# OIG

## Office of the Inspector General
## National Security Agency

# SEMI-ANNUAL REPORT TO CONGRESS

*1 October 2017 to 31 March 2018*

# *Office of the Inspector General*

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

## *AUDITS*

The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

## *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.

## *INTELLIGENCE OVERSIGHT*

Intelligence oversight is designed to ensure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

## *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 IC entities to jointly inspect consolidated cryptologic facilities.

**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 provide context and protect NSA sources and methods.

# A MESSAGE FROM THE INSPECTOR GENERAL

I am very pleased to submit the semi-annual report (SAR) of the National Security Agency/Central Security Service (NSA) Office of the Inspector General (OIG) for the period l October 2017 through 31 March 2018. This is my first SAR as NSA's first Presidentially appointed, Senate-confirmed Inspector General (IG), and it is a tremendous honor to share the many accomplishments of the OIG over the past reporting period.

Since coming on board as the NSA IG in January 2018, I have worked with the outstanding staff of the OIG to ensure that our work is as impactful as possible in promoting positive change within the Agency. I have met with leadership throughout the Agency to discuss the OIG's work and the significant number of outstanding recommendations from our prior reports (actions on many of which have extended well beyond their anticipated completion date), and to encourage action to address them. In that regard, we are implementing new procedures that are intended to foster greater engagement at higher levels across the Agency in order to help ensure that past and future recommendations are addressed in a timely manner. We also are working to make the findings and recommendations in our reports as impactful as possible by identifying and addressing the underlying causes of the issues we find, and by both documenting non-compliance with applicable requirements and making recommendations for means by which the Agency can improve the economy, efficiency, and effectiveness of its operations.

Another area that we have prioritized at the OIG is whistleblower rights and protections. The guiding principle is clear: whistleblowers perform a valuable service to the Agency and the public when they come forward with what they reasonably believe to be evidence of wrongdoing, and they never should suffer reprisal for doing so. To ensure that employees and others fully understand their rights and protections, we have created a Whistleblower Protection page on the OIG's classified website available throughout the NSA community, with frequently asked questions, a comprehensive informational slideshow, relevant videos, and a link to enable employees and others to send inquiries about whistleblower rights and protections to the OIG Whistleblower Coordinator, a position that I created so that people have a readily available point of contact for this important information. In taking these and the other measures described later in this report, we recognize that agencies like the NSA are simply too big, and their operations too diverse, for an OIG to know what is happening throughout the organization if people do not come forward when they see something they believe is wrong, and they cannot be expected to do that if they fear retaliation for doing so. The role of whistleblowers in furthering effective oversight is particularly important at an agency like the NSA, where so much of the work must be performed outside the public eye to be effective. We at the NSA OIG will do everything possible, through our words and our deeds, to ensure that whistleblowers are fully aware of and secure in their rights and protections here at the NSA.

NSA21, the Agency's broad restructuring of operations, reached full operational capability (FOC) during this reporting period, in December 2017. In recent SARs, the NSA OIG has indicated that it was monitoring the implementation of NSA21, and starting to take

preliminary steps toward gathering information regarding its implementation and impact. As the next step in that process, earlier this year, the NSA OIG created an internal inter-disciplinary working group to identify areas regarding NSA21 that would benefit from examination by the OIG. The working group has been gathering information and meeting on a regular basis, and I anticipate seeing its efforts reflected in the OIG's oversight work in the future.

A key principle for OIGs is promoting transparency, and we intend for the first time here at the NSA OIG to produce an unclassified version of this SAR that is available to the public. We also have streamlined the format to make it easier to read and digest. We are taking these steps because even though much of the underlying work over which we conduct oversight is classified, it is important that the public know that there is effective, independent oversight going on here. To further our transparency efforts, we are working to develop a more extensive presence for the OIG on the publicly available internet, which we hope to have operational in the near future.

Pursuant to the Inspector General Act of 1978, as amended (IG Act), I am pleased to report that the OIG experienced no attempts by the Agency to interfere with our independence, and that the Agency fully cooperated with our work and did not refuse to provide or attempt to delay or restrict access to records or other information. In particular, Agency leadership, from the departing Director, Admiral Rogers, to the Deputy Director and throughout the organization, have been open and receptive as I have worked with my team to move forward as an Establishment OIG under the IG Act.

During this reporting period, Agency management agreed with all OIG recommendations, and we have no information to report under the Federal Financial Management Improvement Act of 1996 (FFMIA). During this period, the NSA OIG completed 16 reports of audits, inspections, and special studies, with a wide range of recommendations to improve Agency operations, as described in the pages that follow. These reports were not posted publicly due to the classified nature of many of the activities they address, but they are available on the classified OIG website for access by Agency and other personnel with the appropriate clearances. Copies of the reports completed during this reporting period were enclosed with the classified report to Congress.

It is an exciting time for the NSA OIG, and I am truly honored to lead a team of dedicated and talented men and women working together to improve the integrity and efficiency 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, National Security Operations Center
General Counsel

# TABLE OF CONTENTS

# INDEX OF REPORTING REQUIREMENTS

| | | |
|---|---|---|
| §5(a)(1) | Significant problems, abuses, and deficiencies | 3–5 |
| §5(a)(2) | Recommendations for corrective action | 3–5 |
| §5(a)(3) | Significant outstanding recommendations | 28–31 |
| §5(a)(4) | Matters referred to prosecutorial authorities | 15, 17, 19 |
| §5(a)(5) | Information or assistance refused | i |
| §5(a)(6) | List of completed audit, inspection, and evaluation reports | 24–25 |
| §5(a)(7) | Summary of significant reports | 3–5 |
| §5(a)(8) | Audit reports with questioned costs | 26 |
| §5(a)(9) | Audit reports with funds that could be put to better use | 26 |
| §5(a)(10) | Summary of reports for which no management decision was made | 5 |
| §5(a)(11) | Significant revised management decisions | 5 |
| §5(a)(12) | Management decision disagreements | 5 |
| §5(a)(13) | Information described under 05(b) of FFMIA of 1996 | iv |
| §5(a)(14) | Results of peer review conducted of NSA OIG | 21 |
| §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 | 19–20 |
| §5(a)(19) | Reports concerning investigations of Seniors | 15–17 |
| §5(a)(20) | Whistleblower Retaliation | 17–18 |
| §5(a)(21) | Agency interference with IG Independence | iv |
| §5(a)(22) | Disclosure to the public | iv |
| §5(a)(note) | P.L. 110-181 §845, Final completed contract audit reports | |
| §5(a)(note) | P.L. 103-355 (as amended), Outstanding recommendations past 12 months | 27 |
| * IG Act of 1978, as amended, including the IG Empowerment Act of 2016. | | |

This page intentionally left blank.

# OIG EXECUTIVE SUMMARY

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

## Audit Division

During the six-month reporting period, the Audit Division issued nine final reports with a total of 44 recommendations to improve Agency operations. Reviews were performed as a result of OIG and Agency identified risks as well as congressionally mandated projects. The Audit Division is divided into three branches – Cyber and Technology, Mission and Mission Support, and Financial Management.

The Cyber and Technology branch focused during this period on audits aimed at evaluating the accountability of Agency assets. Three audits reviewed the Agency's processes related to inventory of assets, accountability of software licenses, and support for system authorization decisions.

One of these audits, the *Audit of the Risk Management Framework*, found that Delegated Authorization Officers were not consistently enforcing evidence requirements for the authorization decision to operate (ATO). The audit team found documents missing for every system assessed with an ATO.

During the reporting period, the Mission and Mission Support branch focused its audits on management of two vital processes supporting the Agency's mission – the Records Management Program and Government Furnished Property. In addition, aligning with the Agency's commitment to advance equality, the Mission and Mission Support branch reviewed select Human Resource policies for the inclusion of equality and diversity standards.

The Financial Management branch focused during this reporting period on two congressionally mandated audits – the Audit of NSA's Financial Statements and the Audit of NSA Compliance with the Improper Payments Elimination and Recovery Improvement Act. In addition, the Financial Management branch conducted a service organization control examination and the Special Study of the Government Purchase Card Program.

## Inspections Division

During this reporting period, the OIG completed five inspection reports, four of which were on field sites and one of which was on NSA Washington. There were no attempts to impede our inspection activities, and the Agency and all sites fully cooperated with our work, which resulted in a wide range of recommendations for improvements in operations.

## *Intelligence Oversight Division*

The OIG's Intelligence Oversight Division completed two reports during this reporting period: A special study of certain NSA internet capabilities and a special study of NSA's implementation of another U.S. government (USG) organization's Counterterrorism (CT) Foreign Intelligence Surveillance Act (FISA) Authority.

The Intelligence Oversight Division conducted a special study on certain capabilities that provide access to publicly available information on the internet to determine whether controls for those capabilities are adequate to ensure compliance with Department of Defense and NSA policies to protect the civil liberties and privacy of U.S. persons (USPs). The findings identified by the OIG in this study indicate an increased risk related to three specific capabilities of jeopardizing the civil liberties and privacy of USPs, and of compromising classified information. The OIG made seven recommendations to assist NSA in addressing these risks.

Also, as part of a series of OIG studies on special authorities, the Intelligence Oversight Division conducted a special study to assess NSA's compliance with standard minimization procedures in its implementation of the CT FISA authority of another USG organization. The specific findings identified by the OIG in this study indicate an increased risk of noncompliance with the minimization procedures, potentially impacting privacy rights of USPs. The OIG made 14 recommendations to assist the NSA in addressing these risks.

## *Investigations Division*

During this reporting period, the Investigations Division received and processed 516 complaints, which resulted in the initiation of 30 investigations and 99 inquiries. Three new investigations involve allegations of whistleblower reprisal, and two involve allegations of nepotism. Forty three investigations and 98 inquiries were closed during the reporting period, resulting in the proposed recoupment of approximately $395,000 to the Agency. As a result of OIG investigations, disciplinary actions ranging from termination to counseling were taken against 29 employees. Two cases were accepted for consideration of prosecution by the U.S. Attorney for the District of Maryland, and one case is under review.

## *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. During this period, the OIG opened three new reprisal investigations, and we also closed three reprisal investigations in which we did not substantiate the allegations. Additionally, we have expanded our efforts to inform Agency employees and others regarding whistleblower rights and protections, including making additional informational materials available on the OIG's internal website and establishing a Whistleblower Coordinator position to ensure that employees have a point of contact to obtain information in this area of critical importance for the OIG.

# SIGNIFICANT PROBLEMS, ABUSES, AND DEFICIENCIES AND OTHER SIGNIFICANT REPORTS IN THE REPORTING PERIOD

OIG projects during the reporting period did not reveal serious or flagrant problems or abuses related to the administration of Agency programs or operations that would require immediate reporting to the DIRNSA and Congress pursuant to Section 5(d) of the Inspector General Act. However, the OIG's Special Study of NSA/CSS's implementation of a USG Organization's Counterterrorism Foreign Intelligence Surveillance Act (FISA) authority, the Endorsement of the FY2017 Financial Statement Audit, the Audit of Management and Utilization of Software Licenses, and the Audit of the National Security Agency's Records Management Program each revealed significant problems and deficiencies, as detailed below.

## *Special Study of the National Security Agency/Central Security Service's Implementation of a USG Organization's Counterterrorism Foreign Intelligence Surveillance Act Authority*

The OIG conducted this study of NSA's implementation of a USG organization's CT FISA authority to assess NSA's compliance with standard procedures. The OIG's report, which was part of a series of studies on special authorities, revealed several deficiencies that have the potential to impact the protection of U.S. person (USP) privacy rights. The OIG found that, as a result of human error, incomplete understanding of the rules, and gaps in guidance, analysts have performed some noncompliant queries in the USG organization's CT data using USP identifiers. We also found that incomplete documentation of internal processes and roles and responsibilities associated with foreign dissemination of USP information derived from the USG organization's CT FISA activities increases the risk of noncompliance with authorized procedures. The OIG made 14 recommendations to help NSA to address these deficiencies.

## *Audit of NSA's FY2017 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 FY2017, 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. NSA was not able to provide a complete listing which includes the values of

all capitalized and non-capitalized equipment. In addition, the Agency did not consider the underlying nature of certain leasing agreements, and lacks procedures over the Construction-In-Progress accrual. The Agency had material errors in its estimation methodology for Buildings, Structures, and Facilities. As a result, NSA could not ensure that its General PP&E balances were complete, accurate, and properly valued.

2. **Procurement Activity** NSA did not have sufficient policies, procedures and controls to demonstrate the point in time at which a customer order was established, support the completeness and accuracy of foreign trading partner Deposit Fund accounts, and demonstrate funds availability when establishing the Unfilled Customer Order with Advance and related Advances from Others accounts. NSA had not fully implemented processes, procedures, and controls to track the progress of Military Interdepartmental Purchase Requests and Economy Act Orders from order through delivery to ensure the requirement of the order was satisfied and to provide an adequate audit trail documenting the receipt and acceptance of goods or services. As a result, the Advances and Prepayments, Undelivered Orders, Unfilled Customer Orders, Construction-In-Progress, and Gross Costs may be misstated. NSA did not design, implement, and document management review controls in sufficient detail and with the precision necessary to respond to the risk of material error in the Accounts Payable accrual estimate reported in the financial statements.

3. **Budgetary Activity** NSA did not complete its process to deobligate stale or invalid Undelivered Orders in a timely manner. In addition, the current functionality in the Agency's accounting systems is such that Recoveries are only recorded if adjustments to prior year obligations pertain to an expired fund code. NSA did not establish processes to readily retrieve original supporting documentation for certain budgetary activities.

4. **Fund Balance with Treasury (FBwT)** 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. Further, the inability of NSA to adequately support the validity of the sampled transactions presents uncertainty about whether or not the disbursements or collections should have been charged or credited to NSA's FBwT account or whether other related balance sheet accounts, such as Accounts Receivable, Advances or Prepayments, Accounts Payable, and Deposit Fund Liabilities, are misstated. Additionally, Defense Finance and Accounting Service (DFAS) could not provide complete historical contract populations. As a result, procedures could not be performed to test the completeness and accuracy of Headquarters Accounting and Reporting System data that DFAS used to identify, evaluate, and quantify FBwT differences between DFAS and Treasury that may be attributable to NSA.

5. **Control Environment and Monitoring** Weaknesses existed in the Financial Accounting and Corporate Tracking System (FACTS) related to (1) NSA's processes, procedures, and controls impacting the identification of segregation of duties (SOD) conflicts; (2) the override of SOD conflicts; and (3) insufficient justifications for overriding SOD conflicts. Further, manual mitigating controls were not designed at an appropriate level of precision. In addition, weaknesses existed in NSA's processes,

procedures, and controls related to the preparation and supervisory review of manual journal entries.

## Audit of the Management and Utilization of Software Licenses

The audit objectives were to determine whether the Agency was effectively managing software in compliance with software license agreements, and to determine if software licenses are being utilized in a cost-effective manner. In FY2016, the Agency spent nearly $1 billion on commercial off the shelf (COTS) software licenses and maintenance; however, due to software data deficiencies, we were unable to accurately determine whether the COTS software licenses were being utilized in a cost-effective manner. Although the Agency was able to determine its COTS software purchases through appropriately controlled acquisition processes, once the software was distributed or allocated to organizations and users, the Agency could not assure that it was accurately and completely tracking all licenses available for use and licenses actually in use across the enterprise. We found that this was due to process deficiencies that limit the effectiveness of the Agency's software management and utilization controls. As a result, we found that the Agency may not be accurately reporting COTS software utilization, and the Agency may not be able to fully determine its risk for unauthorized use of COTS software licenses. The Agency agreed with all six recommendations made by the OIG to assist the agency in improving the accountability and effectiveness of its software management and utilization controls.

## Audit of the National Security Agency's Records Management Program

We performed this audit to determine if NSA is in compliance with applicable records management laws and regulations; the topic was chosen because it is a critical process that has not previously been reviewed by the OIG. 44 U.S.C. § 3301 defines federal records broadly as "all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with a transaction of public business...." We found that NSA's records inventory database was not accurate; the vital records program needed improvement; the Records Management Division had not implemented controls to ensure NSA's compliance with records management laws and regulations; NSA's records storage facilities were not in compliance with federal regulations; and the Agency's current process for managing email records was ineffective and was not in compliance with federal regulations. As a result of this audit, the OIG issued 24 recommendations to assist the Agency in improving the records management program.

## Summary of Reports with No Management Decisions

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

## Audits Completed in the Reporting Period

**Report on the National Security Agency's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Control**

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 agency for the period of October 1, 2016 through June 30, 2017, 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, to include exceptions with the design and operating effectiveness of controls which resulted in a qualified opinion.

**Interim Report on NSA/CSS's Compliance with the Federal Information Security Modernization Act of 2014 (FISMA)**

The overall objective of the FISMA review was to evaluate the National Security Agency information security program and practices. In accordance with the Office of Management and Budget (OMB) guidance, we assessed the overall effectiveness of the Agency's information security program. This interim report addresses two fundamental information technology (IT) deficiencies that limit both OIG's and NSA's ability to assess Agency compliance with FISMA IT security requirements. We found that NSA had no authoritative system inventory and had not yet implemented the most current federal security guidance. We made two recommendations to assist the Agency in addressing these deficiencies.

**Special Study of the Government Purchase Card Program**

We reviewed NSA's purchase card transactions to identify and analyze risks of illegal, improper, or erroneous purchases and payments for the period 1 October 2016 through 31 March 2017 in accordance with Public Law 112-194, Government Charge Card Abuse Prevention Act of 2012, dated October 5, 2012. We did not find any transactions that were illegal, improper, or erroneous; however, we did find nine transactions that did not contain a written justification for an exception to policy. The OIG reviewed purchase card program standard operating procedures and user handbooks and did not find a requirement that obligates cardholders to receive and retain written communication for exceptions to the policies within their purchase transaction file. We concluded and recommended that maintaining written justification for exceptions to policy in the purchase transaction file will prove there was a thorough evaluation of the purchase, and the use of a prohibited practice was unavoidable. The report resulted in two recommendations; both actions were completed prior to the issuance of the final report.

**Audit of NSA's FY2017 Financial Statements**

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

**Review of Select Agency Policies that Incorporate Equality and Diversity Standards**

We reviewed NSA's Human Resources (HR) hiring, awards, promotion, and permanent change of station (PCS) policies to identify and evaluate the inclusion of equality and diversity standards as of 15 August 2017. The OIG reviewed applicable federal requirements, met with Agency organizations, and benchmarked those policies with other intelligence agencies. Overall, we did not identify any serious weaknesses or gaps in the NSA policies examined. In some cases, NSA was more explicit in referencing equality and diversity as compared to other Agencies. The OIG identified opportunities for improvement, identified several best practices, and made two recommendations to improve Agency operations.

**Audit of the Management and Utilization of Software Licenses**

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

**Audit of Agency Management of Government Furnished Property (GFP)**

This audit was initiated to assess the effectiveness and efficiency of the NSA's GFP inventory process. The Agency implemented a new GFP inventory process in September 2015 to help remediate a previously identified material weakness in property, plant, and equipment (PP&E) as reported by the OIG on the FY2017 Financial Statement Audit. The new process requires contractors to submit annual and final inventory reports for review. Agency personnel are required to review inventory reports for accuracy and to reconcile them against the Agency's accountable property system of record, ensuring accurate property accountability and valuation. The audit found that the GFP inventory process and the data quality in the Agency's accountable property system needed improvement. The report resulted in four audit recommendations to assist the Agency in improving the efficiency of the GFP reconciliation process.

**Audit of the National Security Agency's Records Management Program**

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

**Audit of the Risk Management Framework**

The Agency has implemented a Risk Management Framework, through NSA/CSS Policy, *Information System Security Authorization Using the Risk Management Framework*, issued 13 June 2016, revised 24 May 2017, establishing requirements and processes for IT systems' risk assessment and security authorization. These decisions are performed by Risk Management Framework (RMF) stakeholders using required system documentation. We reviewed a random sample of 70 systems from the registered population within NSA and found that Agency authorization decisions for systems lacked supporting documentation, system controls were insufficient, and RMF roles are improperly staffed. The report resulted in six audit recommendations to improve the accountability of authorization decisions.

## *Ongoing Audits*

### Audit of NSA's Emergency Management Process

The overall objective of the audit is to determine if NSA's emergency incident and event response process is in compliance with applicable laws, rules, and regulations.

### Audit of Nuclear Command and Control

The overall objective of the audit is to assess mission critical aspects of the NC2 program, including governance, mission assurance, personnel, and facilities. We are issuing two reports to address this topic, one focused on systems, and the other on the remaining issues.

### Audit of Award Fee Contracts

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

### Audit of the Post Publication of Serialized SIGINT Reports

The overall objective of the audit is to determine whether comprehensive, consistent, and effective processes for Post-Publication of Serialized SIGINT Reports exist at the Agency. The NSA's Post-Publication of Serialized SIGINT Reports Service offers consumers of NSA serialized reporting the ability to request approval to share appropriate report intelligence, notwithstanding the original report classification or dissemination control markings, with certain other government customers or partners. Specific processes and associated policies and procedures related to Identity Releases are not in the scope of this audit.

### Audit of CIO Authorities and Oversight

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. Specifically, the audit will assess processes for IT governance, enterprise architecture, program management, information security, and workforce management to ensure that the CIO is executing his responsibilities in these areas.

### Audit of Agency's Travel Program

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

### FY2017 Audit of NSA Compliance with the "Improper Payments Elimination and Recovery Improvement Act" (IPERIA)

The overall objective of the audit is to determine whether the Agency is in compliance with the IPERIA using the OIG procedures in Appendix C of the Office of Management and Budget

Circular A-123, *Management's Responsibility for Internal Controls.*

**FY2018 Review of the Compliance with the "Federal Information Security Modernization Act" at NSA/CSS**

The overall objective of the review will be to evaluate 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 the NSA Corporate Authorization Service (CASPORT)**

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

**Audit of NSA's FY2018 Financial Statements**

The overall objective of the audit is to determine whether the Agency's financial statements are free from material misstatement and will examine the adequacy of internal controls. The audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. The audit 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 year ending 30 September 2018.

**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.

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

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

**Joint Audit of Intragovernmental Transactions**

The objectives of the audit are to determine whether processes for recording and monitoring intragovernmental transactions are effective and in compliance with federal requirements and

whether intragovernmental account balances are accurate and properly supported.

**Audit of NSA's Accountability of 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 System Decommissioning**

The overall objective of the audit is to determine whether the Agency is decommissioning information systems 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 five-year period, was awarded properly and is being administered effectively and in accordance with applicable policies.

# INSPECTIONS

## Inspection Reports Completed in the Reporting Period

**NSA's Personnel Accountability Program Inspection, October 2017**

The OIG performed the biannual inspection of NSA's personnel accountability program, as required by Department of Defense (DoD) Instruction (DoDI) 3001.02, *Personnel Accountability in Conjunction with Natural or Manmade Disasters,* 3 May 2010. The overall objective was to determine whether NSA is in compliance with DoDI 3001.02. This program was last inspected in FY15.

The inspection team found that while NSA has taken steps to ensure the safety of people in NSA-occupied facilities during emergency incidents, NSA is not fully compliant with DoDI 3001.02. The OIG made 3 recommendations to the Agency to assist it in addressing these areas. As a result of the issues identified by the OIG, Human Resources agreed to obtain the appointment by the Director, NSA, of a Personnel Accountability Program Manager.

The classified version of this report contained descriptions of reports on the inspection of four field sites completed by the OIG during this reporting period that cannot be included in the public version of this report. In these inspections, the OIG examined a wide range of topics, including mission operations, intelligence oversight, safety, security, information technology and systems, and emergency practices and procedures. We made findings in these inspections resulting in a total of 289 recommendations to improve operations at the four sites.

## Ongoing Inspection Reports

**Limited Scope Inspection of the Laboratory for Analytic Sciences (LAS), Raleigh, NC, 30 July to 2 August 2017, and of contractor facilities working with LAS, 22 to 23 August 2017**

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

**Limited Scope Inspections of contractor facilities working with Human Language Technologies (HLT), 12 to 13 September 2017, and 25 to 28 September 2017**

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

**NSA Georgia (NSAG), 23 October to 3 November**

A joint NSA, Army INSCOM, Navy FCC, and 25th Air Force inspection team evaluated the overall compliance, effectiveness, and efficiency of NSAG during an inspection from 23 October through 3 November 2017. The last inspection of NSAG was in March 2014.

**NCR DEF/NCR DIA Inspection, 26 to 27 February 2018**

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

The classified version of this report contained descriptions of other pending inspection reports that cannot be included in the public version of this report.

# SPECIAL STUDIES

## Special Studies Completed in the Reporting Period

**Special Study of Certain Internet Capabilities**

The OIG conducted this special study to determine whether controls for certain NSA 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 (USPs). For this study, the OIG examined three such capabilities developed and managed by NSA's Emerging Open Source Activities (EOSA) branch. Our study of these capabilities revealed the following concerns:

- EOSA guidance and training for protecting USP information is incomplete and needs updating;
- EOSA account management practices are inadequate; and
- EOSA capabilities operated in violation of Agency information technology security policy and lack classification guides

The findings identified by the OIG in this study indicate an increased risk of jeopardizing the civil liberties and privacy of USPs and compromising classified information. The OIG made seven recommendations to assist NSA in addressing these risks.

**Special Study of the National Security Agency/Central Security Service's Implementation of a USG Organization's Counterterrorism Foreign Intelligence Surveillance Act (FISA) Authority**

*See* "Significant Problems, Abuses, and Deficiencies and Other Significant Reports in the Reporting Period."

## Ongoing Special Studies

**DoD Training Requirements: Civil Liberty and Privacy Protections and Intelligence Oversight**

The objective of this review is to draw NSA management's attention to the new DoD training requirements for U.S. person privacy protections and intelligence oversight, and to make recommendations to assist NSA in ensuring that it complies with these requirements regarding the content and periodicity of training. We also will address the Agency's need to determine which employees (civilian, military, and contractors) must meet these training requirements.

**OIG Review of Requirements for SIGINT Mission Documentation**

The objective of this review is to examine Signals Intelligence mission documentation based upon deficiencies noted during prior OIG inspections and to make recommendations to address these deficiencies.

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

In this review, the OIG will determine whether select NSA controls are adequate to ensure compliance with Signals Intelligence retention requirements.

**Data Sharing with Third Party Partners**

The objective of this review is to evaluate NSA's controls used to protect U.S. person privacy when sharing raw Signals Intelligence with Third Party partners.

**Special Study of Compliance with Signals Intelligence Policies and Procedures in two programs**

In this review, the OIG is examining whether these two classified programs meet the intent of DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," 8 August 2016, and other related guidance.

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

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

**Special Study of Certain Internet Capabilities, Part II**

The objective of this review is to determine whether additional Agency controls for certain internet capabilities adequately protect civil liberties and safeguard privacy.

# INVESTIGATIONS

## Prosecutions

No cases were criminally or civilly prosecuted during the reporting period.

Two cases referred to the U.S. Attorney for the District of Maryland in October 2017 were accepted for consideration of criminal prosecution. In both cases, the OIG received allegations that contractor employees fraudulently charged the Agency for more than 2,400 hours not actually worked, resulting in shortfalls to the Agency of approximately $470.000.

The U.S. Attorney for the District of Maryland is reviewing a case referred by the OIG in March 2018. The case involves allegations that an employee engaged in, or created the appearance of, a conflict of interest by participating personally and substantially as a Government official in contract matters that would directly and predictably affect his financial interests or those of a family member.

## Agency Referrals

In addition to the three cases discussed above and as required by section 4(d) of the Inspector General Act of 1978 (as amended), 5 U.S.C. appendix, the Investigations Division reported 16 other cases to the Department of Justice during the reporting period. In each case, the OIG had reasonable grounds to believe that a violation of federal criminal law related to employees submitting false timesheets or contractors submitting false labor charges had occurred. We anticipate at this time that the government is likely to handle them administratively, rather than criminally.

The Investigations Division referred 33 cases involving Agency personnel to NSA Employee Relations (ER) for potential disciplinary action. During the reporting period, the OIG received notification of disciplinary action taken against 29 employees, including removal from employment, resignation in lieu of termination, resignation before disciplinary action was taken, suspensions (from two to 45 days), written reprimands, and written counseling.

Fourteen cases substantiating contractor misconduct were referred to the Agency's Contracting Group for action, resulting in the proposed recoupment of more than $300,000.

## OIG Hotline Activity

The Investigations Division fielded 516 contacts through the OIG hotline.

## Significant Investigations

**GG-15: Failure to Comply with Contracting Requirements**

Based on an OIG audit, an allegation was referred to the OIG that resulted in an investigation which found that a GG-15 failed to obtain an appropriate requisition or consult with a

Contracting Officer (CO) before authorizing the purchase and construction of a storage shed via agency contract in violation of Agency policy. Additionally, we concluded that the employee violated additional Agency policy by failing to notify the Associate Directorate for Installation and Logistics of the purchase and construction of the storage shed. This failure caused a building to be constructed that was structurally deficient. The deficiencies necessitated that NSA incur significant expense to renovate the facility, and rendered the facility useless for multiple years.

The investigative findings were forwarded to Human Resources (ER) and the Office of Personnel Security. ER determined that no disciplinary action was appropriate due to the period of time between the employee's actions and completion of the OIG investigation.

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

**GG-15: Preferential Treatment, Failure to Conserve Federal Funds**

An OIG investigation determined that a GG-15 employee created the appearance of giving preferential treatment to a subordinate employee by approving official overseas TDY orders in violation of 5 CFR 2635.101 – "Basic Obligation of Public Service" and Agency policy. In addition, the GG-15 approved TDYs for the subordinate that were unnecessary and in violation of Joint Travel Regulations, VOL 2. We concluded that the GG-15 failed to conserve, protect, and properly use federal funds in violation of Agency policy.

The investigative findings were forwarded to ER and the Office of Personnel Security. Disciplinary action is pending.

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

**GG-15: Sexual Harassment**

An OIG investigation determined that a GG-15 employee engaged in conduct that created a hostile and offensive working environment due to repeated unwelcome comments and touching in violation of Agency policy. Separately, the preponderance of the evidence supported the conclusion that the employee had engaged in conduct that created a hostile and offensive working environment due to repeated unwelcome comments and touching of a sexual nature, in violation of Agency policy.

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

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

**GG-15: Time and Attendance**

Two OIG investigations determined that GG-15 employees had submitted false and inaccurate timesheets for shortfalls to the Government of 392 hours, and 92 hours respectively. These employees were in violation of NSA/CSS Personnel Management Manual (PMM), Chapter 360, § 2-7(a) & (b), and Chapter 366, §§ 2-1(K) and 2-2(B).

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

These cases were reported to the Department of Justice in August and September 2017, respectively, because of the possible violations of 18 USC §§ 287 and 1001. Neither was accepted for prosecution.

**Harassment**

An OIG investigation found that a GG-15 employee did not fail to address allegations of harassment made by a subordinate employee. The preponderance of evidence indicated that the GG-15 responded adequately after becoming aware of the complainant's concerns of harassment.

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

**Whistleblower Reprisal**

An OIG investigation found that that two civilian employees did not reprise against a subordinate for making protected communications to the contracting office and the OIG. The investigation determined that the complainant had made a protected disclosure and thereafter suffered an adverse personnel action, but the agency showed by clear and convincing evidence that the adverse action would have occurred absent the complainant's protected disclosures. To give full consideration to whether Agency personnel acted improperly, the OIG also considered whether under the circumstances the subjects' actions constituted an "abuse of authority" or created a hostile work environment. The OIG did not find sufficient evidence to conclude that conduct by either subject rose to the level of an abuse of authority or had created a hostile work environment.

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

An OIG investigation found that a civilian employee did not reprise against a subordinate for making protected communications to the chain of command. The investigation determined that the complainant had made a protected disclosure and thereafter suffered an adverse personnel action, but the agency showed by clear and convincing evidence that the adverse action would have occurred absent the complainant's protected disclosure. To give full consideration to whether Agency personnel acted improperly, the OIG also considered whether the subject's actions constituted an "abuse of authority." The OIG did not find sufficient evidence to conclude that conduct by the subject amounted to an abuse of authority.

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

An OIG investigation found that a civilian employee did not reprise against a military subordinate for making protected communications to the chain of command. The investigation determined that the complainant had made a protected disclosure and thereafter suffered an adverse personnel action, but the Agency showed by clear and convincing evidence that the adverse action would have occurred absent the complainant's protected disclosure. To give full consideration to whether Agency personnel acted improperly, the

OIG also considered whether the subject's actions constituted an "abuse of authority." The OIG did not find sufficient evidence to conclude that conduct by the subject amounted to an abuse of authority.

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

## *Summary of Additional Investigations*

NSA OIG opened 30 investigations and 99 inquiries while closing 43 investigations and 98 inquiries during the reporting period. Three new investigations involve allegations of whistleblower reprisal, and two involve allegations of nepotism.

### Contractor Labor Mischarging

NSA OIG opened two contractor labor-mischarging investigations and substantiated seven cases that had been opened previously. The substantiated cases resulted in the proposed recoupment of more than $310,000. Six investigations remain open.

### Time and Attendance Fraud

NSA OIG opened nine new investigations into employee time and attendance fraud during the reporting period. Ten investigations that had been opened previously were substantiated during the reporting period, which resulted in the proposed recoupment of more than $84,000. Seven of these employees resigned or retired and action against the remaining three employees is pending. Nine investigations remain open.

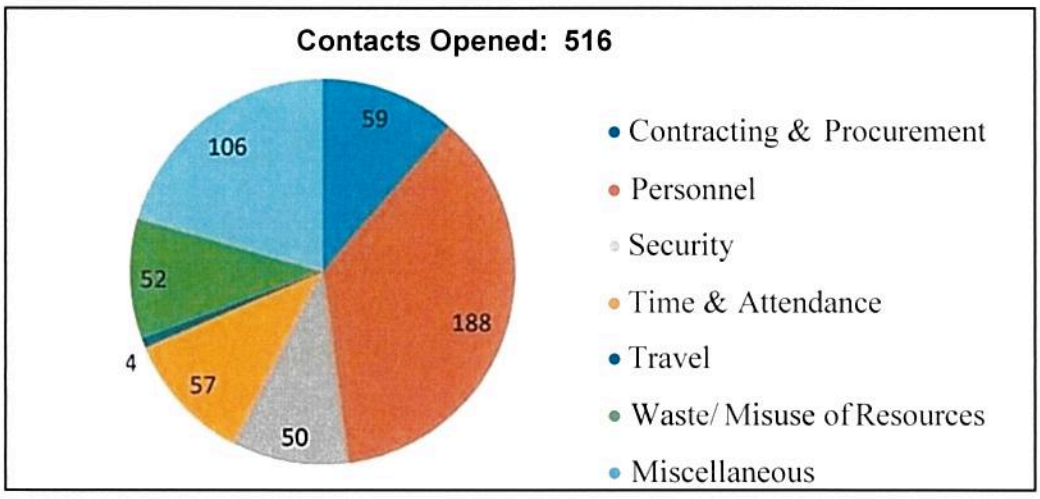
### Computer Misuse

NSA OIG did not open any new investigations involving allegations of computer misuse. We substantiated three existing cases. Two substantiated cases involved employees and were referred to ER for disciplinary action. One case resulted in an employee's suspension from pay and duty; disciplinary action against the other employee is pending. The remaining substantiated case involved a contractor employee and was referred to the appropriate office. The contractor employee resigned prior to any company action. No investigations are open.

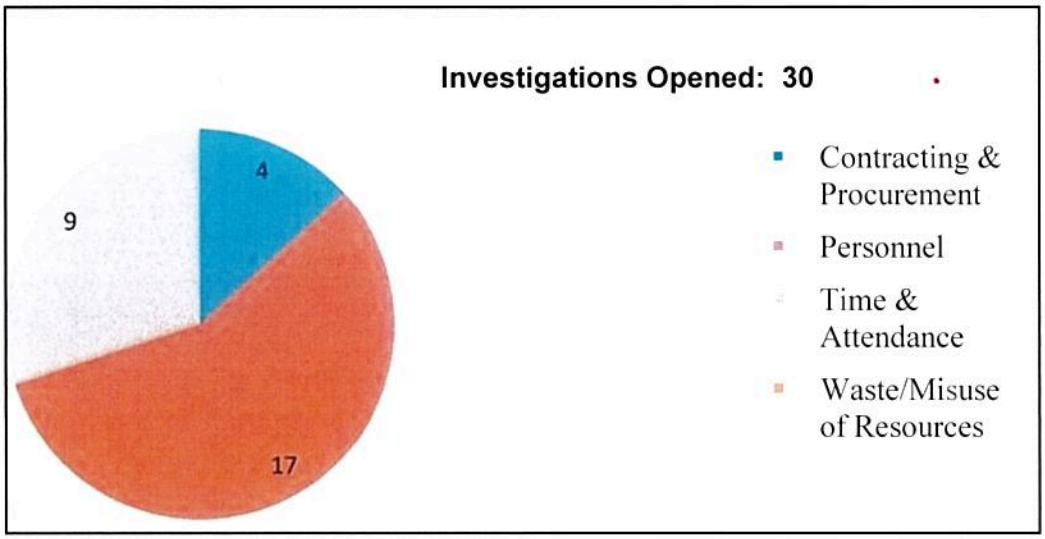
## *Investigations Summary*

| | |
|---|---|
| Total number of investigative reports issued | 43 |
| Total number of persons reported to DOJ for criminal prosecution | 19 |
| 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 Audit Team performed two peer reviews in the reporting period. The reviews were conducted for the NGA IG and the IC IG audit offices.

# WHISTLEBLOWER PROGRAM

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

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

The OIG's Investigations Division examines all credible claims of reprisal. Between 1 October 2017 and 31 March 2018, the OIG opened three new reprisal investigations; it also closed three reprisal investigations in which it did not substantiate the reprisal allegations.

In July 2017, the OIG substantiated a finding that two Agency employees and a military affiliate had taken an adverse personnel action against a subordinate in retaliation for the subordinate making protected disclosure to the subjects of the investigation and the OIG concerning mission-related matters. The Agency suspended both of the subject employees from pay and duty for 10 days, and the OIG referred the military affiliate to the Secretary of the Air Force for appropriate 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. The OIG recently added to its internal NSA website a prominent whistleblower tab that allows the viewer to access a detailed presentation and FAQs on whistleblower rights and protections, and anticipates adding similar information to our public facing website in the near future. The OIG also created a Whistleblower Coordinator position as a resource by which Agency employees and others can obtain further information about their rights and protections.

The OIG has proactively encouraged the Agency to communicate whistleblower rights and protections to the workforce and contractors. In the wake of the passage of the FISA Amendments Reauthorization Act of 2017, which extended whistleblower protections against adverse personnel action to intelligence community contractors, subcontractors, and grantees, the NSA OIG contacted senior Agency leadership about this provision, and recommended that the Agency communicate these expanded protections in writing to all of its contractors, subcontractors, and grantees. We anticipate posting additional information about whistleblower rights and protections on the OIG's public facing website in the near future.

Finally, the OIG has reached out to non-governmental organizations that are active on whistleblower issues and anticipates continuing that dialogue so that we can continue to benefit from their important perspective and experience.

# APPENDIX A: Audits, Inspections, and Special Studies Completed in the Reporting Period

## Audits

**Mission and Mission Support**

- Review of Select Agency Policies that Incorporate Equality and Diversity Standards
- Audit of Agency Management of Government Furnished Property (GFP)
- Audit of The National Security Agency's Records Management Program

**Cyber & Technology**

- Audit of the Management and Utilization of Software Licenses
- Interim Report on NSA/CSS's Compliance with the Federal Information Security Modernization Act of 2014 (FISMA)
- Audit of the Risk Management Framework

**Financial**

- Report on the National Security Agency's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Control
- Special Study of the Government Purchase Card Program
- Audit of NSA's FY2017 Financial Statements

## Inspections

**Field Inspections Completed, Report Not Published**

- NSA/CSS Georgia (NSAG) Joint Inspection, 23 October to 3 November 2017
- NCR DEF/NCR DIA Inspection: 26 to 27 February 2018

**Inspections Completed, Report Published**

- NSA' s Personnel Accountability Program Inspection, October 2017

## *Special Studies*

**Compliance – Operations**

- Special Study of Certain Internet Capabilities
- Special Study of the National Security Agency/Central Security Service's Implementation of Another U.S. Government Organization's Counterterrorism Foreign Intelligence Surveillance Act (FISA) Authority

There were other inspections completed during this period that could not be included in the public version of this report.

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

### Audit Reports with Questioned Costs[1]

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

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

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

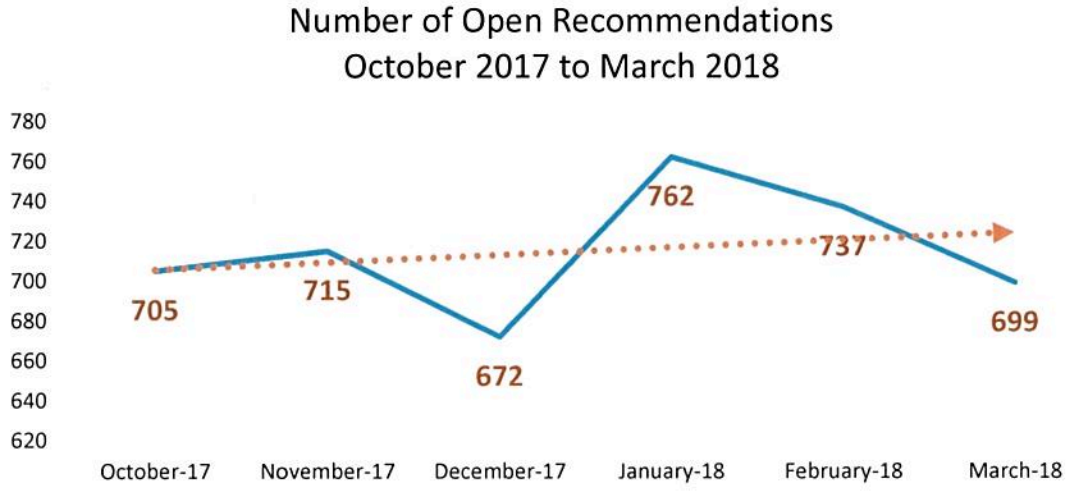
## Recommendations Summary

The OIG made 362 recommendations to NSA management in reports issued in the first half of FY2018. The Agency implemented 85 recommendations in the reporting period.

## Outstanding Recommendations

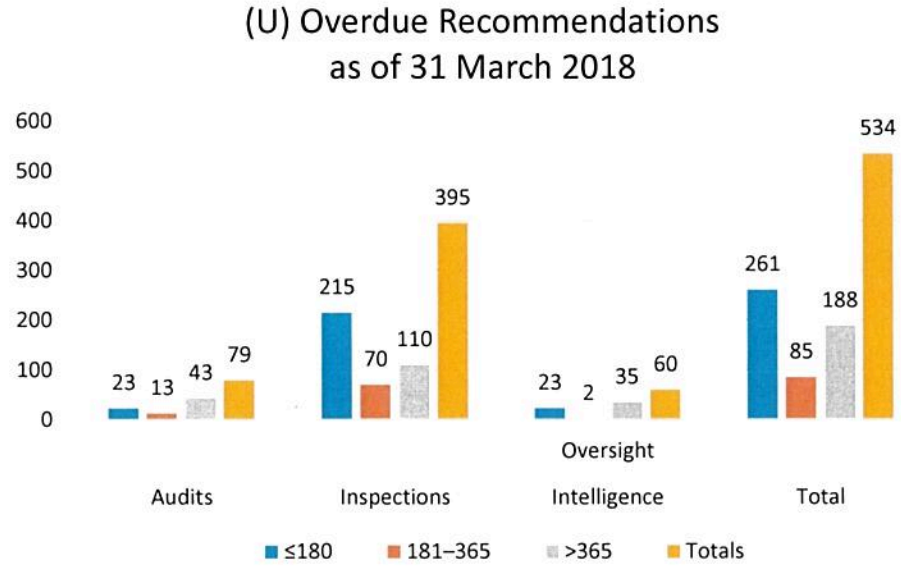
**FY2018 OIG Report and Recommendations Statistics as of 31 March 2018**

| | Audits | Inspections | Intelligence Oversight | Total |
|---|---|---|---|---|
| Open reports | 28 | 36 | 14 | 78 |
| Open recommendations | 120 | 507 | 72 | 699 |
| Overdue recommendations | 79 | 395 | 60 | 534 |
| Overdue recommendations as % of total | 66% | 78 | 83% | 76% |



**Overdue Recommendations Breakdown**

| Days Past Target Completion Date | Audits | Inspections | Intelligence Oversight | Total |
|---|---|---|---|---|
| ≤180 | 23 | 215 | 23 | 261 |
| 181-365 | 13 | 70 | 2 | 85 |
| >365 | 43 | 110 | 35 | 188 |
| Totals | 79 | 395 | 60 | 534 |




**The following represent significant outstanding SAR recommendations.**

## *Significant Outstanding Audits Recommendations*

### NSA Enterprise Solution (NES) and Baseline Exception Request (BER) Processes

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

The OIG also recommended that the Agency develop contract provisions to require contractors to comply with approved processes, as NSA/CSS Policy 6-1, "Management of NSA/CSS Global Enterprise IT Assets," 8 September 2008, requires. This recommendation depends on implementation of the previous recommendation before mandatory contract

provisions or language for hardware purchases and the processes can be developed and included in applicable contracts.

**NSA Export Controls**

The U.S. government has a number of programs to protect technologies critical to U.S. national security interests. The OIG found in 2013 that the export control process is ineffective and recommended that the Agency formally review all Agency export guidance to deconflict guidance and policies, assign a hierarchy to guidance, establish logical links that support hierarchy, and consolidate all responsibilities into NSA/CSS Policy 1-7. Technology Security and Export Control has negotiated a major overhaul to current export control processes with the Operations directorate and has begun discussions with the Capabilities directorate to replicate the same processes. The OIG was told that it expected this action to be completed by the end of December 2017, and then would conduct a thorough review of all export guidance.

The OIG also recommended that the Agency track exports authorized to contractors in an automated centralized database. At a minimum, it should include origin and destination, type of export (defense article, service, or technical data), U.S. munitions list category, estimated dollar value, authority, dates of issue and expiration, and contract number. Two automated Export Control Management Systems have been developed: one UNCLASSIFIED, and one CLASSIFIED. However, user acceptance testing was problematic which has forced needed corrections before going with a conditional initial operating capability (IOC). The Agency's Technology Security office provided evidence on 30 March 2018 that the Export Control Management System went live in November 2017 and is fully functional. The OIG is currently validating that the system meets the intent of the recommendation.

**Information Assurance Workforce Improvement Program (IAWIP)**

DoDD 8570.01-M requires that personnel who perform Information Assurance (IA) duties, regardless of job series or occupational specialty or whether full time or as a collateral duty, maintain a certification corresponding to the highest functions required by their positions. The OIG found in 2014 that NSA's IAWIP should improve the designation and tracking of IAWIP positions within the Agency and recommended that the Agency designate specific positions that meet the IAWIP criteria as outlined in NSA/CSS Policy 6-34, *NSA/CSS Cyberspace Workforce Improvement Program* (CWIP). The OIG has been informed that the Strategic Education Initiatives and Alliances CWIP (formerly IAWIP) team continues to work with Manpower Management on the effort to develop a billet-tracking database.

## *Significant Outstanding Inspection Recommendations*

**Secure the Net / Secure the Enterprise / Insider Threat**

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

- System Security Plans are often inaccurate and/or incomplete;

- Two-person access (TPA) controls not properly implemented for data centers and equipment rooms; and,
- Removable media not properly scanned for viruses.

**Continuity of Operations Planning (COOP)**

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

**Emergency Management Plan**

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

## *Significant Outstanding Special Studies Recommendations*

**Assessment of Management Controls over FAA §702**

Obligation to Review (OTR) alerts are part of NSA's system of controls designed to provide reasonable assurance of compliance with Section 702 of the FISA Amendments Act of 2008 and the targeting and minimization procedures that establish requirements for the Agency's use of the authority. OTR alerts support compliance with targeting requirements and are generated when target communications are not reviewed with the frequency required by NSA internal guidance. As reported during the 2012 study, the OTR system is operational for some FAA §702 selectors. However, our recommendation to implement OTR for certain FAA §702 selectors will not be resolved until NSA's system receives the associated data. The current Agency estimate to implement the required corrective actions is end of 3QFY18.

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

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

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

The OIG reviewed an Office of Oversight and Compliance that is responsible for implementing guidelines, regulations, and directives that govern the United States SIGINT

System's (USSS) acquisition, processing, retention, and dissemination of SIGINT. The OIG found that, in certain respects, the office does not fully perform its oversight responsibilities over the entire USSS and does not fully execute its mission to perform proactive and comprehensive verification of USSS activities. The OIG recommended that the office:

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

Management requested extensions to complete these actions by 31 May 2018.