Office of the Inspector General
National Security Agency

Semi-Annual Report to Congress

1 October 2018 to 31 March 2019

Office of the Inspector General

Pursuant to the Inspector General Act of 1978, as amended, and in accordance with NSA/CSS Policy 1-60, the NSA/CSS Office of the Inspector General (OIG) conducts independent oversight that promotes Agency respect for Constitutional rights, adherence to laws, rules, and regulations, and the wise use of public resources. Through investigations and reviews, we detect and deter waste, fraud, abuse, and misconduct, and promote the economy, efficiency, and effectiveness of Agency operations.

Audits

The Audit Division conducts audits to evaluate the economy, efficiency, and effectiveness of NSA operations and programs, to assess Agency compliance with laws and regulations and whether or not internal controls are in place and operating effectively, and to opine on whether or not Agency financial statements are fairly presented. The Audits Division is divided into three areas of focus: Cybersecurity and Technology, Mission and Mission Support, and Financial audits. Audits are conducted in accordance with generally accepted government auditing standards established by the Comptroller General of the United States.

Inspections

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

Intelligence Oversight

Intelligence oversight (IO) works to ensure that NSA intelligence and intelligence-related activities comply with federal law, executive orders, and Intelligence Community (IC), Department of Defense, and NSA policies, and that Agency activities are conducted in accordance with civil liberties and individual privacy protections. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

Investigations

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

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

A Message from the Inspector General

I am pleased to present the Semiannual Report to Congress (SAR) of the National Security Agency/Central Security Service (NSA) Office of the Inspector General (OIG) for the period 1 October 2018 through 31 March 2019. The SAR describes a significant body of work by this office that is diverse in subject matter, but unified by the OIG's vision to promote positive change through impactful oversight at this critically important agency.

As I write this, it has been more than 15 months since I came on board as the Inspector General here. One area that we at the NSA OIG have emphasized during that period is increasing the impact of our oversight work. In that regard, the OIG has taken a number of steps to foster more timely action by the Agency in response to recommendations made in our prior reports and reviews. In the SAR we issued one year ago, we reported that, as of March 31, 2018, there were 699 recommendations that were open, meaning that the Agency had not yet taken action sufficient to meet the intent of the recommendations. Of these, 534, or approximately 76% were reported as overdue, meaning that they had remained open beyond their target completion dates, and significant numbers of those were overdue for extended periods of time.

The OIG has implemented a number of measures to assist the Agency in addressing such outstanding recommendations, including elevating the level of accountability for recommendations, generally to the Directorate level or its equivalent where there is authority to direct responsive actions, and implementing a requirement for bi-monthly status reports to help ensure that ongoing progress is being made toward completion of the agreed-upon actions. The Director and others in Agency leadership have emphasized to management and across the workforce the importance of taking timely action to meet OIG recommendations and, for that, we are grateful. And I want to particularly acknowledge the efforts of the leadership of the Directorates and their staffs, who have taken on greater responsibility during this period for ensuring action on open recommendations. Even though the OIG issued 34 new reports and oversight memoranda containing 818 new recommendations over the past year, this SAR reports that the total number of open recommendations has dropped to 596, a year-to-year decrease of 15%. There also has been a reduction over the past year in the number of overdue recommendations to 427, a drop of 20% from the same time last year. The numbers and percentages of recommendations overdue for periods of more than six months and more than a year have increased, reflecting that some of the most difficult actions remain. However, it is clear that there has been increased focus at the Agency on responding to the issues identified in the OIG's work, and in the long run, this will enhance the impact of our efforts to promote positive change here.

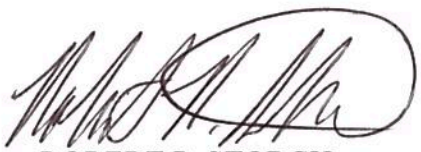
The reports and reviews issued by the OIG during this past reporting period address a wide range of Agency programs and operations. These include reviews in which we identified significant issues and made recommendations for improvement in areas ranging from the Agency's controls to comply with requirements for the retention and age-off of signals intelligence (SIGINT) data to its use of award fee contracts. Agency management agreed with all OIG recommendations made during this period. Moreover, the oversight role of the OIG includes both such programmatic reviews and misconduct investigations – in the latter area, the OIG fielded 457 new contacts during the past 6 months, resulting in the initiation of 27 investigations and 64 inquiries. We also referred

49 cases involving Agency personnel to NSA Employee Relations for potential disciplinary action, and we have several criminal matters pending with the U.S. Attorney's Office. The OIG also has continued to emphasize the importance of whistleblower rights and protections as central to effective government and to the ability of the OIG to obtain information necessary to our work. In addition to our ongoing outreach efforts in this area, we substantiated three cases during this reporting period involving reprisals for making protected disclosures, referring our findings to appropriate authorities. While it is not possible to draw meaningful conclusions from such a limited number of cases, we will continue to be vigilant in this area and all of our investigative efforts to address waste, fraud, abuse, and misconduct.

Another core area for the OIG is enhancing the transparency of our oversight work, and we continued to move forward on this score during the reporting period. Following the public release of our initial unclassified SAR and the roll out of our independent website, https://oig.nsa.gov, during the last reporting period, we followed up during this period with the public release of our second unclassified SAR, and, thereafter, with the public release of our first-ever unclassified audit report. That report, our *Audit of the Agency's Travel Program*, revealed a number of significant issues involving the misuse of travel cards and the Agency's management of its travel program. As I write this message, we have recently released a second unclassified report, and we will continue to look for other opportunities to enhance the transparency of our oversight work. Such transparency is important so that taxpayers can know that their money is being spent legally and wisely, and that is particularly true at an agency such as the NSA, where so much of what is done must remain outside of the public eye in order to be effective.

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. The Agency also has supported the OIG's efforts to increase its ongoing engagement across the Extended Enterprise, including our designation of specific points of contact for the OIG Investigations Division with each of the Cryptologic Centers, and we are exploring additional avenues to increase such valuable interactions.

In closing, I would like to express my, and my office's appreciation for the work of Jim Protin, who served as Counsel to the IG, Assistant IG for Investigations, and, most recently, Acting Deputy IG. Jim had an outstanding career in military and civilian service, and his contributions to the OIG were immeasurable. I often relied on his outstanding judgment (apart from his support for the Pittsburgh Steelers), and we at the OIG wish him all the best in the future.



ROBERT P. STORCH

Inspector General

DISTRIBUTION:

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

Contents

Index of Reporting Requirements

§5(a)(1)	Significant problems, abuses, and deficiencies	3–6
§5(a)(2)	Recommendations for corrective action	3–6
§5(a)(3)	Significant outstanding recommendations	29-31
§5(a)(4)	Matters referred to prosecutorial authorities	16
§5(a)(5)	Information or assistance refused	iv
§5(a)(6)	List of audit, inspection, and evaluation reports	24
§5(a)(7)	Summary of particularly significant reports	1–2
§5(a)(8)	Audit reports with questioned costs	25
§5(a)(9)	Audit reports with funds that could be put to better use	25
§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)	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	22
§5(a)(15)	List of outstanding recommendations from peer review of NSA OIG	N/A
§5(a)(16)	List of peer reviews and outstanding recommendations conducted by NSA OIG	22
§5(a)(17)	Statistical tables of investigations	20-21
§5(a)(18)	Description of Metrics used in statistical tables of investigations	21
§5(a)(19)	Reports concerning investigations of Seniors	17-18
§5(a)(20)	Whistleblower Retaliation	18-19
§5(a)(21)	Agency interference with IG Independence	iv
§5(a)(22)	Disclosure to the public	iv
§5(a)(note)	P.L. 110-181 §845, Final completed contract audit reports	
§5(a)(note)	P.L. 103-355 (as amended), Outstanding recommendations past 12 months	26-29
* IG Act of 1978, as amended, including the IG Empowerment Act of 2016.		

This page intentionally left blank.

OIG Executive Summary

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

Audit Division

The Audit Division of the NSA OIG is divided into three branches – Cybersecurity and Technology, Mission and Mission Support, and Financial Audit. During this reporting period, the Audit Division issued a total of 7 reports containing 47 recommendations to improve Agency operations. These products consisted of five audit reports, an evaluation report, and an examination report.

The Cybersecurity and Technology branch performed a review of the *NSA's Implementation of the Federal Information Security Modernization of 2014 (FISMA).* We evaluated eight information technology (IT) security areas against applicable metrics, and determined that there is 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 Mission and Mission Support branch performed an audit of the *Agency's Travel Program*. The findings identified by the OIG in this audit identified risks of improper entitlement payments and ineffective management of a program that in FY17 processed 43,579 claims totaling $69.4 million dollars. Specifically, we found that Agency personnel did not adequately monitor cardholder activities, which may have permitted improper cash advances and other misuse of individually billed travel cards. We also made several other findings, including that the Agency did not reconcile centrally billed travel charge card accounts in a timely fashion, and that it failed to provide mandatory travel card training. These risks potentially impact the Agency's financial liability and public trust in its stewardship of taxpayer dollars. We also issued a report on the NSA's use of award fee contracts, which involve less objective measures of performance and, therefore, require documentation as to their need, the cost-benefit analysis supporting their use, and the basis for the award fee percentage ranges available under the contracts. For the contracts we examined, we found that these requirements frequently were not met, resulting in our questioning all of the $636 million in fees awarded pursuant to them. We also found that, while the use of award fee contracts across the Department of Defense has dropped markedly, the Agency's use of such contracts has increased, and that the Agency was not collecting or analyzing data to determine if it was achieving the desired benefit from their use. In both of these reports, the OIG made recommendations to the Agency to assist it in improving its operations.

The Financial Audit branch focused during this reporting period on the congressionally mandated *Audit of NSA's Financial Statements,* which revealed a number of material weaknesses as summarized in the Report on Internal Control. In addition, the Financial Audit branch oversaw a service organization control examination related to the Agency's performance of certain financial processing services on behalf of the Defense Intelligence Agency.

Inspections Division

The OIG issued three inspection reports during this reporting period, and conducted three new inspections, all on field sites. The Agency and all sites fully cooperated with our work, which resulted in a wide range of recommendations for improvements in operations. The Inspections Division was also the subject of a Peer Review, conducted by representatives from the NGA, DIA, CIA and IC IGs. The results of the Peer Review are pending.

Intelligence Oversight

The OIG's Intelligence Oversight Division issued two reports on special studies and one quick reaction report during the reporting period. One of the special studies addressed whether NSA deleted all USA Freedom Act data ingested prior to 23 May 2018 from NSA repositories identified by the Agency following its receipt from telecommunications service providers of call dialing records that the NSA was not authorized to receive. The other special study addressed NSA's implementation of controls to comply with SIGINT retention requirements, specifically the aging-off of SIGINT data collected pursuant to Executive Order 12333, as amended, and the Foreign Intelligence Surveillance Act of 1978 (FISA), including the FISA Amendments Act (FAA) of 2008, as amended. The quick reaction report identified the need for NSA to determine what circumstances represent noncompliance with the Department of Defense Directive 5148.13, *Intelligence Oversight*, intelligence oversight familiarization training requirement, and whether those circumstances are violations reportable to the President's Intelligence Oversight Board. In total, 14 recommendations were made in these reports to assist the Agency in improving its operations and to increase compliance with requirements for protecting civil liberties and individual privacy.

Investigations

During this reporting period, the Investigations Division received and processed 457 contacts, which resulted in the initiation of 27 investigations and 64 inquiries. Four new investigations involved allegations of whistleblower reprisal, two involved allegations of ethics violations, one involved allegations of violations of the Uniformed Services Employment and Reemployment Rights Act, and one involved allegations of nepotism. Twenty-nine investigations and 65 inquiries were closed during the reporting period, resulting in the proposed recoupment to the Agency of approximately $90,000 from employees and approximately $236,000 from contractors. As a result of OIG investigations, disciplinary actions ranging from termination to reprimands were taken against eight employees. Three cases referred to the U.S. Attorney for the District of Maryland are pending resolution, and four other referred cases were declined for prosecution.

Whistleblower Program

The Inspector General continues to make whistleblower rights and protections a priority. At the annual Intelligence Community Inspector General Conference in March, he hosted a widely attended whistleblower panel that brought together representatives of the Inspector General community and a leading non-governmental advocate to discuss a variety of topics and concerns. The NSA OIG is also developing additional outreach materials and an on-line whistleblower training presentation that we hope will be available to all NSA employees in the near future.

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:

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

The OIG conducted this study to evaluate NSA's implementation of controls to comply with requirements for aging-off SIGINT data collected pursuant to Executive Order (E.O.) 12333, *United States Intelligence Activities*, as amended, and the FISA, including the FAA of 2008, as amended. Requirements for retention of SIGINT collected under these authorities are established by statute, minimization procedures, national policies, specific Court orders, and NSA policies.

The study revealed the following primary concerns:

1. NSA's primary content repository has retained a small percentage of the large number of SIGINT data objects beyond legal and policy retention limits in the two data stores tested. NSA has not fully implemented age-off calculations that use the most specific retention requirement with which data objects are labeled. The current process to verify key elements of SIGINT data objects prior to their ingestion in the primary content repository is insufficient, though NSA has implemented an improved ingest validation process for 93% of the SIGINT data (and about 11% of the data feeds) being entered in the primary content repository;

2. Planned updates to NSA retention policy and legal and policy working aids have been delayed and do not incorporate all current law and policy;

3. Current oversight must be strengthened if it is to ensure compliance with retention requirements; and

4. Implementation of age-off for some SIGINT collection authorities in some databases was not in compliance with NSA/CSS Policy Instruction 2-0001, *Early Age-off Decisions for Unevaluated or Unminimized Signals Intelligence*.

The OIG's findings reflect significant risks of noncompliance with legal and policy requirements for retention of SIGINT data. These requirements include established minimization procedures for NSA SIGINT authorities, meaning that the deficiencies we identified have the potential to impact civil liberties and individual privacy. The changes to the Agency's ingest validation process (described above) are an effort to improve its age-off methodology and the accuracy of the information used to determine age-off. We believe implementation of this process for all types of SIGINT data is needed. Overall, we made 11 recommendations to assist NSA in addressing the risks, and ensuring that data retention is conducted in accordance with all applicable requirements and privacy rights.

Audit of Award Fee Contracts

The OIG conducted this audit of award fee contracts because of the magnitude of the Agency award fee contract pools and the significant potential financial risk to the Agency and increased administrative burden associated with effectively managing award fee contracts. The OIG questioned all $636 million in award fees associated with 54 contracts from FY2016 and 2017 that we examined during the audit. The OIG found that the Agency did not properly support either a) the use of award fee contracts, which are only to be used when contract performance cannot be measured objectively, or b) that the award fee percentages established under the contracts were properly justified, documented, and in the best interest of the Government. The OIG also found that from FY2010 to FY2017 the Agency's obligations for award fee contracts more than doubled, growing by 139%, while DoD award fee obligations from FY2010 through FY2015 declined from approximately $34 billion to less than $10 billion because they are moving toward objective incentive arrangements. Finally, the Agency did not collect or analyze data to evaluate the effectiveness of its use of award fees. The OIG made three recommendations to assist the Agency in addressing these findings. The Agency agreed with all the recommendations and the OIG concluded that the actions planned by Agency management met the intent of the recommendations.

Audit of NSA's FY2018 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 FY2018, we found that material weaknesses exist in the Agency's ability to provide documentation to support the financial statement assertions.

1. **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. 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. However, a significant number of equipment assets were neither subjected to a valuation methodology nor reported in the financial statements. In addition, there were a high number of instances in which assumptions could not be validated or procedures could not be re-performed based upon information provided by NSA. For assets in the possession of contractors, NSA relies on the accuracy of information provided by its contractors. NSA was not able to substantiate the accuracy or reasonableness of information reported by contractors for 78 percent of government furnished property assets, including assets such as information systems. In addition, the Agency did not consider the underlying nature of certain leasing agreements, and lacked procedures over the Construction-In-Progress accrual related to Military Construction projects executed by the U.S. Army Corps of Engineers on behalf of the Agency. As a result, NSA could not ensure that its General PP&E balances were complete, accurate, and properly valued.
2. **Accounts Payable Accrual** NSA did not design and effectively implement policies, procedures, or controls to validate critical assumptions used in its accounts payable accrual estimation methodology, which is used to estimate amounts owed to vendors and other

government agencies for goods and services. Such validation should be periodically re-performed and subjected to appropriately designed management review controls to ensure that circumstances have not changed that would require revision to previously determined assumptions. Without complete and accurate validations of material assumptions, NSA may not be able to determine if assumptions used in its accrual estimation methodology are appropriate, increasing the risks that the balances recorded are inaccurate.

3. **Budgetary Activity** NSA did not design and implement control activities to effectively monitor, identify, and deobligate invalid obligations in a timely manner. In addition, 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 has 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. NSA did not establish processes to readily retrieve original supporting documentation to support receipt and acceptance of goods or services provided by certain intragovernmental trading partners.

4. **Fund Balance with Treasury (FBwT) and Deposit Funds** NSA did not have fully effective processes to provide adequate and complete supporting documentation for historical disbursements and collection transactions that contribute to the FBwT beginning balance, which reflects account balances held by the U.S. Treasury from which NSA can pay for its operations. Further, NSA and Defense Finance and Accounting Service (DFAS) did not adequately demonstrate that appropriately designed processes and controls had been implemented over the FBwT reconciliation process between DFAS and Treasury. Additionally, NSA did not ensure that internally generated documentation related to deposit funds was reconcilable to external third party documentation.

5. **Financial Reporting** NSA did not implement sufficient processes to obtain or maintain adequate documentation to support manual journal entries, which generally bypass the routine business process of a transaction’s flow and the associated internal controls of an accounting system. In addition, NSA did not ensure that adequate evidence of supervisory review was obtained. Without adequate supporting documentation, NSA could not ensure it accurately recorded and properly approved manual journal entries. As a result, there was a risk that journal entries could be processed for inappropriate activity or amounts, causing misstatements to NSA’s financial statements.

6. **Control Environment and Monitoring** NSA personnel, at all levels of the organization, may not have established adequate corrective action plans and timetables to respond to the complexity of the underlying control deficiencies. In addition, recruiting, developing, and retaining a skilled workforce is a challenge of any organization, and is heightened by the additional security clearance requirements for all NSA candidates and personnel. It appears that the resource constraints encountered during FY2018 may have required NSA managers to prioritize certain internal controls, and resulted in reductions to the number of personnel assigned to other internal controls. Further, NSA did not fully design or implement adequate controls to evaluate the segregation of duties justifications to ensure that mitigating controls were designed and operating effectively throughout FY 2018. As a result, there was a risk that a financial statement misstatement could occur without detection.

While there has been progress in a number of important respects, five of these areas, PP&E, Accounts Payable Accrual (which previously was under Procurement Activity), Budgetary Activity, FBwT, and Control Environment and Monitoring continue from the FY2017 financial statement audit.

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 decision disagreements were published.

Audits

Audit Reports and Oversight Memoranda Completed in the Reporting Period

Audit of the Post-Publication of Serialized SIGINT Reports

Post-publication of serialized SIGINT reporting facilitates the release of National Security Agency information to customers of NSA serialized reporting. The OIG conducted this audit because there were risks identified with post-publication related to the lack of documented roles and responsibilities and the OIG had not reviewed this topic before. The OIG found problems throughout the post-publication process, including the fact that many requests were not processed in accordance with established timelines, with approximately 50 percent of requests submitted from September 2016 through August 2017 not meeting the handling precedence goals. In addition, the Agency had not implemented effective controls or processes to ensure that request tasking and customer responses were consistent and accurate, did not have a formal quality-control process, and had not adequately trained all personnel handling post-publication requests. All of these problems increase the risk of releasing information to unauthorized recipients. The OIG made 11 recommendations to assist the Agency in addressing these issues.

FY2018 *Review of the NSA/CSS Implementation of the Federal Information Security Modernization Act of 2014*

In accordance with U.S. Office of Management and Budget guidance, the OIG is required to assess the effectiveness of information security programs on a maturity model spectrum, which ranges from Level 1 (ad hoc) to Level 5 (optimized). The review found that there is room for improvement in all eight IT security areas.

Table 1. Overall Maturity Levels

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

Contingency planning was assessed as the weakest security area with an overall maturity level of one, ad hoc. The review found that five areas were Level 2, defined but not consistently implemented, and the remaining two areas were Level 3, consistently implemented but lacking quantitative and qualitative effectiveness measures.

NSA's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Controls

We contracted with an independent public accounting firm to perform an examination of NSA's description of its system supporting the performance of financial processing services on behalf of another U.S. Government organization for the period of October 1, 2017, through June 30, 2018, and the suitability of the design and the operating effectiveness of controls to achieve the related control objectives stated in the description. The examination noted certain exceptions, including with the design and operating effectiveness of controls, which resulted in a qualified opinion.

Audit of NSA's FY2018 Financial Statements

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

Audit of Agency's Travel Program

The OIG conducted this audit of the Agency's travel program because of the inherent risk related to reimbursing travel expenses using Government Travel Charge Cards, and other OIGs have found control weaknesses and abuses in their Government Travel Charge Card Program. The OIG found that the NSA had internal controls to obligate, process, and pay travel entitlements. However, the audit identified a number of concerns, including that the NSA did not adequately monitor cardholder activities, which may have permitted improper cash advances and other misuse of individually billed travel cards. The OIG determined that, in a 9-month period from January through September 2017, travel cardholders spent approximately $900,000 on questionable transactions, of which at least $285,000 was determined by the OIG to be inappropriate. The OIG referred a number of these transactions to its Investigations Divisions, which substantiated misuse and referred the employees involved to the Agency for possible disciplinary action. The audit also detailed a number of other findings, including that the Agency's centrally billed travel charge card account was not reconciled in a timely fashion, creating a balance owed of more than $130,000; the Agency did not require travel card training for travelers, managers, or authorizing officials; and the Agency's travel management information systems were in need of modernization. The OIG made 10 recommendations to assist the NSA in ensuring that its travel program is managed appropriately and compliantly. The Agency agreed with all the recommendations, and the OIG concluded that the actions planned by Agency management met the intent of the recommendations.

Audit of Award Fee Contracts

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

Audit of NSA's Nuclear Command and Control Program

Producing and distributing Nuclear Command and Control Information Assurance Material that provides the codes needed to safeguard and validate use of nuclear weapons are two important functions for NSA. Due to the importance of the Nuclear Command and Control (NC2) mission, the OIG agreed with the Agency in 2001 to perform periodic reviews of the NC2 program. In the prior reporting period, the OIG issued an audit regarding NC2 system security controls. In this second audit, the OIG examined the NSA's NC2 program to assess mission critical aspects including governance, mission assurance, personnel, and facilities.

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

Ongoing Audits

Audit of NSA's Chief Information Officer (CIO) Authorities

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

Audit of NSA Corporate Authorization Service (CASPORT)

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

Audit of NSA's Internal Controls Over Second Party Integrees

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

Joint Audit of Intragovernmental Transactions

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

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

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

Audit of NSA's Information System Decommissioning Process

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

Audit of NSA's Facilities and Logistics Service Contract

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

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

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

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 FY2018 Compliance with the Improper Payments Elimination and Recovery Improvement Act of 2012

The overall objective of the audit is to determine whether the Agency is in compliance with the Improper Payments Elimination and Recovery Improvement Act using the OIG procedures in the Office of Management and Budget Circular A-123 Appendix C, *Requirements for Payment Integrity Improvement*, 26 June 2018.

Review of the Agency's Nuclear Weapons Personnel Reliability Program

The overall objective of the review is to determine whether the Agency's Nuclear Weapons Personnel Reliability Program complies with applicable Department of Defense and Agency guidance.

FY2019 Statement of Standards for Attestation Engagement 18, NSA's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Controls

The OIG contracted with an independent public accounting firm to conduct a Type II Service Organization Controls 1 examination and express an opinion on whether (1) NSA management's description of systems fairly presents the systems designed throughout the period 1 October 2018 through 30 June 2019; (2) controls related to the control objectives identified in management's system description were suitably designed throughout the specified period; and (3) controls selected for testing operated effectively to provide reasonable assurance that the control objectives in NSA management's system description were achieved through the specified period.

Audit of NSA's FY2019 Financial Statements

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

Audit of the Agency's Retention Incentive Program

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

Inspections

Inspection Reports and Memoranda Completed in the Reporting Period

Inspection of NSA Kent Island

The OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of NSA's Kent Island (KI) facility during a 4 to 5 June 2018 inspection. The OIG reviewed pertinent documents, support agreements, policies, regulations, and intelligence oversight data. Inspectors conducted interviews with members of the KI workforce and site leadership, and hosted a focus group session to assess the morale, quality of life, human and material resources, and issues of concern to the workforce. Inspectors observed site operations and functions in resource programs, information technology systems, mission operations, intelligence oversight, and safety, facilities, and security.

The OIG noted that KI had a solid program in the areas of Mission Operations and Intelligence Oversight training and knowledge. Nevertheless, although KI is a relatively small site, the OIG identified several concerns, particularly regarding security, safety, and facilities. Overall, the OIG made 45 recommendations to assist KI and the Agency in addressing the findings identified during the inspection, and 23 of the 45 were resolved prior to the publication of this report.

Joint Inspectors General Inspection Report - Alaska Mission Operations Center (AMOC)

The NSA, Army Intelligence and Security Command, U.S. Fleet Cyber Command, and 25th Air Force OIGs Joint Inspection team evaluated the overall climate and the compliance, effectiveness, and efficiency of the Alaska Mission Operations Center (AMOC) during a 16 through 20 July 2018 inspection. The inspection included 11 focus groups, participants of which represented all segments of the military and civilian government workforce at the AMOC. In addition, the OIG team reviewed pertinent documents, support agreements, policies, and regulations. Further input came from AMOC employee responses to the AMOC 2018 Organizational Assessment Survey, which also included data from the May 2017 Intelligence Community Employee Climate Survey. The OIG interviewed members of the workforce and observed site operations and functions in mission operations; intelligence oversight; communications and computers; resource programs; safety, security, facilities, continuity of operations, and emergency management; and training. The OIG also interviewed senior site leaders and senior NSA leaders responsible for AMOC missions.

The OIG identified a number of concerns at AMOC, including mission inefficiencies possibly resulting from the local Directorate of Operations (DO) structure, incomplete resources documentation, and issues related to facilities safety. For information technology (IT), the OIG found some incomplete records and insufficient labeling of IT equipment. The OIG made 52 recommendations and 6 observations to assist the AMOC and the Agency in addressing the findings identified during the inspection. The OIG noted four commendables at AMOC, which highlighted best practices in the areas of intelligence oversight, data center management, and personnel accountability.

Ongoing Inspection Work

Joint Inspectors General Inspection Report - NSA Hawaii: 4 to 14 September 2018

Inspection of NSA/CSS Representative (NCR) Pacific Command (PACOM), 12 to 18 September 2018

Inspection of NCR US Transportation Command (USTRANSCOM), 29 to 30 January 2019

Special Study on the Assignment of Military Affiliates to NSA

The overall objective was to examine if there are any impediments to military affiliates' obtaining access to NSA's classified information and secure facilities. The Inspections Division performed this study in an effort to better understand possible root causes for the concerns raised during the OIG inspections of NSA Georgia, NSA Texas, AMOC, and NSA Hawaii.

Intelligence Oversight

Special Studies and Oversight Memoranda Completed in the Reporting Period

Quick Reaction Report: Determination Needed on Department of Defense Directive on Intelligence Oversight

The OIG issued this quick reaction report identifying the need for NSA, through its Office of General Counsel, to determine what circumstances represent noncompliance with the intelligence oversight familiarization training requirement contained in Department of Defense Directive 5148.13, *Intelligence Oversight*, and whether those circumstances are violations reportable to the President's Intelligence Oversight Board. The OIG made one recommendation to the Agency to address the issue identified in the report, and the Agency has accepted the recommendation for action.

Report on the Review of the NSA/CSS's Deletion of Certain USA FREEDOM Act Data

Following the discovery that the NSA received inaccurate call detail records (CDRs) pursuant to the USA FREEDOM Act (UFA), and a subsequent request by two U.S. Senators for an independent review of certain aspects of NSA's UFA program, including whether NSA's deletion was sufficient to ensure that all inaccurate CDRs were deleted, the NSA OIG conducted a limited scope special study of NSA's deletion of CDRs and data derived from those CDRs (collectively referred to as "UFA data objects") ingested prior to 23 May 2018. The OIG generally found that NSA had been successful in deleting the UFA data objects derived from CDRs that it received from U.S. telecommunications service providers under the UFA program; however, the OIG identified a small number of UFA data objects that should have been deleted, but were not based upon NSA's mistaken assumption regarding the age-off configurations for a single SIGINT repository. As a result, we made one recommendation to assist the Agency in strengthening its controls in the event that a future UFA deletion is required, and one recommendation for the Agency to consider whether it needs to reissue or revise its notifications to the Foreign Intelligence Surveillance Court and the Congress. The Agency agreed with both of the OIG's recommendations, and its planned actions met the intent of the recommendations.

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

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

Ongoing Special Studies and Evaluations

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

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

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

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

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 the Endpoint and Forensics Mission

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

Special Study of 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 such internet capabilities.

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

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

Review of Overcollect Compliance Incidents By Overhead Satellite Systems

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

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

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

Joint Review of Overhead SIGINT Compliance at a Joint Facility

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

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

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

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

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

Investigations

Prosecutions

Two cases referred to the U.S. Attorney for the District of Maryland in October 2017 and one case referred in July 2018, involving allegations that contractor employees fraudulently charged the Agency for hours not worked are pending resolution.

A case referred to the U.S. Attorney for the District of Maryland in June 2017 involving allegations that a contractor company provided unqualified labor in support of an agency contract is pending resolution.

A case referred to U.S. Attorney for the District of Maryland in December 2018 involving allegations that a contractor withheld relevant information and accepted a sole-source contract despite failing to meet Small Business Administration requirements for the contract was not accepted for prosecution.

A case was referred to U.S. Attorney for the District of Maryland in March 2019 involving allegations that an employee had engaged in a conflict of interest by participating substantially in matters affecting an agency contract which her spouse supported, a violation of 18 U.S.C. § 208. The case was not accepted for prosecution.

Two cases involving allegations that contractor employees fraudulently charged the Agency for hours not worked were referred to U.S. Attorney for the District of Maryland during the reporting period. For various reasons, neither case was accepted for prosecution.

Agency Referrals

In addition to the cases discussed above and as required by section 4(d) of the Inspector General Act of 1978 (as amended), 5 U.S.C. appendix, the Investigations Division reported eleven 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 them administratively, rather than criminally.

The Investigations Division referred 49 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 eight employees. One employee was terminated from employment, four employees retired or resigned in lieu of removal, two employees received suspensions of 10 days or less, and one employee received a written reprimand. Forty-one cases referred by the OIG to ER are pending action.

Two cases substantiating contractor misconduct were referred to the Agency's Procurement Office for action, resulting in the recoupment of approximately $53,000. Three cases substantiating

employee timecard fraud were referred to the Agency's Payroll Office, resulting in the recoupment of $11,400.

OIG Hotline Activity

The Investigations Division fielded 457 contacts through the OIG hotline.

Significant Investigations

Former Senior Executive: Use of Public Office for Private Gain

An OIG investigation determined that a former Senior Executive employee, who at the time of the investigation was a reemployed annuitant and employee of a private company, recommended that a Senior Agency Technical Director meet with his private employer. The former Senior Executive recommended his current private employer to the agency as capable of meeting an Agency procurement requirement. The OIG substantiated that the employee had used his public office for private gain, a violation of 5 CFR § 2635.702.

Based on the subject's status as a former Senior Executive, the investigative findings were forwarded to the Department of Defense Office of the Inspector General. 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 did not meet the requirements for reporting to the Department of Justice.

GG-15: Use of Public Office for Private Gain

An OIG investigation determined that a GG-15 employee advocated for the award of a sole source contract to a company operated by a friend. The OIG substantiated that the employee had used his public office for private gain, a violation of 5 CFR § 2635.702. We also found that the employee failed to disclose the friendship and obtain Agency authorization to continue to participate in the awarding of the contract in violation of 5 CFR § 2635.502.

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: Personal and Business Relationships

An OIG investigation determined that a GG-15 employee, formerly a defense contractor, violated ethical standards regarding his covered relationship with his former employer by executing contract officer representative duties associated with a contract supported by his former employer. The OIG found that the employee violated 5 C.F.R. § 2635.502.

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

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

GG-15: Use of Public Office for Private Gain

An OIG investigation determined that a GG-15 employee misused her position as a government official by advocating for her daughter to be hired by an NSA contractor. Additionally, we concluded that the employee improperly recognized her daughter with an honorary award. The employee's actions violated 5 C.F.R. §§2635.101, 2635.702.

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

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

GG-15: Restrictions on Employment of Relatives

An OIG investigation determined that a GG-15 employee tasked, recognized, and advocated for her spouse, in violation of NSA/CSS Policy. The investigation did not substantiate allegations that the employee had created a hostile work environment or provided preferential treatment to a friend.

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: Misuse of Government Resources

An OIG investigation determined that two GG-15 employees misused Government Resources and engaged in inappropriate conduct, of a sexual nature, in violation of DoD JER 5500.7-R and NSA/CSS Policy. The investigation did not substantiate allegations that one of the employees had provided preferential treatment to a friend.

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

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

Whistleblower Reprisal

An OIG investigation found that two Senior Executive civilians and two other civilians did not reprise against a subordinate for making protected communications to supervisors and the OIG. The investigation determined that the complainant had made two protected disclosures and thereafter suffered an adverse personnel action. The investigation found by clear and convincing evidence that the employee would have been removed from his position absent the protected disclosures.

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

Whistleblower Reprisal

An OIG investigation found that a GG-15 civilian employee reprised against a subordinate for having made protected communications to the supervisor and the OIG. The investigation determined that the complainant had made three protected disclosures and thereafter suffered a threat of adverse personnel action. The investigation found that the GG-15 employee reprised against the subordinate, threatening to remove the subordinate from his position.

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

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

Whistleblower Reprisal

An OIG investigation found that a GG-15 civilian employee, and a Senior Executive employee reprised against a subordinate for having made protected communications to Security and his supervisor. The investigation determined that the complainant had made two protected disclosures and thereafter suffered an adverse personnel action. The investigation found that the GG-15 employee reprised against the subordinate when she included negative language in the subordinate's performance evaluation. The investigation also found that the Senior Executive reprised against the subordinate when he reviewed and approved the negative language in the subordinate's performance evaluation.

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

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

Whistleblower Reprisal

An OIG investigation found that a civilian employee reprised against a subordinate for having made protected communications to supervisors. The investigation determined that the complainant had made six protected disclosures and thereafter suffered two adverse personnel actions. The investigation found that the employee reprised against the subordinate when he included negative language in the subordinate's performance evaluation.

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

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

Summary of Additional Investigations

NSA OIG opened 27 investigations and 64 inquiries while closing 29 investigations and 65 inquiries during the reporting period. The new investigations are reviewing various allegations including whistleblower reprisal, ethics violations, violation of the Uniformed Services Employment and Reemployment Rights Act (USERRA), misuse of Government resources, and violations of time and attendance and contract billing policies.

Contractor Labor Mischarging

NSA OIG opened four contractor labor mischarging investigations and substantiated three cases that had been opened previously. The substantiated cases resulted in the proposed recoupment of approximately $227,000. Eight investigations remain open.

Time and Attendance Fraud

NSA OIG opened five new investigations into employee time and attendance fraud during the reporting period. Four investigations that had been opened previously were substantiated during the reporting period, which resulted in the proposed recoupment of approximately $76,250. Disciplinary action against these employees is pending. Six investigations remain open.

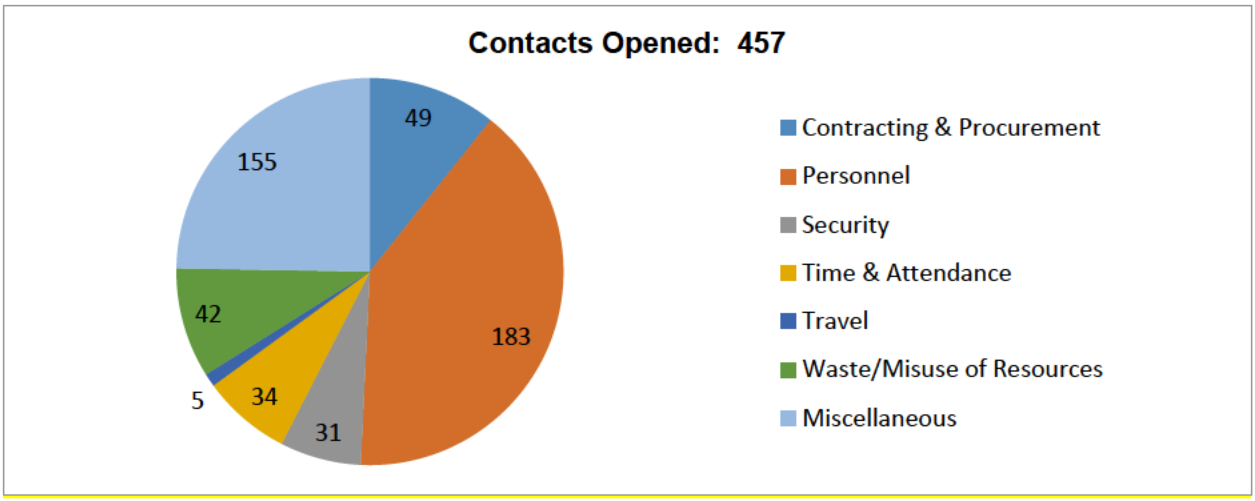
Computer Misuse

NSA OIG opened three new investigations involving allegations of computer misuse. The OIG substantiated one existing case. The substantiated case involved an employee and the results were referred to ER for disciplinary action. Three investigations remain open.

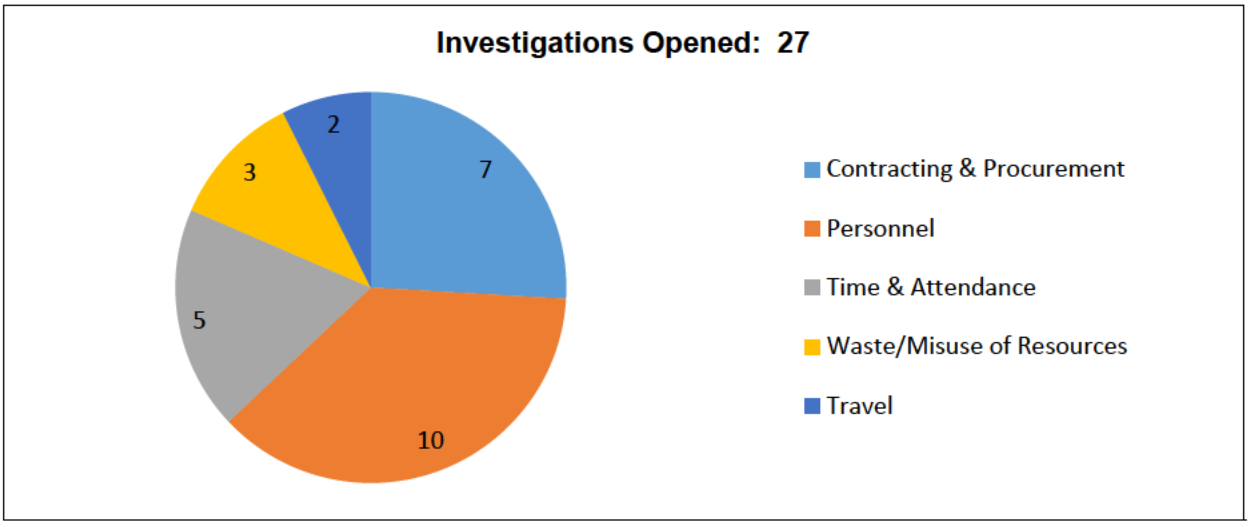
Investigations Summary

Total number of investigative reports issued	29
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	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 National Geospatial Intelligence Agency (NGA) led a peer review of the NSA OIG Inspections Division from 25 February to 5 March 2019. The review team included representatives of the CIA, DIA, and IC IGs and covered the 3-year period which ended on 30 September 2018. The NSA OIG did not peer review another OIG during the reporting period.

Whistleblower Program

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

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

The OIG's Investigations Division examines all credible claims of reprisal. Between 1 October 2018 and 31 March 2019, the OIG opened four new reprisal investigations and closed four other reprisal investigations. Three of the closed investigations substantiated allegations of reprisal and were referred to the proper organization and/or Agency for further action.

Given the importance of whistleblowers to the Agency and the OIG, the OIG has taken steps to help ensure that Agency employees and others are fully informed about whistleblower rights and protections, to include providing guidance to the Agency about the content of the mandatory online training related to whistleblowers. During this period, the OIG continued to disseminate informational cards and posters to employees and locations throughout the enterprise on whistleblower rights and protections, with guidance about how to contact the OIG for additional information. The OIG continues to staff a Whistleblower Coordinator position, which has served as a resource by which Agency employees and others obtain further information about their rights and protections. We also have been working on additional outreach and training materials for the workforce in this important area.

Finally, the OIG continues to reach out to non-governmental organizations (NGOs) that are active on whistleblower issues and encourage dialogue so that the OIG can continue to benefit from their important perspective and experience. At the annual Intelligence Community Inspectors General Conference, IG Storch chaired, and the OIG Whistleblower Coordinator participated in, a panel on whistleblowing within the IC that featured involvement by a leading NGO advocate as well as input from Congressional staff on emerging issues in the area.

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

Audits

Mission and Mission Support

Audit of the Post-Publication of Serialized SIGINT Reports

Audit of Agency's Travel Program

Audit of Award Fee Contracts

Audit of Nuclear Command and Control Program

Technology and Cybersecurity

FY2018 Review of the NSA/CSS Implementation of the Federal Information Security Modernization Act of 2014

Financial Audit

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

Audit of NSA's FY2018 Financial Statements

Inspections

Enterprise Inspections

Inspection of NSA Kent Island

Joint Inspections

Joint Inspectors General Inspection Report - Alaska Mission Operations Center (AMOC)

Intelligence Oversight

Quick Reaction Report: Determination Needed on Department of Defense Directive on Intelligence Oversight

Report on the Review of the National Security Agency/Central Security Service's Deletion of Certain USA FREEDOM Act Data

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

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

Audit Reports with Questioned Costs[1]

Report	No. of Reports	Questioned Costs	Unsupported Costs
For which no management decision had been made by start of reporting period	0	0	0
Issued during reporting period	2	$297,332	~ $636,000,000
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

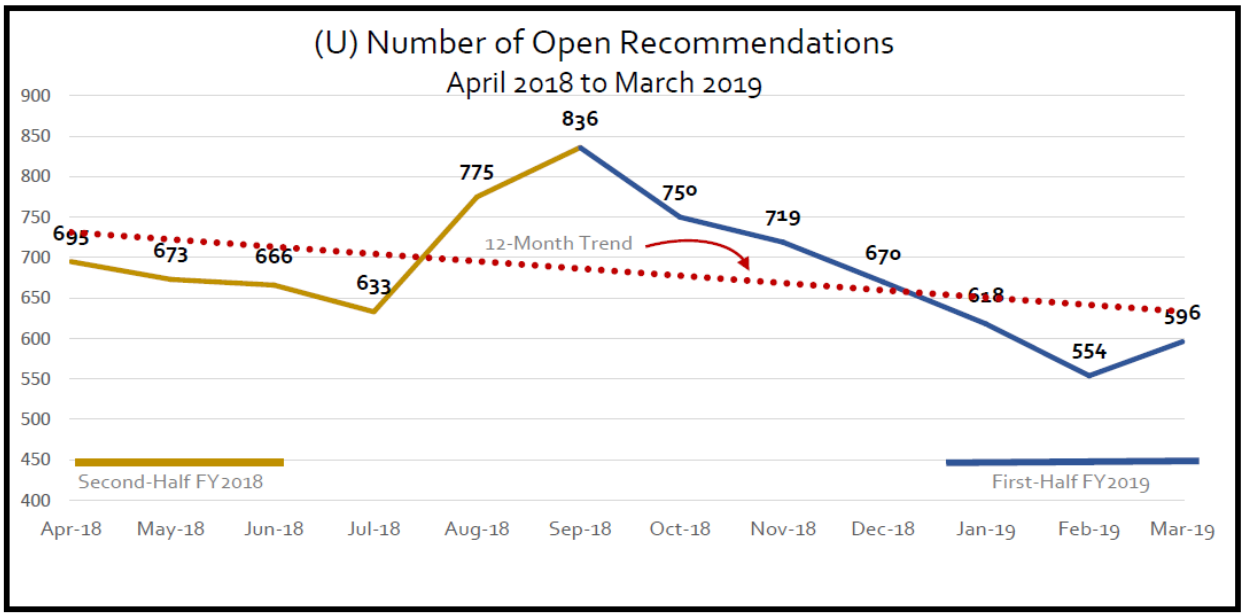
Recommendations Summary

The OIG made 198 recommendations to NSA management in reports and oversight memoranda issued in the first half of FY2019. The Agency closed 69 of the newly published recommendations, and a total of 438 recommendations during the reporting period.

Outstanding Recommendations

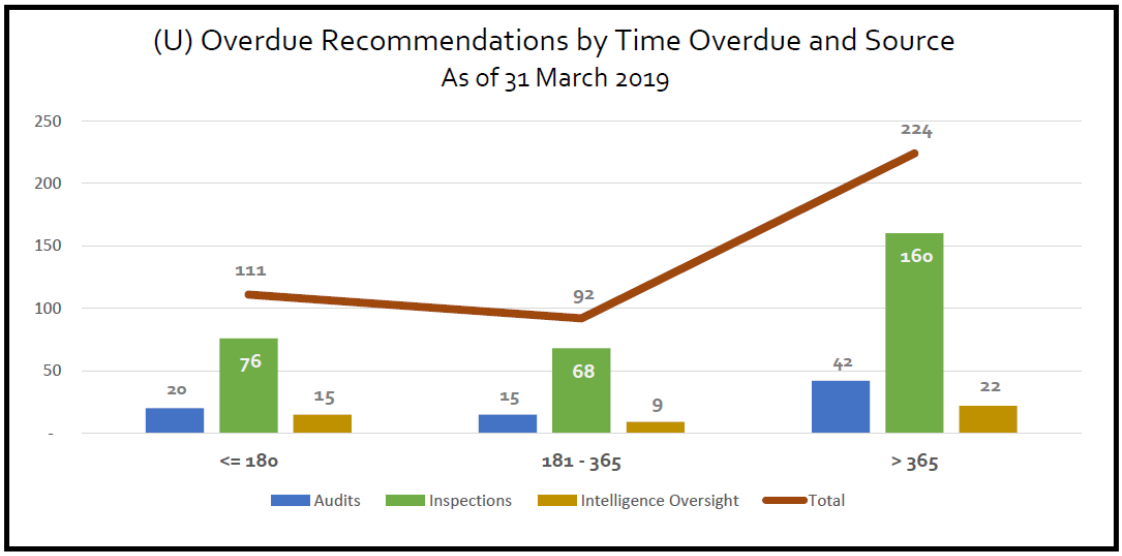
The OIG considers a report open when there are one or more recommendations contained in the report that have not been closed. The number of open recommendations is the total for all reports that remain open. Recommendations are considered overdue when they remain open beyond the target completion date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

	Audits	Inspections	Intelligence Oversight	Total
Open reports	31	40	20	91
Open recommendations	136	372	88	596
Overdue recommendations	77	304	46	427
Overdue recommendation as % of total open	**57%**	**82%**	**52%**	**72%**



Overdue Recommendations Breakdown

Days Past Target Completion Date	Audits	Inspections	Intelligence Oversight	Total	Percent Overdue
<= 180	20	76	15	111	26%
181 - 365	15	68	9	92	22%
> 365	42	160	22	224	52%
Totals	**77**	**304**	**46**	**427**	



Significant Outstanding Recommendations – Audits

Audit of NSA Enterprise Solution and Baseline Exception Request Processes

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

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

Significant Outstanding Inspection Recommendations

Secure the Net / Secure the Enterprise / Insider Threat

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

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

Continuity of Operations Planning

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

Emergency Management Plan

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

Significant Outstanding Recommendations – Intelligence Oversight

Special Study of an Office of Oversight and Compliance Mission Compliance Program

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

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

Management agreed to complete these actions prior to NSA21, but requested extensions as challenges in standing up a new compliance organization delayed resolution. Substantial progress has been made recently toward resolving the outstanding recommendations and, in several cases, all that remains is the publication of finalized documentation.

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

The OIG conducted this study to determine whether select NSA controls are adequate to ensure compliance with the Foreign Intelligence Surveillance Act of 1978 FAA Section 702 targeting and minimization procedures. As part of this study, the OIG tested NSA's controls that ensure that data is queried in compliance with the FAA Section 702 targeting and minimization procedures. The OIG found that NSA did not have a necessary system control. The Agency had previously identified this as a concern and has been working to implement a new system control. 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 target completion date for this recommendation was December 2017. The current Agency estimate is to develop a prototype and implement a pre-query compliance control by December 2020.

The OIG also recommended that NSA ensure that all FAA Section 702 data flows are identified and subject to NSA system controls that verify that FAA Section 702 collection was properly tasked before sending only that data to NSA SIGINT repositories. The target completion date was December 2017. The current Agency estimate to complete the recommendation is June 2019.