Office of the Inspector General
National Security Agency

Semiannual Report to Congress

1 April 2020 to 30 September 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 Semiannual 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 honored to present the Semiannual Report to Congress (SAR) of the National Security Agency (NSA) Office of the Inspector General (OIG) for the period 1 April 2020 through 30 September 2020. This has been such a difficult time for so many. Like so many other offices across our country, the NSA OIG significantly reduced staffing levels in our offices near the end of the prior reporting period, which given the nature of our work, significantly impacted our operations for several months during this reporting period. Nevertheless, the people of the OIG have been exceptionally resilient and, as we have reconstituted our efforts over the past several months, remarkably productive.

Despite the significant limitations imposed by the circumstances, I am proud to say that the OIG team was able to issue 11 substantial oversight products during this period. As detailed in the Executive Summary and the body of this SAR, these covered a range of critical Agency programs and operations, and reflected substantial efforts by all three OIG report-writing divisions. These reports consisted of six important intelligence oversight products, an extensive inspection report, and four highly consequential audits. Additionally, the OIG Investigative Division continued to do outstanding work manning our Hotline and conducting critical investigations throughout the period, including work on a wide variety of criminal, civil, and other misconduct matters. During this reporting period, we also significantly expanded our efforts on the OIG's statutorily-mandated assessment of the top management and performance challenges facing the Agency, and we conducted an enterprise-wide survey regarding the Agency's response to the COVID-19 pandemic that we believe will be important in informing the Agency's activities and our future work in that area. And, of course, we continue to prioritize the areas of transparency, with the preparation and issuance of the unclassified version of our prior SAR, and whistleblower rights and protections, with the completion of our first year of Agency-wide mandatory training and additional outreach efforts in this critical area. Finally, we have been involved in a wide range of activities within the broader Inspector General oversight community, including leading and participating in a number of committees and efforts of the Council of the Inspectors General on Integrity and Efficiency. In short, I could not be prouder of my team for the way they have stepped up to do consequential work during this difficult period.

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 but one OIG recommendation that was made during the reporting period (and has subsequently indicated that it intends to take action sufficient to meet the intent of that recommendation as well). All told, despite the difficult circumstances during this reporting period, the OIG made a total of 221 recommendations to NSA leadership that we believe will be impactful in improving the economy, efficiency, and effectiveness of this critical Agency's operations.

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	4-5
§5(a)(2)	Recommendations for corrective action	N/A
§5(a)(3)	Significant outstanding recommendations	26-27
§5(a)(4)	Matters referred to prosecutorial authorities	17
§5(a)(5)	Information or assistance refused	iii
§5(a)(6)	List of audit, inspection, and evaluation reports	23
§5(a)(7)	Summary of particularly significant reports	1-2
§5(a)(8)	Audit reports with questioned costs	24
§5(a)(9)	Audit reports with funds that could be put to better use	24
§5(a)(10)	Summary of reports for which no management decision was made	6
§5(a)(11)	Significant revised management decisions	6
§5(a)(12)	Significant management decision disagreements	6
§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	21
§5(a)(17)	Statistical tables of investigations	19-20
§5(a)(18)	Description of Metrics used in statistical tables of investigations	19
§5(a)(19)	Reports concerning investigations of Seniors	18
§5(a)(20)	Whistleblower Retaliation	18-19
§5(a)(21)	Agency interference with IG Independence	iii
§5(a)(22)	Disclosure to the public	N/A
§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	25-27
* Citations are to the Inspector General Act of 1978, as amended.		

This page intentionally left blank.

OIG Executive Summary

Despite the impact of the global pandemic on OIG operations, this has been a very 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 four reports containing 39 recommendations to improve Agency operations.

The Mission and Mission Support branch performed an audit of NSA's Installation and Logistics Services (ILS) contract, worth over $400 million, to ensure it was awarded properly and being administered effectively in accordance with applicable policies. We made a number of significant findings, including that the Agency did not have sufficient controls in place to ensure proper award and administration of the FY2016 ILS contract, that it improperly modified the contract by adding services and may have had a potential related Anti-Deficiency Act violation, that it did not have sufficient guidance and procedures in place to manage such contracts, that it had not evaluated the contractor's performance, and that it did not have the metrics necessary to measure such performance.

The Mission and Mission Support branch also performed an audit of the Agency's Retention Incentive Program and found that the Agency lacked controls over retention incentives, thereby increasing the risk of unjustified compensation and limiting the Agency's ability to determine the effectiveness the program. Further, we found that the Agency paid at least $4.2 million in unauthorized retention incentives. During this period, the OIG also completed an audit of the NSA's Enterprise-wide Space Utilization, and found that the Agency's decentralized management and limited oversight of facility space resulted in inconsistent implementation of policy, and that the Agency's space data was not current, accurate, or complete, limiting the Agency's ability to plan and implement space utilization decisions. Finally, we performed an audit of NSA's Compliance with the Improper Payment Elimination and Recovery Improvement Act of 2012 (IPERIA) and determined that NSA is compliant.

Inspections Division

During this reporting period, the OIG issued an extensive report on the 2019 joint inspection of Royal Air Force Menwith Hill. We identified a number of best practices, but also identified a variety of concerns, including issues related to the lack of strategic direction for the site and the need to conduct an analysis to identify staffing needs, the insufficiency of documentation across several functional areas, and a number of property management, information technology (IT), and safety concerns. We made a total of 121 recommendations in the report, 91 of which were assigned to NSA/Washington (NSAW), which had closed 24 prior to report issuance.

Intelligence Oversight Division

The OIG's Intelligence Oversight Division issued five final reports and one Quick Reaction Report during this period. In total, the oversight products issued by the OIG in this critical area contain 92 recommendations to assist the Agency in improving its operations and to increase compliance with requirements for protecting civil liberties and individual privacy. The five reports were:

- A joint report regarding overhead SIGINT compliance at a joint facility in which we found differing interpretations of SIGINT compliance governing documents and conflicting viewpoints regarding authorities and application of compliance procedures, and lack of an escalation process to bring issues to the attention of top-level management. We also found a persistent lack of understanding of the partners' respective missions, cultures, and perspectives, combined with the lack of joint operating instructions, integration of SIGINT experts, and tailored training.
- A review of certain NSA accounts, infrastructures, and services, which allow personnel to navigate the internet and augment and enable a range of missions. We found, among other issues, a lack of implementing guidance for DoD policy, outdated and unimplemented NSA policies, and the lack of a current office of primary interest and an updated policy for open source programs, which includes the internet accounts, infrastructures, and services that were the subject of the review.
- A review in which we examined reported overcollect compliance incidents involving unauthorized collection by overhead satellite systems. We determined that inconsistencies in interpretation of incident reporting standards and incomplete guidance to the workforce raise a significant risk of less than complete incident reporting by NSA.
- A review of NSA's system compliance certification process, which is meant to ensure that NSA mission systems comply with a set of requirements derived from the legal authorities, directives, and policies that protect civil liberties and individual privacy. We found, among other concerns, that the certification requirements are not clearly aligned with the compliance standards from which they are derived, that many NSA systems do not hold a current compliance certification, nor does NSA have a current, actionable plan to achieve certification for all relevant systems.
- A review of a targeting system's control framework, which ensures that targeting complies with NSA's SIGINT authorities to protect U.S. person privacy. We identified several deficiencies, including that the targeting system does not synchronize with all necessary NSA systems and repositories because specific requirements to do so have not been levied, the time required to process targeting requests did not always meet analyst expectations, and although the targeting controls operated properly, the system's inability to confirm implementation of detargeting actions and lack of a convenient process for updating target information increase the risk of unauthorized collection.

Additionally, during the course of an ongoing review into whether the Agency was appropriately documenting the foreign intelligence purpose and using approved U.S. Person (USP) identifiers as query terms against FISA Section 702 data, we discovered 15 Agency-known USP identifiers that appeared to have bypassed a particular NSA tool's internal control framework even after a breakdown in the tool had reportedly been corrected. We issued a Quick Reaction Report for the

Agency to determine what happened and to take appropriate steps to address the situation and report as may be appropriate.

Investigations Division

During this reporting period, the Investigations Division received and processed 393 contacts, which resulted in the initiation of 6 investigations and 22 inquiries. Two new investigations involved allegations of whistleblower reprisal, two involved allegations of computer misuse, one involved allegations of time and attendance fraud, and one involved allegations of contractor labor mischarging. Eleven investigations and 25 inquiries were closed during the reporting period, resulting in the proposed recoupment to the Agency of approximately $33,421 from employees and approximately $1,194,587 from contractors. As a result of OIG investigations, disciplinary actions ranging from termination to reprimands were taken against eight employees. Two cases referred to the U.S. Attorney for the District of Maryland were declined for prosecution.

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 the roll out of the new Agency-wide mandatory training program and the briefing of new Senior Agency leaders on this important topic.

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:

Joint Review of Overhead SIGINT Compliance at a Joint Facility

The NSA OIG conducted a joint review of overhead SIGINT compliance at a joint facility. The objectives of this joint review were to assess the application of SIGINT compliance policies and procedures; 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 technological advances in the overhead radio frequency (RF) collection environment.

The OIGs identified a number of hurdles that may hinder the application of SIGINT compliance policies and their ability to keep pace with technological advances in the overhead radio frequency environment. We also found that a process does not exist for raising questions and effectively resolving disagreements, and that there are no jointly accepted operating instructions for partner laboratory activities, which has resulted in what NSA at times has assessed to be noncompliant SIGINT access. As a result, 18 recommendations were made to assist in addressing the findings detailed in the report.

In response to a draft of this report, the Directors of the NSA and its partner issued a joint statement committing to work together to resolve the issues described by the OIGs in a manner that supports both organizations' unique missions. NSA and its partner agreed with all of the report's recommendations, and agreed to take action sufficient to meet their intent.

Special Study of Certain Internet Capabilities, Part II

The objective of this review was to examine management oversight, policy, training, roles, and responsibilities for certain accounts, infrastructures, and services. These allow NSA personnel to navigate the internet, and augment and enable a range of missions — operations, research, capabilities development, workforce support, security, counterintelligence, business management, and acquisition. This review expanded upon the OIG's earlier review, *Special Study of Certain Internet Capabilities*, issued in December 2017, which determined whether controls for certain NSA internet capabilities were adequate to ensure compliance with DoD and NSA policies to protect the civil liberties and individual privacy.

The current review revealed the following concerns involving NSA's development and use of certain internet accounts, infrastructures, and services:

- NSA lacks both implementing guidance for Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, and an intelligence

oversight program as prescribed by Department of Defense Directive 5148.13, Intelligence Oversight, for users of certain internet accounts, infrastructures, and services. As a result, the Agency cannot ensure that its activities in this area are compliant with DoD and NSA policies, and cannot determine whether its controls are adequate to protect civil liberties and individual privacy.

- NSA policy for these internet access accounts, infrastructures, and services has not been implemented. Unless these requirements are carried out, the Agency cannot ensure that its activities in this area are efficiently and effectively developed and used consistently with DoD and NSA policies for protecting civil liberties and individual privacy.
- NSA lacks a current office of primary interest and an updated policy for open source programs, which includes internet access accounts, infrastructures, and services. As a result, the Agency has no overall coordination and oversight of these activities.

The OIG made 28 recommendations to address the significant problems identified in this report, which the OIG found increased risks to protecting civil liberties and individual privacy, and jeopardized accountability and oversight of the Agency's use of certain internet accounts, infrastructures, and services.

Audit of NSA's Facilities and Logistics Service Contract

NSA's Installation and Logistics Services (ILS) contract requires the contractor to perform routine and minor maintenance, warehousing, storage and distribution, mail, and transportation services. This requirement began with the first contract being awarded in FY2008 and has been a continuous requirement thereafter. The current FY2016 ILS contract was issued in 2015 for over $400 million over a five-year period of performance. The contract was awarded to an Alaska Native Corporation and participant in the Small Business Administration (SBA) 8(a) program. The SBA 8(a) program is designed to level the playing field for socially and economically disadvantaged small businesses by providing aid and assistance with Federal contracting opportunities.

The OIG found that the Agency did not have sufficient controls in place to ensure proper award and administration of the FY2016 ILS contract. We found that the Agency did not properly prepare for the contract award and did not document the contract file sufficiently to support the sole-source award to a small business. Thereafter, the Agency modified the contract by adding $35 million in property services that were not part of the contract requirements and caused the contractor to develop new labor rates and hire additional employees. Lastly, we found the Agency did not have sufficient guidance and procedures in place to manage hybrid contracts funding, that it had not evaluated the contractor's performance, and that it did not have the metrics necessary to measure such performance.

As a result of these findings, we believe the Agency may have improperly awarded the FY2016 ILS contract to a small business, caused an out-of-scope modification as well as a potential ADA violation, and will exceed the contract funding requirements before the end of the period of performance. The OIG made 13 recommendations to assist the Agency in addressing these issues. The Agency provided planned actions in response to these recommendations. However, the planned actions did not fully meet the intent of two of the recommendations, concerning the lack of timely communication with the SBA and the investigation of the potential ADA violation.

Subsequent to the report's issuance, the Agency provided planned actions that, if completed, will meet the intent of these recommendations.

Summary of Reports for Which No Management Decision Was Made

No reports without management decisions were published.

Significant Revised Management Decisions

There were no significant revised management decisions regarding OIG reports.

Significant Management Decision Disagreements

There were no significant management decisions with which the OIG was in disagreement regarding OIG reports.

Audits

Audit Reports and Oversight Memoranda Completed in the Reporting Period

Audit of NSA's Facilities and Logistics Service Contract

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

Audit of the Agency's Retention Incentive Program

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

The OIG found administrative controls and oversight were limited. The Agency lacked controls over the retention incentives program, including a lack of Agency manager training, documented and consistent processes, and established long term goals. We found that this has resulted in retention incentive approval inconsistencies, overpayments, and noncompliance with Agency policy. In addition, without more defined program goals and a documented process for evaluating success, the Agency cannot determine whether the program is effectively expending Agency resources in retaining key personnel, and doing so without risk to other work roles and programs. Also, the OIG found that the Agency paid at least $4.2 million in unauthorized retention incentives. The Agency was not compliant with group retention incentive rules and policies. It paid group retention incentives over the limit authorized by Department of Defense (DoD) policy without a waiver and may have paid impermissible concurrent retention incentives. Compliance with the requirements of these incentive programs is essential to the Agency's success in retaining critical employees in a manner that is consistent with its obligation to be a careful steward of public funds.

The OIG concluded that the findings identified in this audit increased the risk of inefficient and improper payments, and potentially could jeopardize the availability of this important resource to retain employees essential to the Agency's success in meeting its critical mission. The OIG made 12 recommendations to assist the Agency in addressing these issues.

Audit of Enterprise-wide Space Utilization

The Agency's investments in spaces today impact its progress toward facilities space solutions for tomorrow's mission. The findings identified by the OIG during this audit demonstrated an increased risk that space is not being efficiently and economically utilized. Specifically, the OIG found:

- Agency space management was decentralized, and oversight of space was inadequate.
- The Agency lacked a current overall mid- or long-term strategic plan for IT space across the Enterprise.

- The Agency's space data was not current, accurate, or complete because the process for obtaining and tracking the data relies heavily on user input and because regular quality reviews on the data are not performed.
- There was no requirement for an analysis of alternative solutions when making space utilization decisions.

The OIG concluded that the Agency's lack of planning adversely impacts its readiness to meet future requirements. Moreover, the absence of effective oversight over the decisions leading to the creation of space requirements presents an environment that permits unchecked decision-making in directorate silos. With no evidence of due consideration as to whether resources expended on space utilization activities were appropriate, we determined that management controls over space utilization were not sufficient. The OIG made 14 recommendations to assist the Agency in addressing these issues and thereby improve its management of space utilization across the Enterprise.

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

The OIG audit of NSA's Fiscal Year 2019 Compliance with the Improper Payment Elimination and Recovery Improvement Act of 2012 (IPERIA) determined that NSA is in compliance with IPERIA. Using the procedures outlined in the Office of Management and Budget (OMB) Circular A-123, Appendix C, Requirements for Payment Integrity Improvement, 26 June 2018, the OIG found that the Agency complied with all six statutorily-required improper payment reporting requirements for the fiscal year that ended on 30 September 2019.

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

The overall objective of the audit, which may be divided into two reports, 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, 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 Security and Counterintelligence Efforts to Address Insider Threats

The purpose of this Congressionally-directed 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 this annual 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.

Audit of the Implementation of the Coronavirus Aid, Relief, and Economic Security (CARES) Act, Section 3610

In this audit, the OIG will determine whether NSA has economically, effectively, and efficiently implemented Section 3610 of the CARES Act with regard to payments made to Agency contractors.

Inspections

Inspection Reports and Oversight Memoranda Completed in the Reporting Period

Joint Inspectors General Report on Royal Air Force Menwith Hill (RAFMH)

The NSA OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the Royal Air Force Menwith Hill (RAFMH) during an inspection conducted jointly with inspectors from other U.S. Government OIGs. During the inspection, the joint OIG teams conducted focus groups, participants of which represented all segments of the military and civilian government workforce. The OIG teams also interviewed members of the RAFMH workforce and observed RAFMH operations and functions in mission operations; intelligence oversight; resource programs; IT and systems; safety, facilities, and emergency management; security; training; and mission systems and engineering.

Overall, the OIG found site personnel were encouraged by the communications with and restructuring efforts of site's senior leaders. We noted best practices in applying intelligence oversight training, collaborating to review IO processes, preparing temporary auditors, and managing machine room access. However, the OIG also identified a number of concerns for RAFMH, including:

- The lack of strategic direction for the site and the need to conduct an analysis to identify staffing needs;
- Outdated, incomplete, or missing documentation across several functional areas;
- A gap between NSA guidance on the loss of property, and a need for updated NSA security policies; and,
- A number of safety issues related to site facilities. The deteriorated condition of many of these structures poses great risk to personnel and mission, and there was no clear consensus on who is ultimately responsible for repairing or replacing them.

The OIG made a total of 121 recommendations in the report, 91 of which were assigned to NSAW, which had closed 24 prior to report issuance.

Ongoing Inspection Work

As the OIG has reconstituted its workforce during the COVID-19 pandemic, we have continued to work on the reports for inspections conducted between July and November 2019 that evaluated the overall climate and the compliance, effectiveness, and efficiency of the a number of sites, including:

- NSA Cryptologic Representative, U.S. Africa Command;
- NSA Cryptologic Representative, U.S. European Command; and
- Three other overseas sites.

The Inspections team had prepared to inspect four additional overseas locations in March and April 2020. When travel plans and attempts to conduct a virtual inspection were interrupted by the COVID-19 pandemic, the OIG revised its plans and intends to send memoranda to each site describing our assessment of the documentation provided and identifying any areas where that documentation does not meet the terms of applicable policy, regulation, or guidance.

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

Intelligence Oversight Reports and Oversight Memoranda Completed in the Reporting Period

Joint Review of Overhead SIGINT Compliance at a Joint Facility

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

Special Study of Certain Internet Capabilities, Part II

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

Review of Overcollect Compliance Incidents By Overhead Satellite Systems

At the request of the DoD Senior Intelligence Oversight Official (SIOO), the OIG reviewed reported overcollect compliance incidents involving unauthorized collection by overhead satellite systems for the period 1QCY2010 to 3QCY2018. All incidents discussed in the OIG's report were reported as noncompliant in quarterly *Reports to the Intelligence Oversight Board (IOB) on NSA Activities* following an NSA Office of General Counsel (OGC) legal determination. These reported compliance 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. Furthermore, the OIG found that inconsistencies in interpretation of incident reporting standards and incomplete guidance to the workforce raise a significant risk of less than complete incident reporting by NSA. The OIG made six recommendations to assist the Agency in resolving these weaknesses, including:

- Defining and documenting the legal framework for overhead satellite collection;
- Developing, documenting, implementing, and publicizing compliant operating procedures that address the risk to U.S. person information throughout overhead collection; and
- Developing, documenting, and implementing a process to use technical and/or personnel performance mitigation requirements to address recurring overhead overcollection compliance incidents.

Special Study of NSA's System Compliance Certification Process

The objective of this review was to assess the efficiency and effectiveness of NSA's system compliance certification (SCC) process. NSA's certification process is an important internal control meant to ensure that Agency mission systems comply with requirements derived from legal authorities, directives, and policies that protect civil liberties and individual privacy.

While the Agency has initiated efforts to improve guidance, training, procedures, and systems supporting the SCC process, our review revealed the following concerns:

- SCC requirements are not clearly aligned with the compliance standards from which they are derived.

- Several factors contribute to delays in the SCC process, including insufficient training.
- Compliance with SCC standard operating procedures is not enforced.
- NSA does not have a current, actionable plan to achieve certification for all systems.

While the Agency is taking some positive steps in this important area, the OIG determined that the findings identified indicate that the risk that NSA systems do not comply with the legal authorities, directives, and policies that protect civil liberties and individual privacy is not adequately mitigated. The OIG made 15 recommendations to assist the Agency in addressing these issues.

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 targeting system automates the targeting process and offers a one-stop shop for targeting that is conducted under a number of authorities at NSA. The objective of this review was to evaluate the accuracy, reliability, and effectiveness of the targeting system's control framework to ensure targeting complies with NSA's SIGINT authorities to protect U.S. person privacy.

The OIG's review revealed a number of deficiencies that have the potential to impact NSA's compliance with applicable laws and policies as well as the efficiency and effectiveness of the tool in support of NSA's mission, some of the most significant of which include:

- The targeting system does not synchronize with all necessary NSA systems and repositories because specific requirements to do so have not been levied.
- The rules for the system's targeting regime are opaque to users on NSANet and within the tool.
- Personnel selected as the targeting system's releasers for all authorities are assigned inconsistently, and FISA Section 702 adjudicators lack standardized, current training.
- Target information is not regularly updated in the targeting system and other NSA repositories, and the system does not provide reasonable assurance to confirm implementation of detargeting requests. Such insufficient or inconsistent information hinders analytic collaboration and may lead to unauthorized SIGINT acquisition.
- Targeting request processing timeliness fails to meet analyst expectations, particularly for the most critical request categories.

In total, the review of the targeting system's internal control framework revealed deficiencies that the OIG believes have the potential to impact the protection of USP privacy rights. The OIG made 25 recommendations to assist the Agency in addressing these issues.

Quick Reaction Report on the Evaluation of United States Person Identifiers Used to Query Against FISA Section 702 Data

During the course of an ongoing review of USP identifiers used as query terms against FISA Section 702 data, we discovered 15 Agency-known USP identifiers that appeared to have been queried in a particular NSA tool and to have bypassed the tool's internal control framework. The OIG brought its discovery to the attention of the Agency, which researched the issue and advised that it had determined that it had reasonable assurance that the issue was not caused by the tool.

The OIG therefore issued the QRR to request that NSA determine what happened and take appropriate steps to remediate and report to overseers as may be appropriate.

Ongoing Special Studies and Evaluations

Special Study of the Capabilities 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.

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.

Evaluation of 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.

Evaluation of NSA's Implementation of Title I FISA Authority

The objective of the evaluation is to assess the efficiency and effectiveness of the Agency's implementation of Title I FISA authority, to include evaluating compliance with the applicable targeting and minimization procedures as well as the efficiency and effectiveness of the controls designed to reasonably ensure the protection of individual civil liberties and privacy rights.

Investigations

Civil Prosecutions

iNovex Information Systems, Incorporated ("iNovex") located in Annapolis, MD, agreed in a settlement announced by the U.S. Attorney's Office for the District of Maryland to pay the United States $962,742 to resolve federal False Claims Act violations that, for over three years, iNovex knowingly billed the Agency for work performed by employees who did not meet the specialized qualifications under the contract. The OIG investigated iNovex after receiving a tip on the Hotline about suspected labor mischarging. The settlement resolved allegations that iNovex knowingly billed the Agency, and the Agency paid for work performed by iNovex employees who were identified by iNovex on the invoices to the Agency as System Administrator-IV and System Administrator-III positions, despite the fact that those employees did not timely obtain a specific required certification for those labor categories. The settlement was not an admission of liability by iNovex, nor a concession by the United States that its claim was not well founded.

Agency Referrals

In addition to the case 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 two 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 contractors submitting false labor charges. The OIG anticipates that the government is likely to handle both cases administratively, rather than criminally.

The Investigations Division referred six new cases involving Agency personnel to NSA Employee Relations (ER) for potential disciplinary action. During the reporting period, the Agency notified the OIG of disciplinary actions for seven employees based on current and prior OIG reports. Two employees retired or resigned in lieu of removal, one employee resigned prior to disciplinary action being proposed, one employee received a suspension of 10 days or less, and three employees received written reprimands or counseling. A total of 16 cases referred by the OIG to ER were pending action, as of the end of the period.

Seven cases substantiating contractor misconduct were referred to the Agency's Procurement Office for action, resulting in the recoupment of approximately $1,194,587. Two cases substantiating employee timecard fraud were referred to the Agency's Payroll Office, resulting in the recoupment of $33,421.

OIG Hotline Activity

The Investigations Division fielded 393 contacts through the internal OIG hotline. The OIG received 5,307 submissions on the external OIG hotline.

Significant Investigations

Former Senior Executive: Representation to the Agency

An OIG investigation determined that a former senior executive, who was at the time of the incident a re-employed annuitant and also an employee of a non-profit entity, represented that entity before the Agency at a meeting in violation of 5 C.F.R. § 2635.801(d)(3) and 5 C.F.R. § 2635.802(a). The OIG did not find that the employee acted intentionally in violating any of these provisions.

The findings were also forwarded to the NSA 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 9 March 2020 and declined for consideration of prosecution.

Senior Executive: Abuse of Authority

An OIG investigation concluded that a senior executive did not abuse their authority when making a decision to restrict a subordinate's TDY travel. The investigation revealed that the senior executive's action was not arbitrary or capricious and was in fact based on mission requirements.

The investigative findings were forwarded to DoD IG.

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

GG-15: Joint Travel Regulation

An OIG investigation concluded that a GG-15 employee violated Joint Travel Regulations (JTR) by canceling an original official travel airline ticket, and then using personal frequent flyer miles for the official travel. The employee then claimed reimbursement for $1,267 of official airline travel costs. This was an issue that was identified in the OIG's *Audit of the Agency's Travel Program* (AU-18-003, 1 February 2019), an unclassified version of which was released by the OIG on 4 March 2019.

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.

Whistleblower Reprisal

An OIG investigation found that a senior executive did not reprise against a subordinate for making protected communications to the OIG. The investigation determined that the complainant had made a protected disclosure and thereafter suffered an adverse personnel action. However, the investigation found by clear and convincing evidence that the employee would not have received an end of year performance bonus absent the protected disclosures.

The investigative findings were forwarded to DoD IG.

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

Summary of Additional Investigations

NSA OIG opened 6 investigations and 22 inquiries, while closing 11 investigations and 25 inquiries during the reporting period. The new investigations involve a variety of allegations, including whistleblower reprisal, misuse of Government resources, and violations of time and attendance and contract billing policies.

Contractor Labor Mischarging

NSA OIG opened one contractor labor mischarging investigation and substantiated two cases. The substantiated cases closed during the reporting period resulted in the proposed recoupment of approximately $106,916. Six investigations remain open.

Time and Attendance Fraud

NSA OIG opened one new investigation into employee time and attendance fraud and substantiated one such case during the reporting period. The substantiated case resulted in the proposed recoupment of approximately $31,670. Disciplinary action against eight employees for time and attendance fraud is pending with the Agency. Four investigations remain open.

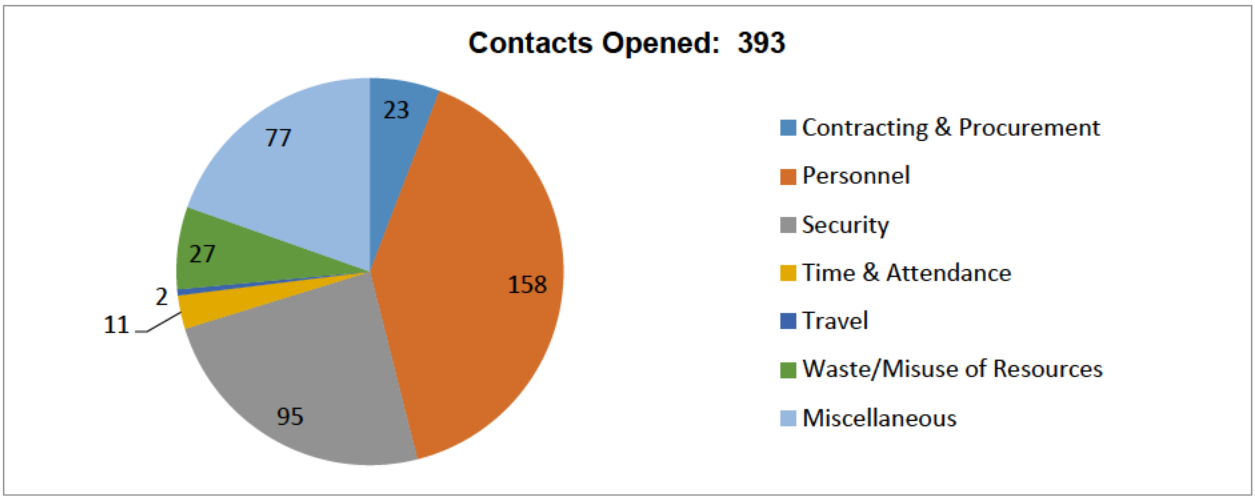
Computer Misuse

NSA OIG opened two new investigations involving allegations of computer misuse. Three investigations remain open.

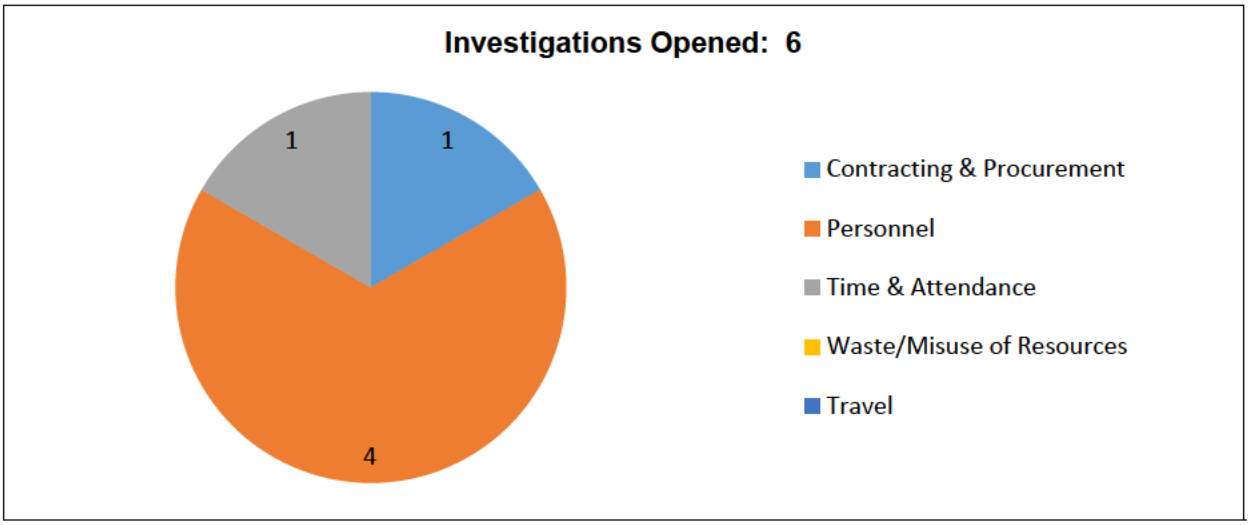
Investigations Summary

Total number of investigative reports issued	11
Total number of persons reported to DOJ for criminal prosecution	2
Total Number of Persons Referred to State and Local Authorities for Criminal Prosecution	0
Total Number of Indictments	0
Data contained in this report and table were obtained from NSA OIG Electronic Information Data Management System (eIDMS))	

Total Hotline Contacts Received



Investigations Opened



Peer Review

No peer reviews were performed during the current reporting period.

Whistleblower Coordinator Program

As previously reported, the OIG worked with the Agency to develop a new training program on whistleblower rights and protections, which the Director made mandatory for all Agency personnel with a completion deadline of 30 September 2020. A number of employees who took the training during this reporting period provided positive feedback to the OIG on it, indicating that they better understood their rights and protections and felt more comfortable with the reporting process. We will continue to refine the program based upon comments received.

The OIG continues all of its efforts to promote whistleblower rights and protections, including various types of outreach to Agency personnel with respect to whistleblower reprisal. At the end of September, IG Storch briefed the new class of senior executives on their obligations to ensure that employees reporting waste, fraud, abuse, and misconduct do not suffer any reprisal for doing so, and provided guidance as to how, as Agency leaders and managers, they can ensure that whistleblower rights are appropriately protected. The OIG will continue to be forward leaning in exploring opportunities to ensure that all persons at NSA feel comfortable coming forward with information regarding suspected wrongdoing, and that they never suffer retaliation for doing so.

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

Audits

Mission and Mission Support

Audit of NSA's Facilities and Logistics Service Contract

Audit of Enterprise-wide Space Utilization

Audit of the Agency's Retention Incentive Program

Financial Audit

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

Inspections

Enterprise Inspections

Joint Inspectors General Report on Royal Air Force Menwith Hill (RAFMH)

Intelligence Oversight

Joint Review of Overhead Compliance at a Joint Facility

Special Study of Certain Internet Capabilities, Part II

Review of Overcollect Compliance Incidents by Overhead Satellite Systems

Special Study of NSA's System Compliance Certification Process

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

Quick Reaction Report on the Evaluation of United States Person Identifiers Used to Query Against FISA Section 702 Data

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 (including Unsupported Costs)	Unsupported Costs
For which no management decision had been made by start of reporting period	0	0	0
Issued during reporting period	2	~ $460,000,000	~ $420,000,000
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

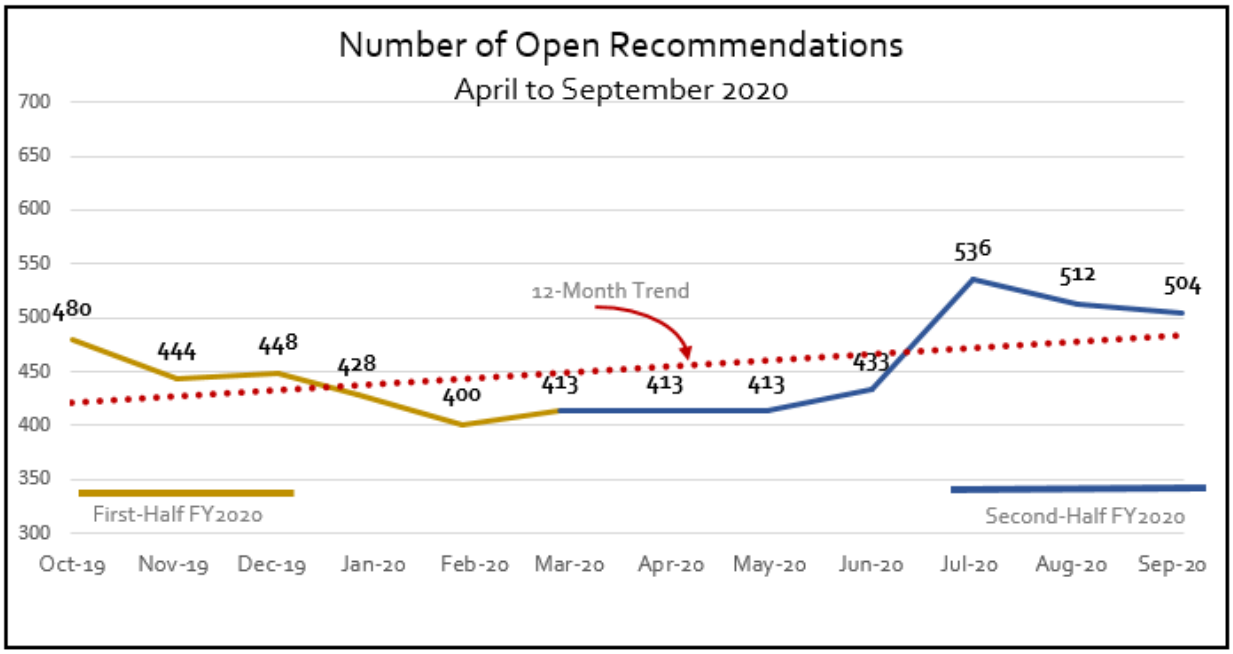
The OIG made 221 recommendations to NSA management in reports and oversight memoranda issued during this reporting period. The Agency closed 53 of the newly published recommendations and a total of 130 recommendations during the reporting period.

Outstanding Recommendations

The OIG considers a report open when one or more recommendations contained in the report have not been closed. The number of open recommendations is the total contained in 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.

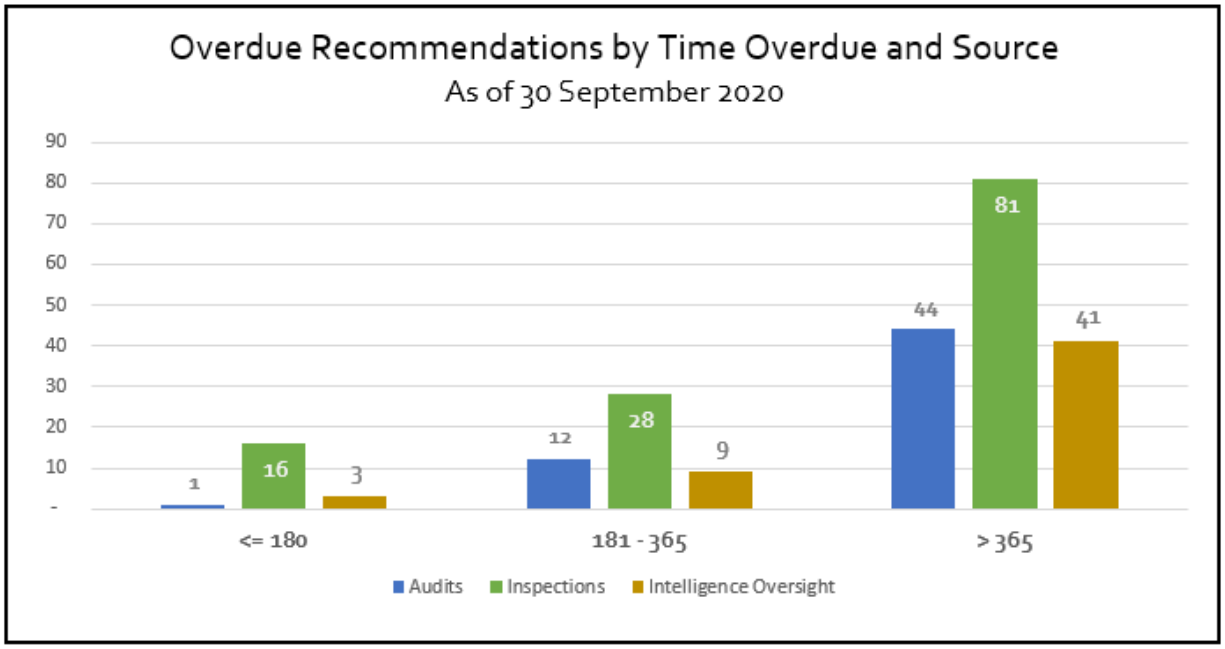
Outstanding Recommendations

	Audits	Inspections	Intelligence Oversight	Total
Open reports	30	35	22	87
Open recommendations	111	246	147	504
Overdue recommendations	57	125	53	235
Overdue recommendation as % of total open	**51%**	**51%**	**36%**	**47%**



Overdue Recommendations Breakdown

Days Past Target Completion Date	Audits	Inspections	Intelligence Oversight	Total	Percent Overdue
<= 180	1	16	3	20	9%
181 - 365	12	28	9	49	21%
> 365	44	81	41	166	71%
Totals	**57**	**125**	**53**	**235**	



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. Of the nine management referrals, eight were closed based upon Agency action, and one 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 implemented such a solution for software acquisitions. However, for hardware acquisitions, the Agency stood up a working group to develop a strategy 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 noncompliance 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.
- 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 September 2021.