers regarding how NSA handles such data, and that these tagging requirements are fully documented and promulgated to the NSA workforce.

Ongoing Special Studies and Evaluations

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 the Capabilities Compliance Incident Management Process (renamed from 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 documenting, tracking, and reporting Capabilities Directorate compliance incidents, in particular, those that involve Capabilities Directorate-owned or managed systems and personnel.

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 NSA's Rules Based Targeting (RBT) Controls

The objective of the evaluation is to determine whether NSA's RBT controls are performing efficiently, effectively, and in a manner that complies with NSA's SIGINT collection authorities.

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.

Inspectors General of the IC and NSA Joint Review of Management and Intelligence Oversight at the Intelligence Community Advanced Campaign Cell (ACC)

The objective of this joint review by the Inspectors General of the IC and the NSA is to determine whether management and intelligence oversight of the IC ACC ensures that processes and procedures are in place to conduct operations that comply with IC and DoD policies. The joint review will present any issues to the Director of National Intelligence and the Director, NSA for resolution, as appropriate.

Evaluation of the Procedures for Continental U.S. (CONUS) Wireless Signals Testing and Training

The objective of the evaluation is to determine the effectiveness and efficiency of procedures for conducting wireless signals collection testing and training in CONUS facilities and the degree to which those procedures ensure compliance with the laws, directives, and policies that protect civil liberties and individual privacy.

Evaluation of Select NSA Partner Data Sharing Capabilities

The objective of the evaluation is to assess the effectiveness and efficiency of the controls for select NSA processes and capabilities when sharing data and information with foreign partners and the degree to which those controls ensure compliance with the laws, directives, and policies that protect civil liberties and individual privacy.

Evaluation of a Targeting System's Control Framework for Domestic and Foreign Partner Targeting Systems

The objective of the evaluation is to determine the effectiveness and efficiency of a targeting system's control framework as it relates to domestic and foreign partner targeting systems, with emphasis on NSA's handling of partner targeting requests. The evaluation will also examine how NSA prepares some targeting requests prior to sending them to partner targeting systems, as well as evaluate the targeting system's internal controls and the degree to which those controls ensure compliance with the laws, directives, and policies that protect civil liberties and individual privacy.

Evaluation of NSA's LEGALEAGLE System Enrollment, Data Ingest, and Decision-Logic Processes

The objectives of the evaluation are to determine the effectiveness of NSA's process for identifying and registering systems, ensuring the integrity of ingested records, validating the decision-logic processes, and validating the effectiveness of LEGALEAGLE's operations and associated controls in ensuring compliance with the laws, directives, and policies that protect civil liberties and individual privacy.

Investigations

Criminal Prosecutions

The NSA OIG conducted two separate criminal investigations that substantiated significant instances of labor mischarging. Based on their felony pleas in the U.S. District Court for the District of Maryland, Kyle Smego and Todd Leasure were sentenced in separate proceedings in December 2019, and ordered to pay restitution to the government totaling over $400,000.

Kyle Smego, who was employed by two NSA subcontractors, pled guilty to submitting false claims to the government. He admitted to fraudulently inflating the number of hours he worked by at least 40% (1700 hours) over a period of 2 years. The Court sentenced him to 8 months of home detention as a special condition of 3 years' probation and ordered him to pay restitution of $252,527. Mr. Smego was listed in the Government's System for Award Management as debarred on March 19, 2020.

Todd Leasure, who was working as a database administrator for an Agency contractor, pled guilty to making false statements. Over a period of 3 years, he submitted timesheets falsely listing at least 607 hours that he did not actually work. The Court sentenced him to 6 months of home detention as part of 5 years' probation and ordered him to pay restitution of $150,001.

False Claims Act

In a civil settlement, Eagle Alliance agreed to pay the Government $110,000 to resolve allegations the company overbilled for computer hardware, without admitting liability. This whistleblower False Claims Act case was brought by the U.S. Attorney for the District of Maryland after a joint investigation by the OIG and the Defense Criminal Investigative Service.

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 14 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, 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 19 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 23 employees. One employee was terminated from employment, seven employees retired or resigned in lieu of removal, eight employees received suspensions from pay and duty, five employees received letters of counseling or reprimand, and two employees received no corrective action. Eighteen cases referred by the OIG to ER are pending action.

Three cases substantiating contractor misconduct were referred to the Agency's Procurement Office for action, resulting in the recoupment of $278,449.69. Three cases substantiating employee timecard fraud were referred to the Agency's Payroll Office resulting in the recoupment of $27,722.88.

OIG Hotline Activity

The Investigations Division fielded 524 contacts through the OIG hotline.

Significant Investigations

Senior Executive: Hostile Work Environment and Misuse of Position

An OIG investigation determined that a senior executive:

- Created a hostile work environment by using abusive and offensive language toward subordinate employees, in violation of Agency policy;
- Requested 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;
- Solicited gifts of food from subordinates on at least nine occasions by requesting subordinates bring donuts and other food to the office without payment, in violation of 5 CFR § 2635.302; and
- Misused the NSA/CSS information systems in a manner that served no legitimate public interest and which would reflect adversely on NSA, in violation of DoD Joint Ethics Regulation and Agency policy.

The investigative findings were forwarded to the DoD OIG, 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: False and Inaccurate Timesheets and Misuse of Position

An OIG investigation determined that a senior executive knowingly submitted false and inaccurate timesheets for a total shortfall to the government of more than 40 hours, resulting in a loss of approximately $3,500 to the government. The OIG also determined that the senior official requested a subordinate use official time to perform activities other than those required in the performance of their official duties. The employee's actions violated 5 CFR §§ 2635.101, 2635.705, and Agency policy. The senior official resigned prior to the completion of the investigation.

The investigative findings were forwarded to the DoD OIG and the Office of Personnel Security. The results were not forwarded to ER as the subject resigned from the Agency before the investigation was complete.

The case was referred to the U.S. Attorney for the District of Maryland on 3 June 2019 and declined for consideration of prosecution.

Senior Executive: Preferential Treatment and Travel Overpayments

An OIG investigation determined that a senior executive failed to act impartially and granted preferential treatment to an external applicant in the hiring process. The OIG also determined that the senior executive improperly claimed government reimbursement for meals provided by another entity during multiple temporary duty assignments. The employee's actions violated 5 U.S.C. § 2302, 5 CFR § 2635.101, the Joint Travel Regulations § 010302, and Agency policy. The senior official retired prior to the completion of the investigation.

The investigative findings were forwarded to the DoD OIG and the Office of Personnel Security. The results were not forwarded to ER as the subject resigned from the Agency before the investigation was complete.

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

GG-15: Hostile Work Environment/ Misuse of Position

An OIG investigation determined that a GG-15 engaged in threatening physical behavior, created a disturbance, and used abusive and offensive language toward subordinate employees. Additionally, the employee failed to exercise courtesy and respect in interactions with fellow workers. The employee's actions violated Agency policy. The OIG also determined that the employee used their public office for private gain in violation of 5 CFR § 2635.702, and that the employee misused the government information system to conduct private business activities in violation of the Joint Ethics Regulation 5500.7-R and Agency policy.

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: Preferential Treatment

An OIG investigation determined that a GG-15 violated ethical standards by creating an appearance of giving preferential treatment to individuals whom the GG-15 or their domestic partner represented in the sale or purchase of real estate. The employee's actions violated 5 CFR § 2635.101, and Agency policy.

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: False and Inaccurate Timesheets

An OIG investigation determined that a GG-15 knowingly submitted false and inaccurate timesheets in violation of Agency policy, for a total shortfall to the government of 178 hours and a loss of approximately $13,000.

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 15 January 2020 and declined for consideration of prosecution.

GG-15: False and Inaccurate Timesheets

An OIG investigation determined that a GG-15 knowingly submitted false and inaccurate timesheets in violation of Agency policy, for a total shortfall to the government of 158 hours and a loss of approximately $9,700.

The investigative findings were forwarded to the Office of Personnel Security. The results were not forwarded to ER as the subject resigned from the Agency before the investigation was complete.

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

GG-15: False and Inaccurate Timesheets

An OIG investigation determined that a GG-15 knowingly submitted false and inaccurate timesheets in violation of Agency policy, for a total shortfall to the government of more than 60 hours and a loss of approximately $4,400.

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.

GG-15: Conflict of Interest

An OIG investigation reviewing allegations that an employee violated conflict of interest laws was not substantiated. The OIG determined that the employee's actions did not violate 5 CFR §§ 2635.101, 2635.801, DoD Joint Ethics Regulation 5500-07-R, or Agency policy.

GG-15: Personal Services Contract and Preferential Treatment

Two separate OIG investigations into allegations that two GG-15s created personal services contracts and provided preferential treatment to a specific contractor were not substantiated. The OIG determined that neither employee's actions violated 5 CFR § 2635.702, the Federal Acquisition Regulation § 37.104, or Agency policy.

Whistleblower Reprisal

An OIG investigation found that a GG-15 did not reprise against a subordinate for making protected communications to the chain of command and the OIG by detailing the employee to another position. The investigation determined that the complainant had made protected disclosures to the chain of command and the OIG, 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 did not reprise against a subordinate for making protected communications to the chain of command by changing the employee's duties. The investigation determined that the complainant had made protected disclosures to the chain of command, 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.

Summary of Additional Investigations

NSA OIG opened 22 investigations and 69 inquiries while closing 27 investigations and 63 inquiries during the reporting period. The new investigations are reviewing various allegations including whistleblower reprisal, misuse of position, misuse of Government resources, ethics violations, and violations of time and attendance and contract billing policies.

Contractor Labor Mischarging

NSA OIG proposed recoupment of $706,282.81 during the reporting period. Six contractor labor mischarging investigations were opened and four previously opened cases were substantiated. Eleven investigations remain open.

Time and Attendance Fraud

NSA OIG proposed recoupment of $41,675.06 during the reporting period. Three new investigations into employee time and attendance fraud were opened and four previously opened cases were substantiated. Disciplinary action against seven employees is pending. Four investigations remain open.

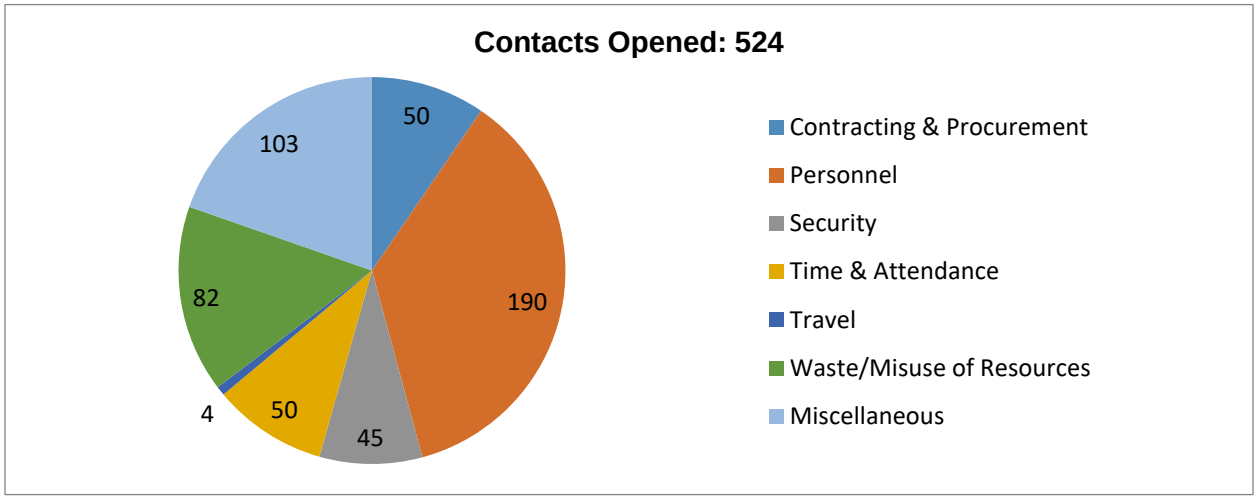
Computer Misuse

NSA OIG opened one new investigation involving allegations of computer misuse. Four previous investigations were substantiated during the reporting period. Three of the substantiated cases involved employees and the results were referred to ER for disciplinary action. One computer misuse investigation remains open.

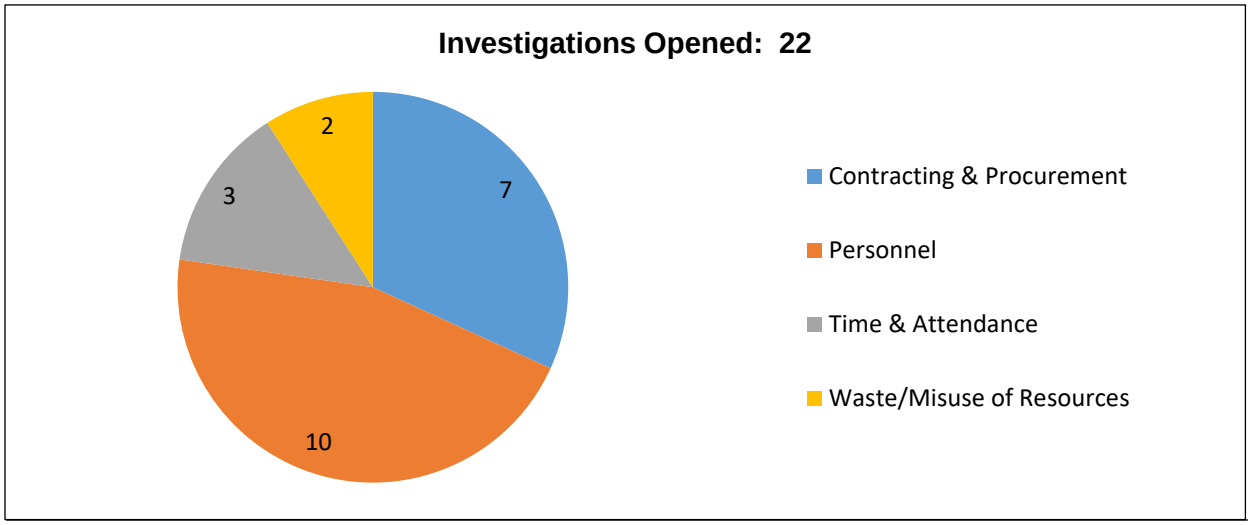
Investigations Summary

Total number of investigative reports issued	27
Total number of persons reported to DOJ for criminal prosecution	14
Total number of persons referred to state and local authorities for criminal prosecution	0
Total number of Indictments/Informations	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 OIG led a peer review of another OIG Audit Division during the current report period.

Whistleblower Coordinator Program

Whistleblowers perform an invaluable service to the agencies where they work and the public at large when they come forward with what they reasonably believe to be evidence of wrongdoing. They should never suffer reprisal for doing so. These core principles remain at the heart of our work at the NSA OIG. Since coming to the NSA in 2018 from the Department of Justice OIG, where he founded and chaired the Whistleblower Ombudsperson Working Group of the CIGIE, IG Storch has prioritized all reprisal matters. To that end, we have taken a variety of steps to ensure that all NSA employees, contractors, and military affiliates are aware of their respective rights and protections. Both our internal website and independent external public facing website (https://oig.nsa.gov) have designated pages with extensive whistleblower information and FAQs, with contact information for the OIG's designated Whistleblower Coordinator to address any additional questions. We have prepared a variety of educational materials and videos, and during this reporting period completed development of an online training program on which the OIG served as the subject matter expert. The OIG was pleased that the Agency agreed to make this new training module mandatory for all agency employees on an annual basis, helping to ensure that they have the essential information regarding their rights and protections such that they are confident coming forward when they see something they believe is wrong.

The NSA OIG's commitment to whistleblower rights and protections is also reflected in how we handle reprisal complaints and investigations. We are required by statute to maintain the confidentiality of individuals coming forward with complaints (unless they give written consent or the disclosure of their identity would be unavoidable), and all NSA OIG employees rigorously uphold this requirement. The IG and Counsel to the IG both personally monitor the status of each reprisal investigation on a weekly and as needed basis and review the outcome of each case. NSA OIG has also adopted a forward-leaning policy by which complainants in investigations that preliminarily have not been substantiated are given an opportunity to review our tentative findings and conclusions and provide comments and/or additional information for our consideration prior to finalizing the report. Not only does this help to ensure the accuracy of our work, but it highlights the institutional justice that we believe is critical to maintaining the trust and confidence of the agency workforce. In that regard, a number of complainants have told the OIG that while they were disappointed that their reprisal claims were not substantiated, they appreciated the input they had in the process and understood more fully the outcomes of the investigations.

Like all Inspectors General, the NSA OIG relies on agency employees, contractors, and military personnel to report what they reasonably believe to be evidence of waste, fraud, abuse, or misconduct. We also recognize that unless those people feel comfortable in coming forward, we may never become aware of such potential wrongdoing, whether it be time and attendance fraud, misuse of government property, or violations of the NSA's legal authorities. We are working every day at the OIG to make sure that all NSA employees, contractors, and military personnel have confidence that their complaints will be taken seriously, that they will be objectively reviewed and timely investigated where appropriate, and that they will suffer no adverse consequences for doing the right thing.

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

Audits

Mission and Mission Support

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

Technology and Cybersecurity

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

Audit of the Agency's Information System Decommissioning Process

Financial Audit

Audit of NSA's FY2019 Financial Statements

Inspections

Enterprise Inspections

Inspection of NSA/CSS Representative and Cryptologic Services Group to U.S. Transportation Command

Evaluation of NSA's Personnel Accountability Program

Special United States Liaison Office, London

Oversight Memoranda

Quick Reaction Report on the Personnel Accountability Concerns Found During the Joint Inspection of an Overseas Field Site

Quick Reaction Report on the Regional Service Center/Operations Center (ROC) Concerns Found During the Joint Inspection of an Overseas Field Site

Intelligence Oversight

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

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

Audit Reports with Questioned Costs[2]

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[3]

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

[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.

[3] 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

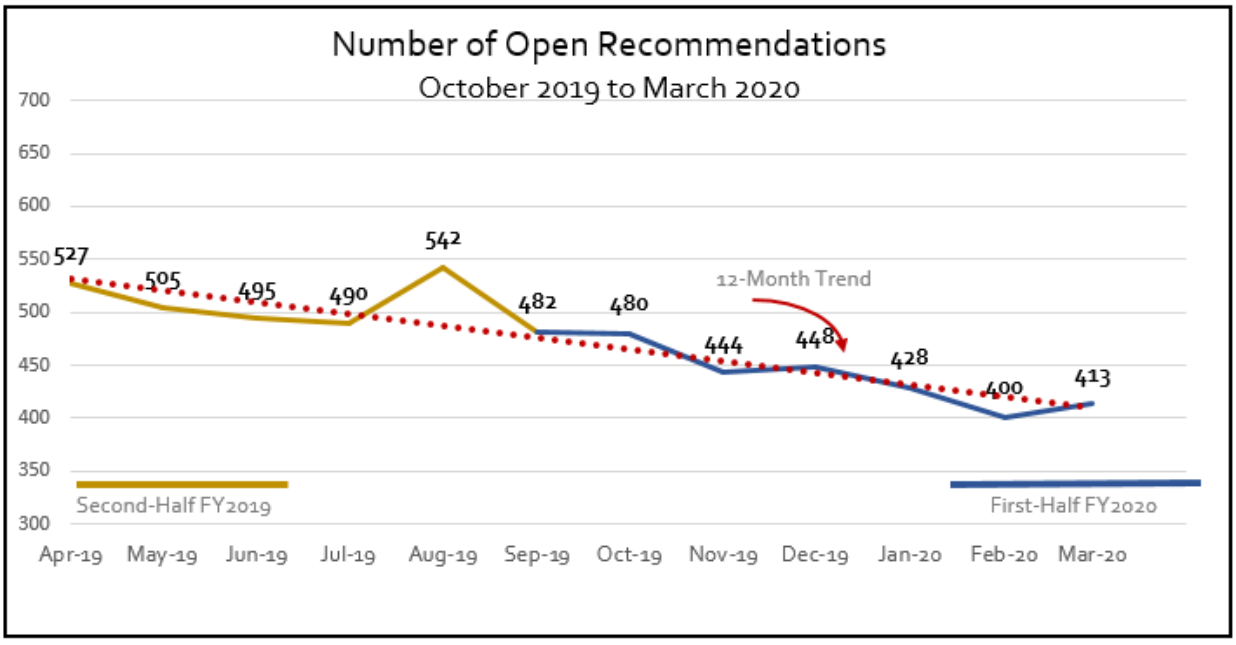
The OIG made 94 recommendations to NSA management in reports and oversight memoranda issued during this reporting period. The Agency closed 39 of the newly published recommendations, and a total of 208 recommendations during the reporting period.

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.

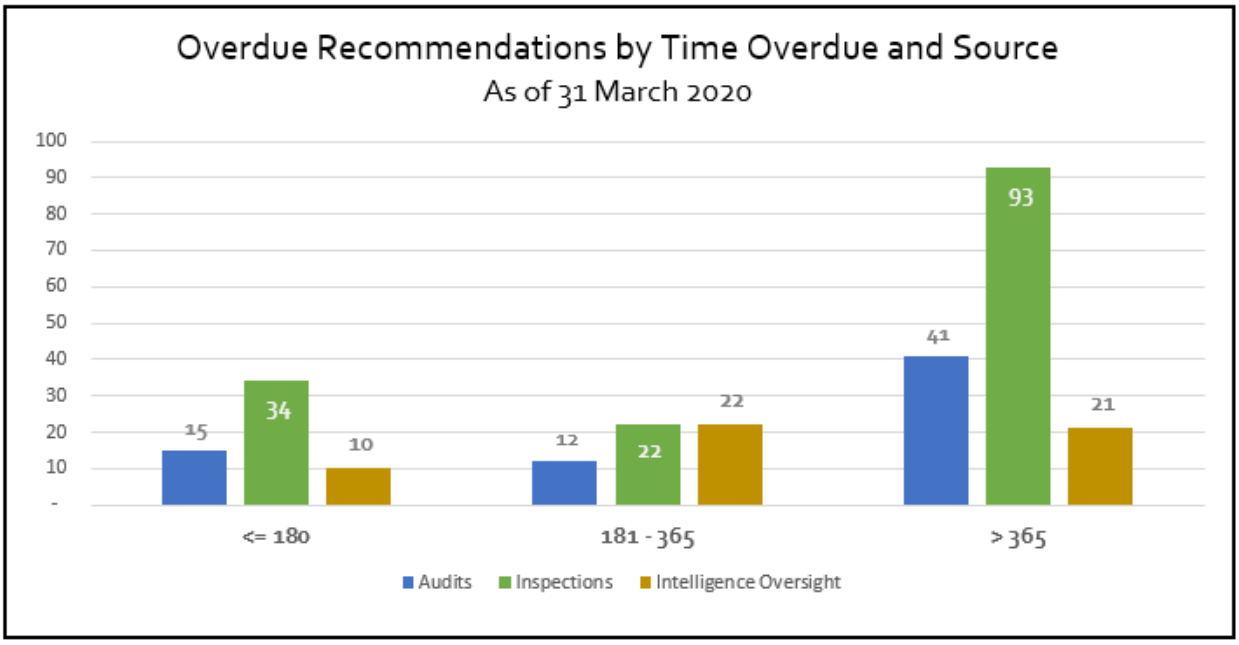
Outstanding Recommendations

	Audits	Inspections	Intelligence Oversight	Total
Open reports	29	39	19	87
Open recommendations	100	246	67	413
Overdue recommendations	68	149	53	270
Overdue recommendation as % of total open	**68%**	**61%**	**79%**	**65%**



Overdue Recommendations Breakdown

Days Past Target Completion Date	Audits	Inspections	Intelligence Oversight	Total	Percent Overdue
<= 180	15	34	10	59	22%
181 - 365	12	22	22	56	21%
> 365	41	93	21	155	57%
Totals	**68**	**149**	**53**	**270**	



Management Policy Referrals

In addition to the recommendations arising from audits, inspections, evaluations, and reviews detailed above, the OIG has issued nine referrals to Agency management involving policy issues since August 2018, including two issued during this reporting period – one relating to personnel issues and another related to whether access is considered dissemination for the purpose of Section III(D)(4) of the NSA Section 704 standard minimization procedures. Of the nine management referrals, six were closed based upon Agency action, and three remained 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. The Agency has now implemented such a solution for software acquisitions; however, for hardware acquisitions, the Agency plans to charter a working group to address requisite acquisition approval controls.

The OIG also recommended that the Agency develop contract provisions to require contractors to comply with NES and BER 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 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 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. 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 implement a pre-query compliance control by December 2020.