NATIONAL SECURITY AGENCY

OFFICE OF THE INSPECTOR GENERAL

Semiannual Report to Congress

1 October 2020 to 31 March 2021

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

Message from the Inspector General

Resilience, flexibility, commitment – these are the sort of words that come to mind when I think about the work of the women and men of the National Security Agency (NSA) Office of the Inspector General (OIG) over the past half year. Back in the office, with strict adherence to health and safety mitigations and protocols, with travel restricted and many balancing the competing demands brought on in taking care of family and carrying out their lives in the midst of an ongoing global pandemic, the OIG nevertheless was able to have a remarkably productive reporting period, producing a total of 16 oversight products from 1 October 2020 through 31 March 2021 that made impactful findings and recommendations for improvement across the full gamut of Agency programs and operations. The OIG Inspections Division, in particular, had to revamp its procedures and devise creative solutions to continue to conduct impactful oversight over the wide range of Agency operations without being able to visit the sites being inspected. Similarly, despite necessary and prudent limitations on in-person contacts, the OIG Investigations Division continued its outstanding work, manning the OIG Hotline and conducting investigations that uncovered waste, fraud, abuse, and misconduct, including completing six investigations involving senior Agency personnel, in two of which the allegations were substantiated, and seven investigations involving allegations of reprisal against whistleblowers, one of which was substantiated as well. The OIG Intelligence Oversight and Audit Divisions continued to produce a range of outstanding work, and all four OIG Divisions worked together with our Data Analytics team on an Advisory Memorandum reporting the results of the OIG's survey of the civilian and military workforce regarding the Agency's response to the global coronavirus pandemic. We will continue to explore ways to be most impactful in that and other critical areas here.

One development that I want to highlight that is reflected in the Recommendations Overview in Appendix C is that I made the decision effective this reporting period that the OIG would track recommendations as outstanding from issuance until closure, without requiring or tracking "target completion dates" that previously had been provided by the Agency and reflected in our reports. While the Agency has made significant progress in addressing the number of outstanding recommendations over the past few years, I believe this change will promote even prompter action by the Agency to complete actions necessary to address the issues identified in our reports, and that it is more reflective of our statutory independence as well.

In addition, toward the end of this reporting period, we were pleased that the Director of the NSA issued a powerful message that was disseminated across the NSA enterprise emphasizing the importance of cooperating with the OIG and reporting suspected wrongdoing to us. The message, which is described in more detail in the Whistleblower Coordinator Program section of this report, also advised personnel that they are protected from any adverse personnel action being taken against them for reporting to the OIG, and encouraged them to report any concerns about reprisal or retaliation to the OIG immediately. We appreciate the support for our continued efforts to ensure that whistleblowers at the NSA are encouraged to come forward, and that they never suffer for doing so.

Finally, I'd note that, as with our underlying reports, we have updated the format and style of this Semiannual Report to Congress, in an effort to make the information contained in it more readily accessible to the reader. My thanks to the talented people here at the OIG who have worked long and hard to make this new look a reality.

Pursuant to the IG Act, I am pleased to report that the OIG experienced no attempts by the Agency to interfere with our independence, and that the Agency fully cooperated with our work and did not refuse to provide or attempt to delay or restrict access to records or other information. Agency management agreed with all OIG recommendations that were made during the reporting period. All told, despite the continued difficult circumstances during this reporting period, the OIG made a total of 256 recommendations to NSA leadership that we believe will be impactful in improving the economy, efficiency, and effectiveness of this critical Agency's operations.

ROBERT P. STORCH

Inspector General

Contents

OIG Executive Summary

Oversight Work Involving Multiple Divisions

As the Agency reconstituted its workforce during the COVID-19 pandemic, personnel from across the OIG Intelligence Oversight, Inspections, Audit, and Investigations Divisions worked with our Data Analytics team to prepare, conduct, and analyze a survey of civilian and military personnel across the NSA enterprise in order to ascertain their views on a wide range of Agency actions and responses to the pandemic. The results were provided to Agency leadership to inform their consideration of additional steps to address the ongoing pandemic, and a response regarding actions taken, or planned, to address the challenges identified was obtained.

Audit Division

During this reporting period, the Audit Division issued a total of five reports to improve Agency operations.

The Cybersecurity and Technology branch performed the annual evaluation of the NSA's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA). Specifically, we evaluated eight information technology (IT) security areas against applicable metrics and determined that there was room for improvement in all areas: risk management, configuration management, identity and access management, data protection and privacy, security training, continuous monitoring, incident response, and contingency planning. For the third consecutive year, identity and access management was deemed the strongest security area, and despite progress in contingency planning, this area was still the most in need of attention.

During this reporting period, the Financial Audits branch focused on the congressionally mandated Audit of NSA's Financial Statements, which identified a number of material weaknesses as summarized in the Report on Internal Control. In addition, the Financial Audits branch completed a joint

Work At a Glance

Work Involving Multiple Divisions	**1**
Audits Division	**5**
Inspections Division	
Inspections	**3**
Advisory Memoranda	**5**
Intelligence Oversight Division	**2**
Investigations Division	
Contacts	**715**
Closed Investigations	**34**
Closed Inquiries	**107**
Proposed Recoupment	**$110K**
Cases Referred to U.S. Attorney	**18**

audit to determine whether processes for recording and monitoring intragovernmental transactions between NSA and a trading partner were effective and in compliance with federal requirements, and intragovernmental account balances between the two agencies were accurate and properly supported. The audit found the agencies could not support the accuracy and timely recording of financial transactions. Further, neither NSA nor its partner provided the documentation necessary for the requesting agency to determine whether amounts billed were commensurate with goods or services received. In addition, neither NSA nor its partner conducted effective reconciliations of the activity and balances between the two agencies because the reconciliations either were not performed or not performed timely, and unreconciled items were not resolved.

Inspections Division

During this reporting period, the OIG issued three inspection reports and five advisory memoranda. Four of the advisory memoranda resulted from instances where we had gathered information and documentation in advance of planned inspections that had to be delayed due to travel restrictions resulting from the COVID-19 pandemic. While we were not able to travel to those sites to conduct in-person inspections, we found that there were valuable insights that could be gleaned from our preparatory work, and we adjusted our procedures to provide that to the sites through advisory memoranda, with recommendations for improvement where we could support them based on the available information. Similarly, as a result of the pandemic, we shifted four new inspections from in- person to virtual. While in-person inspections yield results that virtual inspections may not, we again found that conducting an assessment of written documentation against defined criteria and drawing insights from individual interviews enables us to produce findings and recommendations that site leaders agreed would improve their site. In addition, these inspections can inform a shorter, in-person inspection at a later date, when items that require in-person assessment can be the focus of the visit. We also identified a number of commendable or best practices at the inspected sites that we believe could be replicated elsewhere.

Intelligence Oversight Division

The OIG's Intelligence Oversight Division issued two final reports during this period. One special study evaluated the efficiency and effectiveness of the NSA Capabilities Directorate's compliance incident management process for systems-related compliance matters. We found, among other issues, NSA has not completed certain aspects of the Capabilities compliance incident management process leaving an environment where incident management functions were handled inconsistently, that external and internal timelines for reporting compliance incidents were not always met, and that the NSA Incident Reporting Tool did not include all the necessary functionality. We also found that resources, expertise, and training for managing Capabilities' compliance incidents were insufficient, which we believe contributed to incidents being open for prolonged periods.

An evaluation completed later in the reporting period assessed whether the procedures for disseminating FISA Section 702 counterterrorism collection to certain partners were sufficient to ensure compliance with the current legal and policy framework, including the protection of U.S. privacy. We also examined whether this process enabled the efficient and effective dissemination of this information to certain

partners. The OIG found many of the dissemination operations were functioning as designed within legal, policy, and procedural parameters; however, we made a number of findings reflecting room for improvement, including that not all personnel had completed the required intelligence oversight training, FISA Section 702 query procedures were not releasable to thecertain partners, queries into SIGINT collection were suppressed from NSA's post-targeting review monitoring system, and the inherently manual nature of the evaluation, minimization, and dissemination processes increased the likelihood of noncompliance with approved procedures and adversely impacted overall efficiency.

Investigations Division

During this reporting period, the Investigations Division received and processed 715 contacts, which resulted in the initiation of 35 investigations and 112 inquiries. The investigations included allegations into acquisition fraud, violations of standards of conduct, computer misuse, hostile work environment, contractor labor mischarging, travel card misuse, time and attendance fraud, government vehicle misuse, and reprisal. The OIG closed 34 investigations and 107 inquiries during the reporting period, resulting in the proposed recoupment to the Agency of approximately $40,000 from employees and approximately $71,000 from contractors. OIG investigations also resulted in actual recoveries of over $350,000 to the Government. As a result of OIG investigations, disciplinary actions ranging from termination to reprimands were taken by the Agency against eight employees. Eighteen cases referred to the U.S. Attorney for the District of Maryland were declined for prosecution.

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:

Pandemic Response Survey - Advisory Memorandum

The OIG conducted a Pandemic Response Survey, open from 31 August through 2 October 2020, to understand how the civilian and military workforce assessed the Agency's pandemic response efforts. The OIG used data analytics to assist in the review of 3,573 total responses, as well as considering 1,823 narrative comments received through the survey instrument from civilian and military affiliates across the NSA enterprise.

Utilizing the same data analysis methodology employed in the annual Intelligence Community Climate Survey, the OIG found that respondents reported a number of strengths and challenges in the Agency's response to the pandemic. Reported strengths, for which 80 percent or more of the responses were positive, included mission sustainment during reconstitution, immediate supervisor communication and concern for employees' well-being, the availability of flexible leave options that helped employees balance individual needs consistent with mission requirements, and the clarity of policy and guidance concerning requirements for facial coverings and physical distancing, as well as leave policies. Reported challenges, for which 20 percent or more of the responses were negative, included concerns in the area of health and safety, in which a number of respondents reported that they did not feel physically safe largely due to their concerns regarding the implementation of workplace distancing mitigations and the availability of sanitation supplies, and due to the perception that senior Agency leaders did not sufficiently value their health and well-being. Respondents also identified as challenge areas communication from leadership, which many respondents felt was confusing, inconsistent, and lacked transparency, and a lack of clarity in Agency guidance and implementation of initiatives involving telework, reconstitution, personal travel, campus transportation, and the Department of Defense (DoD) Stop Move order. Respondents outside of NSA/CSS Washington (NSAW) reported as a challenge enterprise-wide policy implementation and guidance that they believed was inconsistent and too "NSAW-centric."

The OIG provided a detailed summary of the results of the survey to the NSA Deputy Chief of Staff on 5 November 2020 for consideration by the Board of Directors as it considered additional steps in response to the ongoing pandemic. While we did not have sufficient basis from the survey responses alone to make specific recommendations at this time, we published the full results in the Advisory Memorandum and requested that the Agency report back regarding the steps taken, or planned, in response to the challenges identified. The Agency provided its response to the Advisory Memorandum on 12 March 2021.

Audit of NSA's FY2020 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 FY2020, we found that material weaknesses exist in the Agency's ability to provide documentation to support the financial statement assertions. While there has been progress in a number of important respects, five areas—General Property, Plant & Equipment, Procurement Activity and Accounts Payable Accrual, Budgetary Activity, Fund Balance with Treasury and Deposit Funds, and Entity Level Controls—continued from the FY2019 financial statement audit. For those areas, which are discussed below, NSA was unable to complete its remediation efforts, which may have been affected by the coronavirus pandemic.

1. **General Property, Plant and Equipment (PP&E).** NSA did not have effective policies, processes, procedures, or controls to identify, accumulate, and report all classes of PP&E, to include General Equipment, Leasehold Improvements, Communications Security assets, and Software. For equipment, NSA did not maintain historical documentation to support equipment balances and, therefore, has developed a number of estimation methodologies to value its equipment based on equipment attributes and assumptions. In prior audits, controls related to the Agency-wide wall-to-wall inventory were not operating as designed to detect and correct material errors in the general equipment balance or validate the accuracy of critical data elements necessary for the estimation methodologies. As stated, NSA did not complete remediation efforts necessary to correct the previously identified control deficiencies.

2. **Procurement Activity and Accounts Payable Accrual.** In prior audits, it was determined that NSA did not effectively design and implement policies, procedures, or controls to ensure the reliability and consistency of source documentation as it relates to both Federal and non-Federal procurement activity, as well as the key source of critical data inputs and assumptions used in its accounts payable methodology. In addition, NSA had not fully implemented corrective actions to demonstrate that Economy Act Order (EAO) managers with direct knowledge of program costs could validate the date when goods or services were received by NSA, or that EAO managers timely certified receipt and acceptance of the goods or services. As stated, NSA did not complete remediation efforts necessary to correct the previously identified control deficiencies.

3. **Budgetary Activity.** NSA's processes, procedures, and controls impacted its ability to provide sufficient documentation to support the validity of its reported undelivered orders balance. Additionally, the Agency did not design and implement control activities to effectively monitor, identify, and deobligate invalid obligations in a timely manner.

4. **Fund Balance with Treasury (FBwT) and Deposit Funds.** FBwT represents the aggregate amount of available monetary resources held at the U.S. Treasury for NSA to pay liabilities and finance future authorized expenditures. NSA did not fully implement effective controls to demonstrate that, working through the Defense Finance and Accounting Service, all NSA-related activities were completely and accurately reconciled with Treasury and appropriately routed to NSA. In addition, NSA's processes, controls, and associated

documentation were not sufficient to ensure accurate reporting of its activity with foreign trading partners. Further, NSA removed previously recorded deposit fund asset and liability balances relating to foreign customers from its FY2020 financial statements but did not provide adequate documentation to support that the accounting treatment complied with generally accepted accounting principles.

5. **Entity Level Controls.** A material control weakness was identified in NSA's entity level controls related to control environment, risk assessment and monitoring, and information and communication. The audit noted that because of health and safety precautions implemented in response to the coronavirus pandemic, NSA implemented a reduced work schedule which delayed the performance of certain internal control activities, and caused NSA to defer the implementation of many corrective action plans to address internal control deficiencies identified in prior year audits.

Joint Audit of Intragovernmental Transactions

Because of the widespread concerns regarding intragovernmental transactions (IGTs) across Federal agencies, the NSA OIG and another OIG conducted this joint audit to determine whether processes for recording and monitoring IGTs between NSA and a trading partner were effective and in compliance with federal requirements, and intragovernmental account balances between the two agencies were accurate and properly supported. The objectives of the audit were to determine whether processes for recording and monitoring IGTs between NSA and another agency were effective and in compliance with federal requirements, and intragovernmental account balances were accurate and properly supported. NSA and its partner agency engage in IGTs for goods and services under the Economy Act of 1932, as amended, when such an agreement can achieve economies through the full use of Government resources and eliminate duplication and overlap of Government activities. In addition, NSA enters into joint programs that use the Economy Act Order process.

The audit identified the following weaknesses in supporting and monitoring IGTs:

- The allocation of expenses for a joint program was not properly supported. As a result, the NSA and its partner agency could not support the accuracy and timely recording of financial transactions.
- When acting as the servicing agency in providing goods or services to the other agency, neither NSA nor its partner provided the documentation necessary for the requesting agency to determine whether amounts billed were commensurate with goods or services received. As a result, the requesting agency could not substantiate the accuracy, completeness, and timeliness of the expense transactions, or that the agency received the services for which it paid.
- The NSA and its partner agency did not conduct effective reconciliations of the activity and balances between the two agencies because the reconciliations were either not performed or not performed timely, and unreconciled items were not resolved. As a result, there is an increased risk that the agencies' intragovernmental account balances, related to both EAOs and joint programs, reported on the financial statements may be materially incorrect and that information used for the execution of funds may not be accurate.

The OIGs made a total of six recommendations to assist NSA and its trading partner in addressing the findings detailed in the report.

Summary of Reports for Which No Management Decision Was Made

No reports without management decisions were published.

Significant Revised Management Decisions

There were no significant revised management decisions regarding OIG reports.

Significant Management Decision Disagreements

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

Oversight Work Involving Multiple Divisions

Pandemic Response Survey – Advisory Memorandum

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

AUDITS

Audit Reports and Oversight Memoranda Completed in the Reporting Period

Audit of NSA's FY2020 Financial Statements

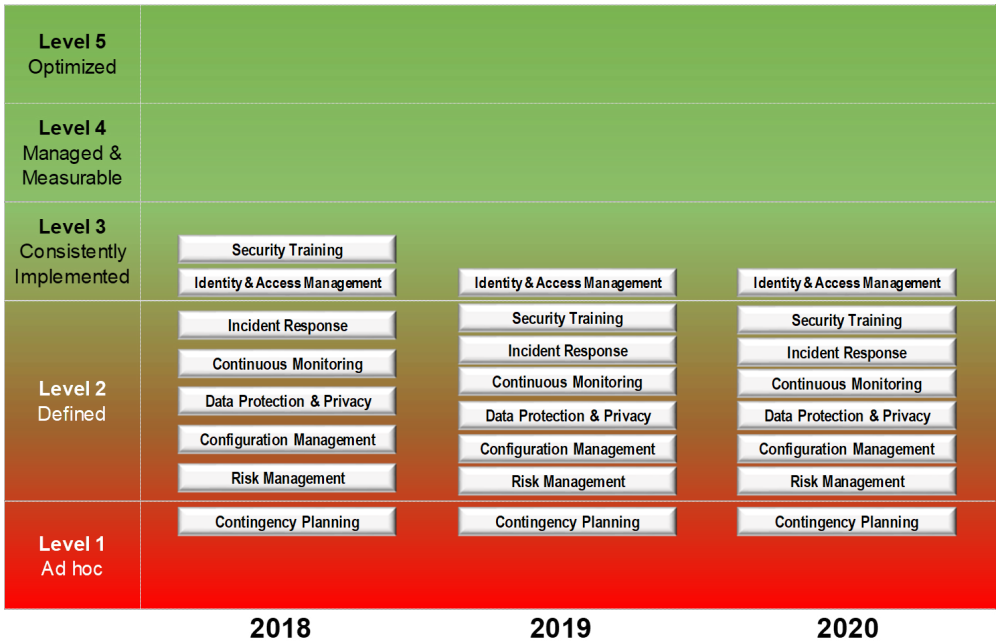
See the "Significant Problems, Abuses, and Deficiencies and Other Significant Reports in the Reporting Period" section of this report.

Joint Audit of Intragovernmental Transactions

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

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

In accordance with U.S. Office of Management and Budget guidance, the OIG is required annually to assess the effectiveness of information security programs on a maturity model spectrum, which ranges from Level 1 (ad hoc) to Level 5 (optimized). Our assessment of eight IT security areas revealed that while progress was made in some areas from FY2019 to FY2020, there continues to be room for improvement in all eight IT security areas.



For the third consecutive year, identity and access management was deemed the strongest security area with an overall maturity level rating of 3, consistently implemented. Although the Agency remains Consistently Implemented for this area, to meet the next level 4, Managed and Measurable criteria, the Agency would need to demonstrate that they quantitatively and qualitatively measure policies, procedures, and strategies from across the Enterprise and assess to make necessary changes. Also for the third consecutive year, contingency planning was assessed at an overall maturity level of 1, Ad Hoc. Although the Agency has made some improvements to the program, additional improvements need to be made.

Review of the Agency's Implementation of Executive Order 13950 on Combating Race and Sex Stereotyping

On 22 September 2020, the President of the United States established Executive Order (E.O.) 13950 on Combating Race and Sex Stereotyping, which required federal agencies, federal grantees, federal contractors, and the Uniformed Services to address trainings that include divisive concepts, race or sex stereotyping, and race or sex scapegoating, as defined in the E.O. E.O. 13950 directed that each agency head request the agency Inspector General to thoroughly review and assess by the end of the calendar year. Based on discussions with the Department of Defense Office of the Inspector General, the NSA OIG agreed to coordinate our review with the DoD OIG and provide our report to them.

The overall objective of the review was to assess the Agency's progress in implementing the requirements of E.O. 13950 on Combating Race and Sex Stereotyping. The OIG assessed that the Agency had been proactive and had made significant efforts and substantial progress in implementing E.O. 13950 since its issuance on 22 September 2020. At the time the report was issued, the Agency was waiting for guidance from DoD on changes to the federal grants process and according to the Diversity, Equality and Inclusion office, the Agency was on pace to meet the 11 January 2021 date to have Diversity and Inclusion Training submitted to the Office of the Under Secretary of Defense for Personnel and Readiness for approval. The OIG did not make any recommendations to the Agency.

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

The overall objective of the oversight review was to ensure that the audits performed by an independent public accounting (IPA) firm of the financial statements of the NSA Restaurant Fund and the NSA Civilian Welfare Fund as of and for the fiscal years ended 30 September 2019 and 2018 were performed in accordance with U.S. generally accepted government auditing standards and the terms of the contract for non-appropriated fund instrumentalities audit services. In its audit, the IPA firm reported the financial statements were fairly presented, in all material respects, in accordance with U.S. generally accepted accounting principles, there were no material weaknesses in internal control over financial reporting, and there was no reportable noncompliance with provision of laws tested or other matters. The NSA OIG reviewed the IPA firm's report and related documentation and inquired of its representatives, which disclosed no instances in which the IPA firm did not comply, in all material respects, with U.S. generally accepted government auditing standards.

Ongoing Audits

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

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

Audit of Cost-Reimbursement Contracts

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

Audit of Tactical Serialized Reporting

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

Audit of the Agency's Parking and Transportation Initiatives

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

Audit of Enclaves with Distributed Monitoring Oversight

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

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

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

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

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

Evaluation of the NSA's FY2020 Application of Classification Markers, Compliance with Declassification Procedures, and the Effectiveness of Declassification Review Processes

In accordance with the National Defense Authorization Act for Fiscal Year 2020, the objective of this evaluation is to submit to the congressional intelligence committees a report that includes analyses of the following with respect to fiscal year 2020:

- The accuracy of the application of classification and handling markers on a representative sample of finished reports, including such reports that are compartmented.
- Compliance with declassification procedures.
- The effectiveness of processes for identifying topics of public or historical importance that merit prioritization for a declassification review.

Audit of NSA's FY 2020 Compliance with the Payment Integrity Information Act of 2019

The objective of this audit is to determine whether the Agency is in compliance with the Payment Integrity Information Act of 2019.

Audit of the FY2021 National Security Agency Financial Statements

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

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

The overall objective of the evaluation will be to review the Agency's information security program and practices. In accordance with the Office of Management and Budget guidance, we will assess the overall effectiveness of the Agency's information security policies, procedures, and practices.

INSPECTIONS

Inspection Reports and Oversight Memoranda Completed in the Reporting Period

Joint Inspections of Three Overseas Sites

NSA, the Army Intelligence and Security Command, U.S. Fleet Cyber Command, and 25th Air Force Offices of the Inspector General (OIG) jointly conducted inspections of two overseas locations, and NSA OIG conducted an inspection of a third overseas location, all of which evaluated the overall climate, compliance with laws and policies, and the efficiency and effectiveness the activities at these locations. During the inspections, the OIG conducted focus groups, participants of which represented all segments of the civilian and military government workforce. The OIG also interviewed members of the workforce and observed operations and functions in mission operations; intelligence oversight; resource programs; information technology and systems; safety, facilities, and emergency management; security; and training.

The OIG identified a number of concerns across these three locations, including the quality and efficacy of communications across organizational levels. We noted facilities concerns related to the delayed move of two of the organizations inspected, with problems ranging from bankruptcy of the original contractor to power testing issues to disagreements between the second contractor and the Army Corps of Engineers. The OIG also found a number of safety concerns related to site facilities, particularly related to fire services and emergency exits.

In addition, the OIG noted outdated, incomplete, or missing documentation across several functional areas inspected, including an out-of-date and incomplete continuity of operations plan; the lack of designated records management officers; and a number of information system security concerns, including concerns about data center management.

The OIG also noted a best practice in the area of removable media management in which the organization inspected uses a SharePoint tool to manage lifecycle tracking of removal media such as compact disks. The media tracker SharePoint site provides the ability to create serial numbers for the media, identify the contents, assign ownership, and document the destruction of the media at the end of its useful life. The OIG also called out as best practices a regional compliance periodical used to keep personnel informed about intelligence oversight initiatives and a standard operating procedure for personnel working in a mixed-authorities environment.

Assessment of Far East Data Call Responses – Four Advisory Memorandums

Assessments Data Call Responses for Four Overseas Sites – Advisory Memoranda

The Office of the Inspector General (OIG) Inspections team had prepared to inspect four overseas sites during March and April 2020. Due to the COVID-19 pandemic, however, the OIG revised its plans and instead assessed the documentation provided by the sites in response to the OIG's pre-inspection data call. During these assessments, the OIG reviewed pertinent documents, support agreements, policies, regulations, and intelligence oversight data, and identified areas where the documentation did not meet the terms of applicable policy, regulation, or guidance. The goal of these assessments and the resulting Advisory Memoranda was to assist site leaders in addressing observations and potential deficiencies until the inspections can be rescheduled. To help address issues that were evident based on the review of documentation and assist with preparations for the future inspection, the OIG made recommendations to address specific findings and also included comments on what steps should be taken to uncover the root causes of observed or possible deficits.

Classification Portion Markings on Email and Other Electronic Media Files – Advisory Memorandum

On 21 December 2020, the OIG issued an Advisory Memorandum on Classification Portion Markings on Email and Other Electronic Media Files. Based on observations from multiple inspections and at NSAW that many emails and other electronic media files—such as Skype messages and websites—do not contain portion markings, the OIG issued two recommendations, one of which was closed by the time the Advisory Memorandum was issued, in order to aid the Agency in achieving adherence to NSA/CSS Policy Manual 1-52, NSA/CSS Classification Guide, 10 January 2018, Intelligence Community Directive (ICD) 710, Classification Management and Control Markings System, 21 June 2013, and DoD Manual (DoDM) 5200.01, Volume 2, DoD Information Security Program: Marking of Classified Information, Incorporating Change 2, 19 March 2013.

Ongoing Inspection Work

The NSA OIG continues to work on the report for one inspection conducted jointly with Army Intelligence and Security Command, U.S. Fleet Cyber Command, and 16th Air Force OIGs that evaluated the overall climate and the compliance, effectiveness, and efficiency of an overseas field site.

The NSA OIG also continues to work on the reports for two NSA-only inspections conducted in person prior to the pandemic and four such inspections conducted virtually during the current reporting period that evaluated the overall climate and the compliance, effectiveness, and efficiency of the following organizations:

- NSA Cryptologic Representative, U.S. Africa Command;
- NSA Cryptologic Representative, U.S. European Command;
- NSA Cryptologic Representative, Defense Information Systems Agency (DISA)/Joint Force Headquarter-Department of Defense Information Network (JFHQ-DODIN);
- NSA Cryptologic Representative, U.S. Southern Command;
- NSA Cryptologic Representative, U.S. Central Command; and
- NSA Cryptologic Representative, U.S. Special Operations Command.

Intelligence Oversight

Special Studies and Oversight Memoranda Completed in the Reporting Period

Special Study of the Capabilities Compliance Incident Management Process

The OIG conducted this study to determine the efficiency and effectiveness of the NSA Capabilities Directorate's compliance incident management process for systems-related compliance matters. The Office of Compliance for Capabilities is accountable for the execution of this incident management process.

The study revealed the following concerns:

- NSA has not completed implementation of certain aspects of the Capabilities compliance incident management process, creating an environment in which such incidents are not handled consistently and timeliness requirements for reporting are not always met;
- Some incident management functions are performed inconsistently, which the OIG believes increases the risk that the Agency may fail to report incidents as required by law and policy, or fully address or mitigate such incidents;
- Resources, expertise, and training for managing Capabilities compliance incidents are insufficient, which contributed to incidents remaining in an open state for prolonged periods;
- NSA has not consistently met external and internal timeliness requirements for reporting Capabilities compliance incidents; and
- The NSA Incident Reporting Tool does not include all the functionality or information needed by incident managers to review, investigate, and process Capabilities compliance incidents.

The OIG made 15 recommendations to assist NSA in improving the execution and oversight of NSA's incident management process for Capabilities compliance incidents. Seven of the recommendations were closed before report publication.

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

The OIG conducted this evaluation to assess whether the procedures for disseminating FISA Section 702 counterterrorism collection to certain partners were sufficient to ensure compliance with the current legal and policy framework, including the protection of U.S. privacy, and whether the procedures enabled the efficient and effective dissemination of this information to certain partners.

The OIG found many of the dissemination operations were functioning as designed within legal, policy, and procedural parameters; however, the evaluation revealed a number of concerns, including but not limited to the following:

- Not all personnel conducting dissemination operations had completed the required intelligence oversight training as required by NSA policy. Failure to meet this requirement increased the likelihood of non-compliance with the law, policy, and procedures and increased NSA's risk posture while conducting these operations;
- Although all personnel were required to adhere to the law and procedures governing the implementation of FISA Section 702 for all phases of the SIGINT cycle, NSA's FISA Section 702 query procedures were not releasable to the partners, increasing the likelihood of personnel executing noncompliant queries;
- Queries into SIGINT collection were suppressed from NSA's post-targeting review monitoring system, which increased the likelihood of the retention and collection of unlawful information in violation of the law and NSA policy; and
- The inherently manual nature of the evaluation, minimization, and dissemination processes increased the likelihood of noncompliance with approved procedures and adversely impacted overall efficiency.

The OIG made 16 recommendations to assist NSA in improving the execution and oversight of NSA's dissemination of FISA Section 702 collection to certain partners. Five of the recommendations were closed before report publication.

Ongoing Special Studies and Evaluations

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.

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

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

Limited Scope Evaluation of NSA's Rules Based Targeting (RBT) Controls

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

Limited-Scope Evaluation of Mission Correlation Table Data

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

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

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

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

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

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

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

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

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

Evaluation of NSA's Implementation of Title I FISA Authority

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

INVESTIGATIONS

Criminal Prosecutions

Two providers of foreign-language services, Comprehensive Language Center, Inc., based in the Washington, D.C. area, and Berlitz Languages, Inc., based in New Jersey, were charged in a case brought by the U.S. Department of Justice Antitrust Division with participating in a conspiracy to defraud the United States by facilitating the submission of false and misleading bid information to the NSA. As a result, competition was suppressed among legitimately qualified bidders for the contract, obstructing, by dishonest means, the government's ability to benefit from a competitive bidding process. The one count felony charges were filed in the U.S. District Court for the District of New Jersey, and both companies entered into deferred prosecution agreements in which they agreed to pay criminal penalties totaling $287,000, as well as restitution to the Agency in the amount of $56,984.

Jacky Lynn McComber, a former NSA contractor, was indicted by a federal grand jury in the District of Maryland on charges of submitting false claims of over 2,000 hours and making false statements to the NSA OIG. An indictment is not a finding of guilt. The case was investigated by the OIG and the Defense Criminal Investigative Service, and is being prosecuted by the United States Attorney's Office for the District of Maryland.

OIG Referrals

At the end of the last reporting period, there were 16 substantiated cases pending Agency action. During the reporting period, the Investigations Division referred 22 new cases involving Agency personnel to NSA Employee Relations (ER) for potential disciplinary action, and the Agency notified the OIG of disciplinary decisions or other employment actions with regard to 14 employees based on current and prior OIG reports. Three of those employees retired or resigned in lieu of removal, one employee was removed, two employees received a suspension of 10 days or more, two employees received written reprimands or counseling, and six employees did not receive disciplinary action. A total of 24 cases referred by the OIG to ER were pending action at the end of the reporting period.

OIG referrals pending ER action as of 9/30/2020	OIG referrals to ER from 10/1/2020-3/31/2021	Employment Actions reported to the OIG from 10/1/2020- 3/31/2021	OIG referrals pending ER action as of 3/31/2021
16	22	14	24

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 18 cases to the Department of Justice during the reporting period. In each case, the OIG had reasonable grounds

to believe that a violation of federal criminal law had occurred. The allegations referred included contractors submitting false labor charges. The OIG anticipates at this time that the government is likely to handle these cases administratively, rather than criminally.

OIG Hotline Activity

The Investigations Division fielded 715 contacts through the internal OIG hotline. The OIG received 6,318 submissions on the external OIG hotline.

Significant Investigations

Senior Executive: Courtesy and Respect/ Preferential Treatment

An OIG investigation determined that an Agency senior official failed to treat their subordinates with courtesy and respect, and created the appearance of preferential treatment to an individual.

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

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

Senior Executive: False Statement and Lack of Candor

An OIG investigation determined that an Agency senior official made false statements to OIG and Agency Security investigators in the course of separate official investigations. The senior official resigned in lieu of termination.

The investigative findings were forwarded to DoD OIG.

The case was referred to the U.S. Attorney for the District of Maryland and declined for prosecution.

Senior Executive and GG15: Whistleblower Reprisal

An OIG investigation determined that one Agency senior official and one GG15 Agency supervisor did not reprise against a subordinate employee for making protected disclosures to the employee's chain of command by removing the subordinate from their position and not promoting the subordinate. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel actions absent the protected disclosures.

The investigative findings were forwarded to DoD OIG.

Senior Executive and GG15: Whistleblower Reprisal

An OIG investigation determined that one Agency senior official and two Agency supervisors did not reprise against a subordinate employee during the promotion process. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel action absent the protected disclosures. The OIG also determined that the senior official and two supervisors did not abuse their authority.

Senior Executive and GG15: Whistleblower Reprisal

An OIG investigation did not substantiate allegations that an Agency senior official and a GG15 Agency supervisor retaliated against a subordinate by failing to consider the subordinate for promotion in reprisal for the subordinate's protected disclosures. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel action absent the protected disclosures. The OIG also determined that the senior official and the GG15 supervisor did not abuse their authority.

The investigative findings were forwarded to DoD OIG.

Senior Executive: Preferential Treatment

An OIG investigation determined that an Agency senior official did not misuse temporary duty funds while on official government travel orders and did not abuse their authority or give preferential treatment to specific individuals in violation of various Federal and Agency policies.

The investigative findings were forwarded to DoD OIG.

GG14: Whistleblower Reprisal

An OIG investigation did not substantiate allegations that two Agency supervisors retaliated against a subordinate by failing to consider the subordinate for promotion in reprisal for the subordinate's protected disclosures. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel action absent the protected disclosures. The OIG also determined that the two supervisors did not abuse their authority.

The investigative findings were forwarded to DoD OIG.

GG14: Whistleblower Reprisal

An OIG investigation into allegations that a GG14 Agency supervisor retaliated against a subordinate by failing to consider the subordinate for promotion in reprisal for the subordinate's protected disclosure was not substantiated. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel action absent the protected disclosure. The OIG also determined that the GG14 supervisor did not abuse their authority.

The investigative findings were forwarded to DoD OIG.

GG 13: Whistleblower Reprisal

An OIG investigation determined that allegations that an Agency supervisor retaliated against a subordinate by issuing a letter of reprimand in reprisal for the subordinate's protected disclosures were not substantiated. The investigation found by clear and convincing evidence that the employee would have been subjected to the same personnel action absent the protected disclosures. The OIG also determined that the supervisor did not abuse their authority.

The investigative findings were forwarded to DoD OIG.

Semiannual Reports on Investigations of Unauthorized Disclosures of Classified Information

In December 2019, the President of the United States signed into law the National Defense Authorization Act for Fiscal Year 2020 (NDAA). Section 6718 of the NDAA amends Title XI of the National Security Act of 1947 by adding Section 1105 – Semiannual Reports on Investigations of Unauthorized Disclosures of Classified Information. This section requires the OIG to submit to the congressional intelligence committees a report on investigations of unauthorized public disclosures of classified information, and do so not less frequently than once every six months.

During the period 1 October 2020 through 31 March 2021, the OIG has not opened or completed any investigations of disclosures of information that have been determined to be classified.

Summary of Additional Investigations

The OIG opened 35 investigations and 112 inquiries, while closing 34 investigations and 107 inquiries during the reporting period. The new investigations are reviewing various allegations including whistleblower reprisal, hostile work environment, violations of time and attendance, and contract billing misconduct.

Contractor Labor Mischarging

The OIG opened five new contractor labor mischarging investigations and substantiated seven cases. The substantiated cases closed during the reporting period resulted in the proposed recoupment of approximately $71,000. Ten investigations remain open.

Time and Attendance Fraud

The OIG opened five new investigations into employee time and attendance fraud and substantiated three cases during the reporting period. The substantiated cases resulted in the proposed recoupment of approximately $40,000. Disciplinary action against eight employees for time and attendance fraud is pending with the Agency. Four investigations remain open.

Computer Misuse

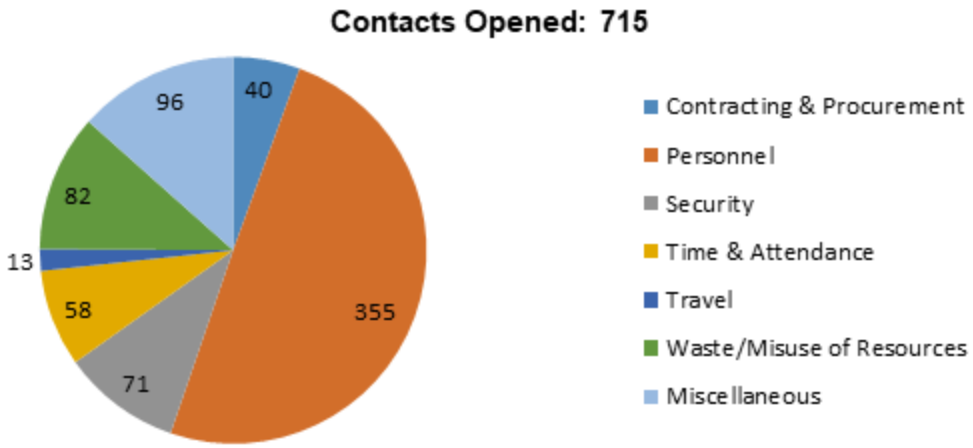
The OIG opened three new investigations involving allegations of computer misuse and substantiated eight cases during the reporting period. Disciplinary action against one employee for computer misuse is pending with the Agency.

Investigations Summary

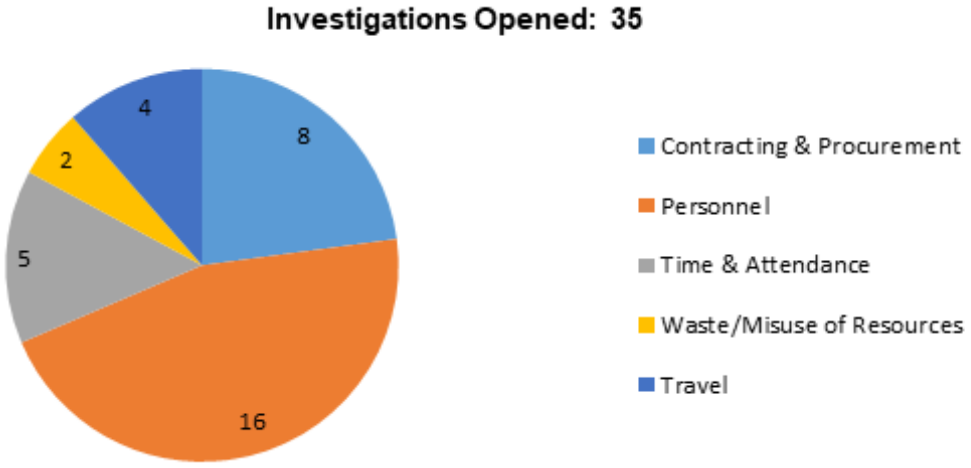
Total number of investigative reports issued	34
Total number of persons reported to DOJ for criminal prosecution	18
Total Number of Persons Referred to State and Local Authorities for Criminal Prosecution	0
Total Number of Indictments	1

Data contained in this report and table were obtained from NSA OIG Electronic Information Data Management System (eIDMS)

Total Hotline Contacts Received



Investigations Opened



Peer Review

No peer reviews were performed during the current reporting period.

Whistleblower Coordinator Program

The OIG continued its efforts to promote whistleblower rights and protections at the NSA. We also conducted various types of outreach to Agency personnel with respect to whistleblower reprisal. In that regard, the Assistant Inspector General for Investigations spoke about reporting misconduct in a presentation recorded for distribution across the NSA enterprise as part of the Agency's Stand Down on Extremism.

We also applaud the willingness of the Director to emphasize the importance of such reporting. The Director's Message entitled "Report Wrongdoing to the OIG," which was disseminated across the enterprise near the end of the reporting period, stated in part: :

> I encourage and expect all Agency employees and affiliates to cooperate fully with the OIG, and to promptly report to the OIG what they reasonably believe to be evidence of misconduct. Such reporting is required by law and NSA policy, and it enables the OIG to pursue such matters through its investigations and reviews, which benefits the Agency as a whole.

The Director's message went on to highlight that personnel are protected against any adverse personnel action for reporting suspected wrongdoing, and that any concerns about reprisal or retaliation should be reported to the OIG immediately. As the Director told the workforce: "You perform a valuable service to this Agency when you come forward to report such information to the OIG, and it is critically important that you feel comfortable doing so. … The bottom line is clear: If you see something, say something. Make the call."

The OIG appreciates the Director's support in delivering this important message, and we will continue to be forward leaning in exploring opportunities to ensure that all persons at NSA feel comfortable coming forward with information regarding suspected wrongdoing, and that they never suffer retaliation for doing so.

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

Oversight Work Involving Multiple Divisions

Pandemic Response Survey - Advisory Memorandum

Audits

Cybersecurity and Technology

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

Mission and Mission Support

Review of the Agency's Implementation of Executive Order 13950 on Combating Race and Sex Stereotyping

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

Financial Audits

Audit of NSA's FY2020 Financial Statements

Joint Audit of Intragovernmental Transactions

Inspections

Enterprise Inspections

Limited Scope Inspection of an overseas field location

Joint Inspections

Oversight Memoranda

Assessments of four Overseas Field Locations

Advisory Memorandum on Classification Portion Markings on Email and Other Electronic Media Files

Intelligence Oversight

Special Study of the Capabilities Compliance Incident Management Process

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

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

Audit Reports with Questioned Costs[1]

Report	No. of Reports	Questioned Costs (including Unsupported Costs)	Unsupported Costs
For which no management decision had been made by start of reporting period	2	$460,000,000	$420,000,000
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	2	$460,000,000	$420,000,000

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

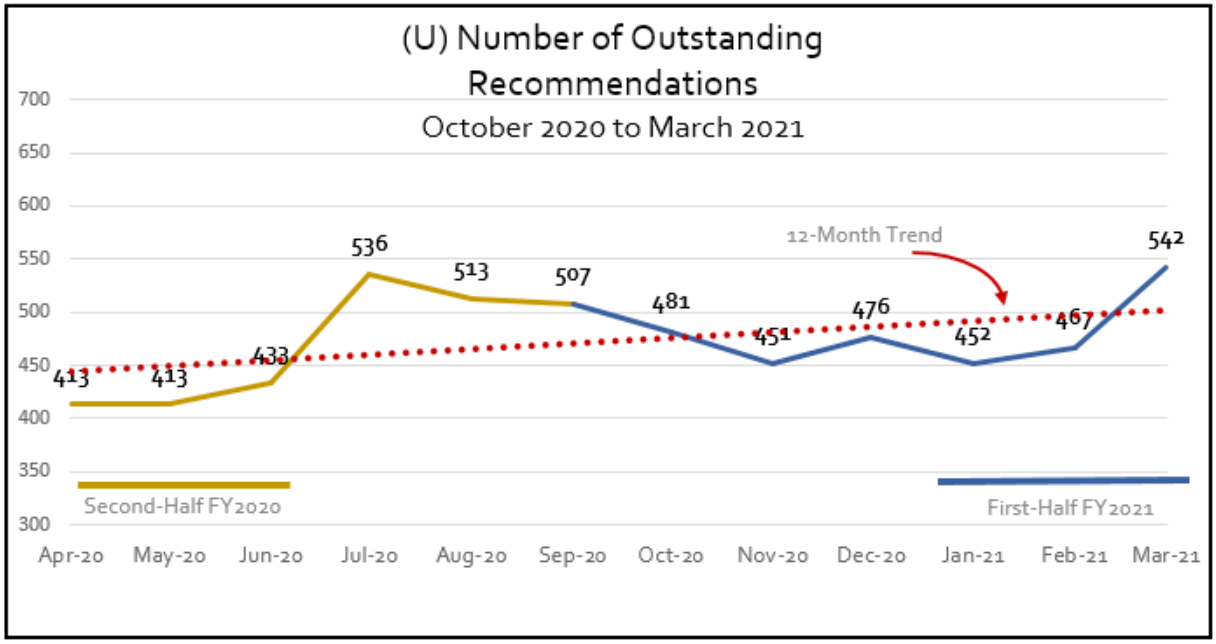
The OIG made 256 recommendations to NSA management in reports and oversight memoranda issued during this reporting period. The Agency closed 93 of the newly published recommendations and a total of 220 recommendations during the reporting period.

The OIG published 16 reports or other oversight products in the first half of FY2021.

Outstanding Recommendations

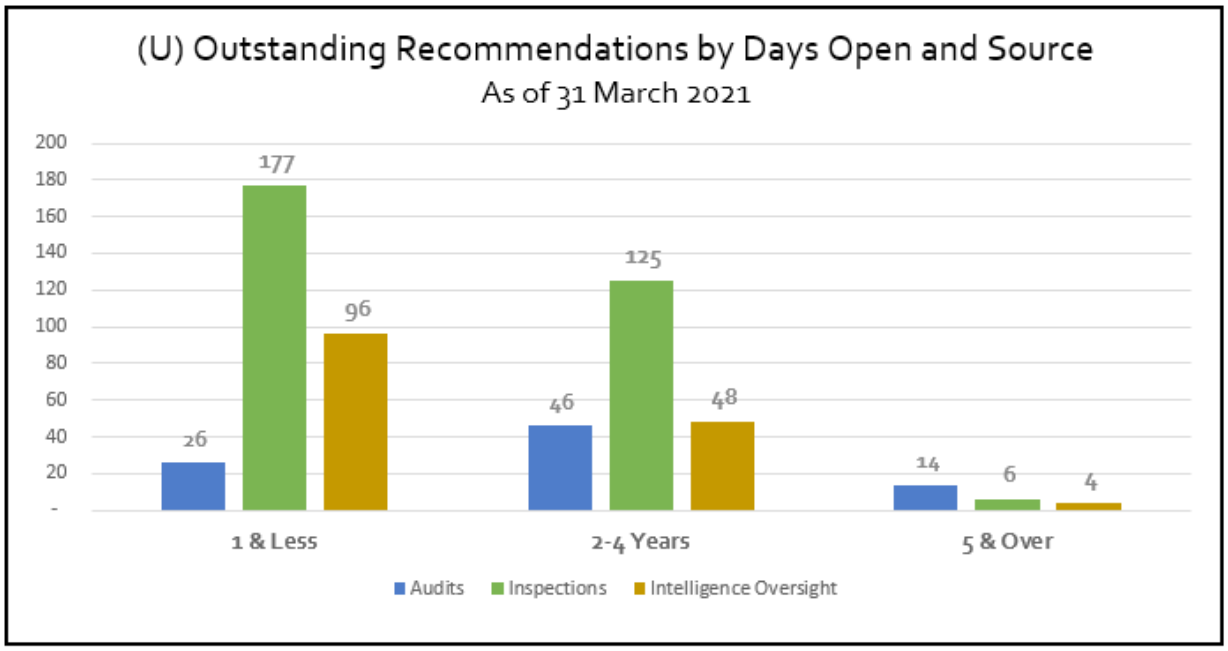
The OIG considers a report open when one or more recommendations contained in the report have not been closed. The number of outstanding recommendations is the total contained in all reports that remain open.

	Audits	Inspections	Intelligence Oversight	Total
Open reports	30	37	23	90
Outstanding recommendations	86	308	148	542



Outstanding Recommendations Breakdown

Days Open Groupings	Audits	Inspections	Intelligence Oversight	Total
1 & Less	26	177	96	299
2-4 Years	46	125	48	219
5 & Over	14	6	4	24
Totals	**86**	**308**	**148**	**542**



Management Policy Referrals

In addition to the recommendations arising from audits, inspections, evaluations, and reviews detailed above, the OIG has issued 11 referrals to Agency management involving policy issues since August 2018. All 11 referrals were closed based upon Agency action as of the end of the reporting period.

Significant Outstanding Recommendations – Audits

Audit of NSA Enterprise Solution and Baseline Exception Request Processes

The OIG found in 2011 that Agency organizations and contractors are able to purchase IT items without requisite approvals and recommended that the Agency implement automated compliance controls to address the issue. The Agency has implemented such a solution for software acquisitions. However, for hardware acquisitions, the Agency is reviewing IT policy to underpin a new process and automated solution.

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

Audit of Removable Media

Removable Media (RM) is any type of storage device (e.g., CDs, DVDs, USB drives) that can be removed from a computer while it is running. RM makes it easy for a Data Transfer Agent (DTA) to move data from one computer (or network) to another. The failure to manage and monitor the import or export of data using RM could result in the compromise of classified information or increase the risk of malware being transferred to critical networks. Although at the end of the reporting period the Capabilities Directorate provided a corrective action plan, the OIG identified additional steps needed to address the intent of report's recommendations.

Joint Audit of Intragovernmental Transactions

Prior audits of NSA's financial statements determined that NSA was unable to substantiate the accuracy of transactions between the NSA and another agency and this deficiency continues to contribute to a reported material weakness in the Agency's annual Report on Internal Control. Specifically, NSA has been unable to substantiate the accuracy of the amount its partner agency invoiced and liquidated against NSA advance payments or to demonstrate that NSA received the associated goods or services.

To address the deficiencies identified by the OIGs as discussed in the "Significant Problems, Abuses, and Deficiencies and Other Particularly Significant Reports" section of this report, the OIGs recommended that the agencies establish and formally document an agreement on the reporting responsibilities of each agency and the allocation of joint program expenditures to each agency. In addition, the NSA OIG recommended that NSA implement procedures to ensure that the transactions associated with joint programs are recorded in accordance with U.S. generally accepted accounting principles. The OIGs for both agencies also recommended that each agency implement procedures for providing detailed and timely transaction-level documentation to the requesting agency to support expense activity on Economy Act Orders. Successful implementation of the recommendations will provide NSA increased assurance that it received what it paid for and improved accountability and financial reporting on its financial statements. All three of these recommendations are significant and outstanding as of the end of the reporting period.

Significant Outstanding Recommendations – Inspections

Secure the Net / Secure the Enterprise / Insider Threat

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

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

- Two-person access controls are not properly implemented for data centers and equipment rooms.
- Removable media are not properly scanned for viruses.

Continuity of Operations Planning

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

Emergency Management Plan

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

Inspection of NSA's Personnel Accountability Program

The NSA OIG has performed five biannual inspections 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 of our inspections has been to determine whether NSA is in compliance with DoDI 3001.02. We repeatedly have determined that, while NSA did have policies that directly or indirectly reference aspects of personnel accountability, it did not have an implementing policy for DoDI 3001.02.

As DOD instruction will require the OIG to conduct another biennial assessment of the program in FY22, continued lack of action soon could result in a decade-long lack of adherence.

Significant Outstanding Recommendations – Intelligence Oversight

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

The OIG conducted this study to determine whether select NSA controls are adequate to ensure compliance with the Foreign Intelligence Surveillance Act of 1978 FAA Section 702 targeting and minimization procedures. As part of this study, the OIG tested NSA's controls that ensure that data is queried in compliance with the FAA Section 702 targeting and minimization procedures. The OIG found that NSA did not have a necessary system control. The Agency had previously identified this as a concern and has been working to implement a new system control. The OIG assessed that, until this system control is implemented, the Agency will be at risk for performing queries that do not comply with NSA's FAA §Section 702 authority. The Agency has indicated that until the recommended system control is available, it has in place multiple processes to aid in ensuring query compliance. Nevertheless, the OIG believes that this recommendation, which has an original target completion date of December 2017, remains valid and significant for the Agency to address. The OIG understands that the Agency continues to work toward taking action to implement a pre-query compliance control by June 2022.

Appendix D: Index of Reporting Requirements*

IG Act Reference	Reporting Requirements	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	1–4
§5(a)(2)	Recommendations for corrective action	N/A
§5(a)(3)	Significant outstanding recommendations	22-25
§5(a)(4)	Matters referred to prosecutorial authorities	14
§5(a)(5)	Information or assistance refused	i-ii
§5(a)(6)	List of audit, inspection, and evaluation reports	20
§5(a)(7)	Summary of particularly significant reports	1–4
§5(a)(8)	Audit reports with questioned costs	21
§5(a)(9)	Audit reports with funds that could be put to better use	21
§5(a)(10)	Summary of reports for which no management decision was made	4
§5(a)(11)	Significant revised management decisions	4
§5(a)(12)	Significant management decision disagreements	4
§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	19
§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	N/A
§5(a)(17)	Statistical tables of investigations	17-18
§5(a)(18)	Description of Metrics used in statistical tables of investigations	17-18
§5(a)(19)	Reports concerning investigations of Seniors	15-16
§5(a)(20)	Whistleblower Retaliation	15-16
§5(a)(21)	Agency interference with IG Independence	ii
§5(a)(22)	Disclosure to the public	N/A
§5(a)(note)	P.L. 110-181 §845, Final completed contract audit reports	N/A
§5(a)(note)	P.L. 103-355 (as amended), Outstanding recommendations past 12 months	22-25

* Citations are to the Inspector General Act of 1978, as amended.

OFFICE OF THE INSPECTOR GENERAL

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

AUDIT

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

INSPECTIONS

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

INTELLIGENCE OVERSIGHT

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

INVESTIGATIONS

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

How to Reach Us

9800 Savage Road, Suite 6247

Fort George G. Meade, Maryland 20755

HOTLINE

301.688.6327

FAX: 443.479.0099