NATIONAL SECURITY AGENCY

OFFICE OF THE INSPECTOR GENERAL

Semiannual Report to Congress

1 October 2021 to 31 March 2022

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 the wise use of public resources; adherence to laws, rules, and regulations; and respect for Constitutional rights. 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.

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

Message from the Inspector General

It is my honor and pleasure to submit the Semiannual Report for the National Security Agency (NSA) Office of the Inspector General (OIG) for the period ending 31 March 2022. As reflected in this report, the OIG engaged in a wide range of oversight activities during this reporting period, all of which enhanced the integrity and efficiency of the programs and operations of this important Agency. This included the issuance of 14 reports and other oversight products prepared through the efforts of our Intelligence Oversight, Inspections, and Audits Divisions that addressed a wide range of programs and operations, including significant reports on NSA's procedures for wireless testing and training within the continental United States, the annual Financial Statement Audit, the state of Agency compliance with the Federal Information Security Management Act of 2014, and our latest evaluation of the Agency's critical Personnel Accountability Program. Our Investigations Division continued to handle a workload that has substantially increased over the past several years, resolving a number of complex matters as detailed in the "Investigations" section of this report. As reflected in this report, our Whistleblower Coordinator Program and Diversity and Engagement Committee have continued their important work, and we have a new section in the report highlighting the evolution of our assessment of the top management and performance challenges faced by the Agency into a more dynamic and impactful product.

During this reporting period, we at the OIG also engaged in the valuable process of reassessing the vision, mission, and values of our organization, as well as our strategic goals and objectives in achieving same. We reaffirmed that the simple but essential vision of the OIG here at NSA is to promote positive change through impactful oversight. Our mission is to conduct independent oversight that promotes the wise use of public resources; adherence to laws, rules, and regulations; and respect for Constitutional rights. Through our audits, evaluations, inspections, and investigations, we detect and deter waste, fraud, abuse, and misconduct, and promote the economy, efficiency, and effectiveness of Agency operations.

We pursue our vision and achieve our mission through application of our values. At the NSA OIG, our core values are integrity, independence, and transparency. For our work to be authoritative, it must be imbued with integrity and the product of the independence through which we conduct our oversight efforts. We have continued to enhance transparency, including in this reporting period, issuing two unclassified versions of previously issued audits. In the *Audit of the Agency's Parking and Transportation Initiatives*, we found, among other things, that due to a lack of internal controls related to project oversight, risk assessment, and dispute resolution, the Agency wasted $3.6 million

constructing a parking structure that had never been built in the United States before and ultimately had to be demolished without ever being used. In the *Audit of Cost-Reimbursement Contracts*—the latest in our public reporting on Agency contracting practices—we made a number of significant findings, including that the Agency's Contracting Officer Representative process was ineffective and inefficient, and that its review of actual costs was insufficient. This caused us to question labor charges of approximately $227 million and travel charges of over $226,000, totaling approximately 75 percent of the invoices sampled in our audit. This Semiannual Report itself will mark the ninth consecutive time we will have prepared an unclassified version of our overarching reporting vehicle, substantially enhancing transparency across the full range of our oversight work. As in the past, all of these public reports have been and will be released on our independent website, https://oig.nsa.gov, as well on the aggregator site operated by the Council of the Inspectors General on Integrity and Efficiency, https://www.oversight.gov. And this reporting period marks the next step in our transparency efforts, as our office joined many in the broader OIG community on Twitter, where people interested in our work can follow us @NSAOIG.

Pursuant to the Inspector General (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 uncertainty and challenges of travel during this reporting period, the OIG made a total of 171 recommendations to NSA leadership that we believe will be impactful in improving the economy, efficiency, and effectiveness of this critical Agency's operations.

I have often said that I believe one of the most difficult things for an IG, or an OIG, is to maintain the proper balance in their relationship with the department or agency they oversee—close enough to be supported in our oversight efforts but not so close as to adversely impact the critical independence of that work. I was pleased that, during this reporting period, the Director, NSA, issued a message to the workforce, building on the recommendation contained in the Office of Management and Budget's 3 December 2021 Memorandum, *Promoting Accountability through Cooperation among Agencies and Inspectors General*, M-22-04. That message crystallized many of these core principles and reflected Agency leadership's support for the OIG's independent oversight work here. We have a great team at the NSA OIG, and we will continue to work with integrity, independence, and transparency to conduct impactful oversight here.

ROBERT P. STORCH
Inspector General

Contents

OIG Executive Summary

Work at a Glance by Division

	Products
Work Involving Multiple Divisions	**1**
Intelligence Oversight	**5**
Inspections	**4**
Audits	**4**

Investigations

Contacts	**711**
Closed Investigations	**31**
Closed Inquiries	**115**
Proposed Recoveries	**$222K**
Cases Referred to U.S. Attorney	**14**

Oversight Work Involving Multiple Divisions

National Security Agency (NSA)/Central Security Service (CSS)—hereinafter referred to as NSA—Office of the Inspector General (OIG) Intelligence Oversight, Inspections, Audits, and Investigations personnel worked with our Data Analytics team to prepare, conduct, and analyze results of a follow-on COVID-19 pandemic survey of NSA civilian and military personnel. The objective was to obtain the views of the workforce, developed in the year since the Agency reconstituted its workforce and since the 2020 survey, regarding which NSA pandemic measures worked well and which measures could have been improved. The results were provided to Agency leadership on 14 March 2022 to assist the Agency in assessing measures it could implement to address both the current and possible future pandemic response efforts. The OIG also requested a response regarding actions taken or planned to address challenges identified.

Intelligence Oversight Division

The OIG's Intelligence Oversight (IO) Division issued five oversight products during this period. One quick reaction report (QRR) addressed concerns about NSA's failure to address a potential deficiency related to the Agency's handling of U.S. person (USP) information found in specific content collection acquired pursuant to Executive Order (EO) 12333, *United States Intelligence Activities*, issued 4 December 1981, amended 2008. The OIG made four recommendations for NSA to research and address this potential deficiency.

A second IO QRR stemmed from an evaluation of NSA's corporate query review system, LEGALEAGLE. During the evaluation, the OIG found 11 NSA systems with active Mission System Compliance Certifications that were not sending their respective query records to LEGALEAGLE from 1 March through 1 June 2021, including one certified to hold Foreign Intelligence Surveillance Act (FISA) data. The OIG made two recommendations to assist NSA in addressing these concerns.

An IO evaluation on NSA's process to purge unauthorized and otherwise noncompliant signals intelligence (SIGINT) data in accordance with legal and policy requirements revealed that the purge processes were generally effective and efficient. However, the OIG found that purge upon recognition was used for reasons unrelated to the purge process, resolution of tainted reports delays impacted completion of the purge process, and NSA's inconsistent management of compliance critical identifiers (CCIs) through the SIGINT data lifecycle resulted in incomplete purge of data from its repositories. The OIG made 10 recommendations to assist NSA in addressing these issues.

Another IO evaluation focused on NSA's procedures for continental United States (CONUS) wireless testing and training, used by NSA and U.S. Armed Forces personnel working under SIGINT authorities or using SIGINT hardware and software, to develop, test, and train using equipment in environments that have the potential to collect content and/or metadata from non-consenting USPs or expose NSA capabilities and equities. The evaluation revealed potential performance of inherently governmental functions by contractor personnel, outdated policy, inadequate guidance and procedural documentation, untimely pre-activity reviews, and unclear IO training requirements, and questioned whether there were adequate resources for spectrum management review of proposed activities. The OIG made 23 recommendations to assist the Agency in resolving these weaknesses.

The OIG of the Intelligence Community (IC IG) and NSA OIG IO Division completed a joint review focused on whether the management and IO of the Intelligence Community (IC) Advanced Campaign Cell (ACC) ensured that processes and procedures were in place to conduct operations that complied with laws and IC and Department of Defense (DoD) policies. The OIGs identified inconsistencies in management and internal management controls and exceptions that increased risk to handling data despite the IC ACC having processes and procedures in place to operate within laws and IC, DoD, and NSA policies. The joint review resulted in 18 recommendations. However, the IC ACC was closed prior to the issuance of the report, so recommendations in the report were provided for informational and guidance purposes only.

Inspections Division

During this reporting period, the Inspections Division issued two inspection reports, one evaluation report, and one advisory memorandum.

In response to the ongoing global COVID-19 pandemic, we continued adapting our approach to inspections, conducting two new "hybrid" inspections. The OIG performed the majority of these hybrid inspections virtually and then sent small teams to the site to assess areas that required in-person inspection.

Audits Division

The Audits Division is divided into three branches: Mission and Mission Support, Cybersecurity and Technology, and Financial Audits. During this reporting period, the Audits Division issued four reports to improve Agency operations. Some highlights from this reporting period include:

The Mission and Mission Support branch issued the *Audit of the Implementation of the Coronavirus Aid, Relief, and Economic Security (CARES) Act*, which found that the Agency had significant issues implementing the CARES Act, including insufficient invoice reviews. Evolving guidelines, reduced contract oversight staffing during the COVID-19 pandemic, an over-reliance on contractor-provided information, and the absence of clear and comprehensive Contracting Officer Representative oversight procedures for CARES invoices caused the OIG to question more than $16.4 million, or 40 percent of sampled CARES invoice charges.

The Cybersecurity and Technology branch performed the annual *Evaluation of the NSA's Implementation of the Federal Information Security Modernization Act of 2014* (FISMA). We evaluated the Agency's information technology (IT) security posture against eight Office of Management and Budget (OMB)-stipulated metric areas and found that NSA had consistently implemented its policies, procedures, and strategies for six of eight evaluated IT security areas: Incident Response, Identity and Access Management, Information Security Continuous Monitoring, Risk Management, Data Protection and Privacy, and Security Training. This is a considerable improvement from FY 2020; however, there remains significant room for improvement in all IT security areas.

The Financial Audits branch focused on the congressionally mandated audit of NSA's financial statements, which identified a number of material weaknesses, as detailed in the "Significant Problems, Abuses, and Deficiencies and Other Particularly Significant Reports" section below. While there has been progress in a number of important respects, six areas—General Property, Plant & Equipment; Procurement Activity and Accounts Payable Accrual; Budgetary Activity; Fund Balance with Treasury and Deposit Funds; Financial Reporting; and Entity Level Controls— were reported as material weaknesses.

Investigations Division

During this reporting period, the Investigations Division received and processed 711 contacts on our classified systems that resulted in the initiation of 17 new investigations and 89 new inquiries. Investigations include allegations into acquisition fraud, standards of conduct violations, computer misuse, hostile work environment, contractor labor mischarging, travel card misuse, time and attendance fraud, government vehicle misuse, and reprisal. The OIG closed 31 investigations and 115 inquiries during the reporting period, and referred to the Agency proposed financial recoveries of approximately $221,600 based on substantiated fraud. Based on current period and past OIG investigations, the Government recovered a total of approximately $421,190. As a result of OIG investigations, four employees retired, resigned in lieu of removal, or had other disciplinary actions taken, ranging from suspensions to reprimands. Fourteen 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 (DIRNSA), and Congress pursuant to Section 5(d) of the Inspector General (IG) 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:

Evaluation of the Procedures for CONUS Wireless Testing and Training

The OIG conducted this evaluation to determine the effectiveness and efficiency of procedures for conducting certain wireless signals collection testing and training exercises and to determine the degree to which those procedures ensure compliance with the laws, directives, and policies that protect civil liberties and individual privacy. These activities have the potential to collect content and/or metadata from non-consenting U.S. persons (USPs) or expose NSA capabilities and equities. The evaluation revealed potential performance of inherently governmental functions by contractor personnel, outdated policy, inadequate guidance and procedural documentation, untimely pre-activity reviews, and unclear IO training requirements. The review also questioned whether resourcing was adequate for spectrum management review of proposed activities. The findings identified by the OIG in this evaluation increase the risk that wireless testing and training activities may be performed inefficiently or in a noncompliant manner, potentially impacting the privacy rights of USPs and adherence to policy and regulation.

The OIG made 23 recommendations to assist the Agency in resolving these weaknesses, including:

- Evaluating functions related to the review and concurrence for wireless testing and training requests to determine if they constitute inherently governmental functions and, if so, taking appropriate action related to contractor personnel activities;
- Updating existing, or creating new, policies to more effectively address wireless testing activities;
- Clarifying and publicizing IO training requirements for personnel performing these activities; and
- Addressing the lack of trained spectrum management professionals.

Out of the 23 recommendations, management's planned actions met the intent for 15 recommendations, 2 other recommendations were closed upon issuance of the report, and the OIG assessed the Agency's action plans did not meet the intent for the remaining 6 recommendations.

Evaluation of NSA's Personnel Accountability Program

The OIG performed the biennial evaluation of NSA's personnel accountability program, as required by Department of Defense Instruction (DoDI) 3001.02, *Personnel Accountability in Conjunction with Natural or Manmade Disasters*, issued 3 May 2010. The overall objective of the evaluation was to ensure NSA's compliance with DoDI 3001.02, which prescribes 15 responsibilities for the accounting and reporting of DoD-affiliated personnel following a natural or man-made disaster. The OIG's evaluation revealed that NSA's personnel accountability program does not comply with 5 of the 11 requirements applicable to the Agency. Deficiencies included:

- NSA has not officially appointed a Personnel Accountability Program Manager,
- NSA personnel accountability procedures are contained in a draft policy that has not been finalized,
- NSA has not provided the necessary information and guidance to educate the workforce on their personnel accountability roles and responsibilities, and
- NSA has not established internal procedures to monitor compliance with DoDI 3001.02.

The first deficiency listed above is new to this report, but the other four were retained from the OIG's *Evaluation of NSA's Personnel Accountability Program*, issued 21 February 2020. This first deficiency was resolved when the DIRNSA, signed the staff processing form *Designation of Personnel Accountability Program Manager (A35)* on 27 October 2021.

The OIG made two recommendations to assist the Agency in addressing these issues, including one recommendation addressing the four remaining outstanding areas of noncompliance that was carried forward from the 2020 OIG evaluation. NSA has not been fully compliant with DoDI 3001.02 since the instruction was issued in 2010, resulting in a decade-long lack of adherence in this important area.

Audit of NSA's FY 2021 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 (GAAP). 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 FY 2021, the audit 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, six areas—General Property, Plant & Equipment; Procurement Activity and Accounts Payable Accrual; Budgetary Activity; Fund Balance with Treasury and Deposit Funds; Financial Reporting; and Entity Level Controls—were reported as material weaknesses during the FY 2021 financial statement audit.

1. **General Property, Plant and Equipment (PP&E).** NSA did not have effective policies, processes, procedures, or controls to identify, accumulate, and report all classes of PP&E, to include General Equipment, Leasehold Improvements, 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. During FY 2021, NSA's estimation methodologies to value equipment reported in its financial statements remained in various stages of remediation and implementation. As a result, NSA did not utilize a comprehensive estimation methodology and therefore, did not implement management review controls during FY 2021 to value its equipment. In prior audits, long-standing issues with the completeness, existence, and accuracy of NSA's annual inventory control were noted. However, during FY 2021, limited testing procedures were performed at NSA Washington (NSAW) sites over the completeness and existence of the Agency's with regard to equipment and the accuracy of the data elements recorded for these assets.

2. **Procurement Activity and Accounts Payable Accrual**. NSA contracts with vendors and other third parties for goods and services for its use, and under reimbursable agreements, performs work on behalf of other government agencies and foreign governments. NSA uses accrual methodologies for its accounts payable balances, which estimate an amount for goods and services received that were not yet billed at fiscal-year end. In prior audits, NSA did not have controls designed and implemented related to the accuracy and validation of key data inputs, as well as the validation of key assumptions associated with NSA's accounts payable accrual methodology for Federal and non-Federal vendors. These deficiencies also impacted the design and implementation of management's lookback controls over the associated 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. Further, NSA did not have sufficient business processes and controls to consistently distinguish between costs that should be recorded as an expense versus costs that should be recognized as an advance or prepayment.

3. **Budgetary Activity.** Prior audits determined that NSA's processes, procedures, and controls related to the completeness and existence of its Undelivered Orders (UDOs) were not designed and operating effectively. As a result of control deficiencies noted in NSA's monitoring of UDOs from prior audits dating back to FY 2017, NSA developed corrective actions to monitor, identify, and correct invalid Unliquidated Obligations but was not able to complete such remediation efforts during FY 2021. These deficiencies continued to impact NSA's ability to provide sufficient documentation to support its UDOs.

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 receives funding in advance from its foreign partners to perform various projects under accommodation buy agreements. NSA records the initial inflow to non-Entity FBwT with an offsetting Deposit Fund Liability. During FY 2020, NSA adopted a new DoD policy that instructed that all Defense-wide deposit funds and related liabilities be reported at the Defense-wide level and not reported by the individual component entities. As a result, NSA removed the deposit fund asset and liability balances as of 30 September 2020. Subsequent to adopting DoD's policy, NSA formalized its accounting and reporting policy for its foreign accommodation buy process in the subsequent fiscal year. NSA's accounting and reporting policy for its foreign accommodation buy business process departed from GAAP. The policy departed from GAAP because NSA: 1) did not accurately represent its comprehensive relationship with the foreign partner activity and overstated the role of DoD in the process and 2) did not adequately evaluate certain aspects of GAAP when documenting its accounting policy as it relates to the fair presentation of NSA financial statements but instead concluded that

it must follow DoD policies. The audit also determined that NSA's processes, controls, and associated documentation relating to the accommodation buy business process were not sufficient to demonstrate whether NSA recorded and tracked partners' funds at the appropriate level for the partner based on the nature of the relationship, ensure that the Unfilled Customer Order with Advance was established for the full amount of funds advanced pursuant to the letter of agreement, and support the closeout of projects upon completion of the order. Additionally, 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.

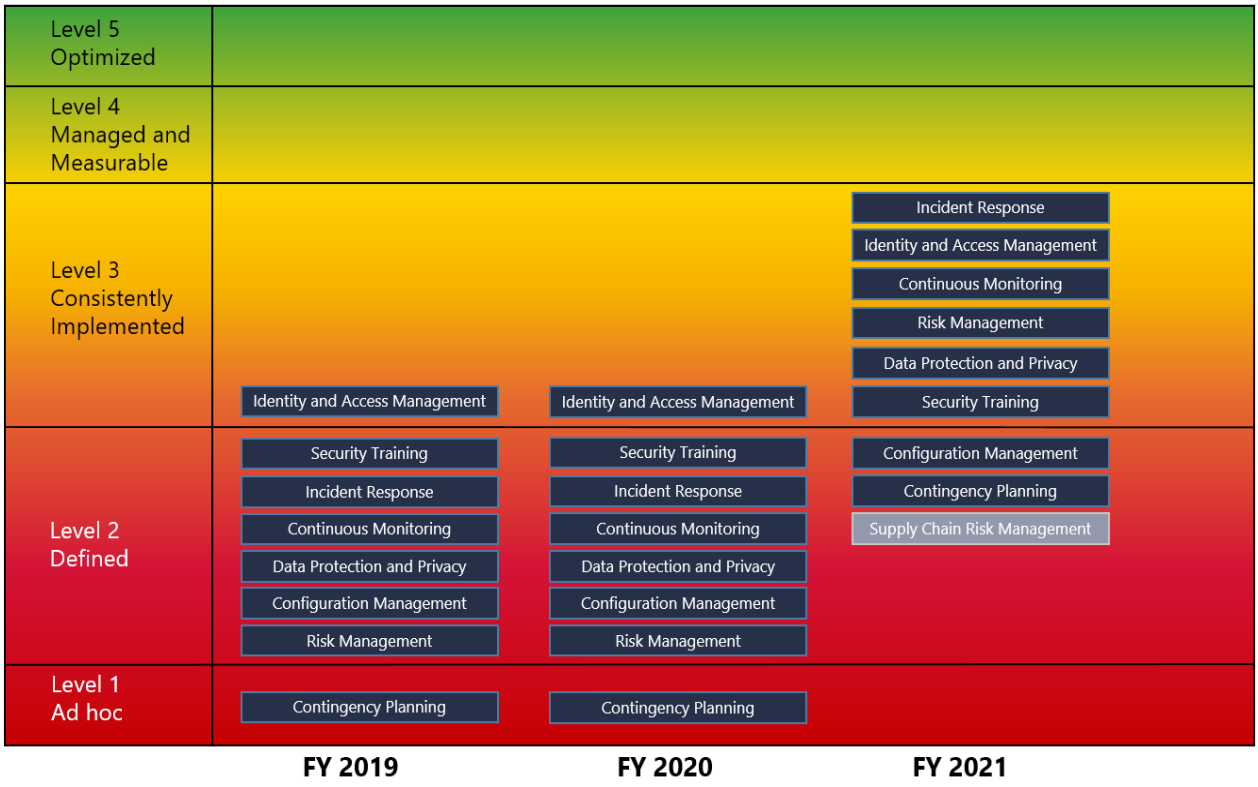
5. **Financial Reporting.** NSA did not adequately design all financial statement review controls to detect all material misclassifications, omissions, and presentation errors. Specifically, key internal controls related to the review of significant and unusual transactions and the review and approval of draft financial statements did not detect an error in the reporting of a material advance from a foreign partner received during FY 2021. Further, NSA did not establish adequate processes and controls to determine and evaluate whether significant or material vendor requests for equitable adjustments were appropriate for reporting or disclosure in the financial statements.

6. **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 weaknesses in NSA's entity level controls were caused by the following, in addition to the material weaknesses discussed above. Resource constraints encountered during FY 2021 may have required NSA managers to prioritize certain internal controls and reduce the number of personnel assigned to other internal controls. In addition, NSA did not complete a robust risk assessment throughout its business processes to identify and analyze risks related to the achievement of its defined financial reporting objectives. Further, NSA did not establish and document a sufficient process to assess its system of internal control over financial reporting and financial systems that incorporates the 17 principles of *GAO Standards for Internal Control in the Federal Government*, also referred to as the Green Book. Also, NSA did not fully implement adequate controls to evaluate segregation of duties to ensure that mitigating controls were designed and operating effectively throughout FY 2021. Finally, NSA did not obtain reliable data from internal and external sources needed to adequately support the amounts recorded within its financial statements.

Evaluation of the NSA/CSS Implementation of the Federal Information Security Management Act of 2014

In accordance with OMB guidance, the Federal Information Security Modernization Act (FISMA) of 2014 requires the OIG to annually 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 NSA had consistently implemented its policies, procedures, and strategies for six of eight evaluated IT security areas: Incident Response, Identity and Access Management, Information Security Continuous Monitoring, Risk Management, Data Protection

and Privacy, and Security Training.[1] As shown below, this is a considerable improvement from FY 2020 when only one IT security area, Identity and Access Management, was assessed as Level 3, Consistently Implemented. We also identified improvements in Contingency Planning, which moved from Level 1, Ad Hoc, to Level 2, Defined, over the past year.



FISMA IT Security Areas Over Three-Year Period

Note: Supply Chain Risk Management was assessed at a Level 2 but is not included in the Identify function rating. Additionally, the order of FY 2021 security areas in the figure above is based on the number of Level 4 and Level 3 maturity levels achieved from highest to lowest.

The OIG concluded that the improvements made by the Agency reflected increased control implementation, heightened leadership focus on these areas, and integration of information system security processes, and that the Agency continues to make improvements in all IT security areas. However, since none of the security areas reached an overall maturity of Level 4, Managed and Measurable, there remains significant room for improvement in all nine IT security areas.

[1]The FY 2021 FISMA metrics added a ninth area, Supply Chain Risk Management (SCRM) domain, within the Identify function area. This new domain focused on the maturity of agency SCRM strategies to ensure that products, system components, systems, and services of external providers are consistent with cybersecurity and SCRM requirements. In accordance with OMB A-130, these new metrics were not be considered for the purposes of the Identify framework function rating in order to provide agencies with sufficient time to fully implement NIST SP 800-53, Revision 5, though we conducted an initial assessment to determine the baseline maturity level of this domain in support of future assessments and for Agency consideration in anticipation of its inclusion in future years.

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

Oversight Work Completed in the Reporting Period

Office of the Inspector General COVID-19 Pandemic Response Survey Advisory Memorandum

The NSA OIG conducted a COVID-19 Agency Pandemic Response Survey from 12 October through 4 November 2021 with the objective of obtaining the perspectives of the NSA workforce—civilian and military—regarding which of NSA's continued pandemic measures worked well and which measures could have been improved. This was the second NSA OIG COVID-19 Pandemic Response Survey; the initial survey ran from 31 August through 2 October 2020, so the current survey covered roughly one year since the close of the initial survey. The current survey results, gathered from the review of 4,263 responses and the consideration of 18,832 narrative comments, were provided to assist the Agency in assessing measures that it could implement to address both the current and any future emergency situations. As in the initial survey, the OIG used the same five-point scale and assessment methodology as the annual IC Climate Survey, with areas having 80 percent or more positive responses identified as strengths and those with 20 percent or more negative responses identified as challenges. Though the negative responses did not reflect a majority of respondents' views in these areas, they do reflect that a significant portion of respondents had a negative view of the Agency's continued pandemic response in these areas, which the OIG believes the Agency should consider both now and in responding to future circumstances.

As illustrated in the table, the OIG analysis of the current survey responses and comments revealed the following:

2021 OIG Pandemic Response Survey Categories and Results

2021 Survey Categories	Challenge (20% or higher)	Neutral (% criteria not met)	Strength (80% or higher)
Mission Adaptation and Continuity			X
Infection and Vaccination Guidance and Processes[a]	X		X
Denied-Access Guidance and Processes	X		
Pandemic Mitigations	X		
Communications and Sources	X		
Telework	X		
Work Schedule Flexibility		X	

[a] Note: This category resulted in the Vaccination Process being identified by the workforce as a strength while Infection Guidance and Processes was deemed a challenge.

Strengths

- Mission Adaptation and Continuity:
  - The ability of organizations to adapt and continue important mission functions during this time.
- Vaccination Process:
  - NSA's vaccination process, including the registration process, staffing of the vaccination sites, and administration of the vaccines.

Challenges

- Infection Guidance and Processes:
  - The management and monitoring of COVID-19 cases, specifically minimal and inconsistent contact tracing and difficulty in contacting Occupational Health, Environmental & Safety Services (OHESS) via telephone.
- Denied-Access Guidance and Processes:
  - The denied-access notification process, specifically the lack of consistent, timely notifications from OHESS when employees were put in denied-access status.
  - Inconsistent and confusing return-to-office guidance, such as unclear messaging or notification regarding the exact dates an employee could return to work and regarding what requirements had to be met prior to returning.
- Pandemic Mitigations:
  - Physical barriers that were either nonexistent or inadequate, minimal workspace disinfection, and workspaces that did not allow for proper six-foot distancing between employees.
  - The lack of an effective enforcement mechanism for maintaining adherence to masking and social distancing requirements, which did not appear to be based on scientific data.
  - The Agency's implementation of Centers for Disease Control and Prevention guidance for increased-risk employees.
- Communications and Sources:
  - NSAW shuttle guidance that seemed ever changing and unclear.
  - Communications from senior leadership—i.e., heads of departments or members of the leadership team responsible for directing policies and priorities of departments—to the workforce that were confusing, inconsistent, and/or lacked transparency.
- Telework:
  - Difficulty accessing government-furnished equipment for telework assignments.
  - A lack of telework opportunities and recognition received for work performed while teleworking.

- Policies and guidance related to telework that were confusing and resulted in guidance being inconsistently applied.
- Supervisor difficulty in accounting for employees' performance, as well as a lack of overall acceptance and support for telework among leadership in supervisors' chains of command.

Although not tied to specific strengths or challenges, the following emerged as other items of note from the OIG's review of written comments:

- The desire that the ability to meet, train, and attend events virtually should continue.
- Dissatisfaction with reduced services—mainly cafeteria, shuttle, and IT services.
- Dissatisfaction that NSA employees were not afforded workplace flexibilities similar to other government and/or IC agencies (e.g., 10 hours of administrative leave for parents).
- Per respondents outside of NSAW, dissatisfaction with inconsistent enterprise-wide policy implementation and guidance that was "NSAW-centric."

While the OIG did not have sufficient basis from the survey responses alone to make specific recommendations, we requested that the Agency report back to the OIG regarding the steps taken or planned in response to the challenges identified in the report.

Intelligence Oversight

Evaluations and Oversight Memoranda Completed in the Reporting Period

Quick Reaction Report Regarding NSA's Handling of U.S. Person Information Found in Specific EO 12333 Content Collection

The NSA OIG issued this quick reaction report as a result of questions and concerns brought to our attention regarding NSA's handling of U.S. person (USP) information found in specific content collection acquired pursuant to Executive Order (EO) 12333. Specifically, the OIG was notified about a potential ongoing deficiency in NSA controls that are designed to remove known USP information from specific non-targeted EO 12333 content collection prior to ingest into NSA repositories. The OIG made four recommendations for NSA to research and, as needed, issue updated guidance and modify controls to address this potential deficiency.

Quick Reaction Report on the Evaluation of NSA's LEGALEAGLE System Enrollment and Data Ingest Processes

While conducting an evaluation of NSA system enrollment and data ingest processes under what is known as LEGALEAGLE, the OIG identified a matter that warranted NSA's prompt attention before the completion of the evaluation.

During the OIG's assessment of NSA systems required to send data to corporate auditing system, the OIG discovered 11 systems with active Mission System Compliance Certifications that appeared not to be sending data to LEGALEAGLE from 1 March through 1 June 2021. Agency personnel reported to the OIG that one of the systems, which is certified to hold Foreign Intelligence Surveillance Act (FISA) data, failed to send data to corporate auditing system for approximately 18 months (from 27 April 2020 through 31 October 2021). We learned that approximately six months of data was not sent to LEGALEAGLE and was not retained locally and, therefore, are no longer available for review.

The OIG made two recommendations to assist NSA in addressing the concerns with regard to the metrics and the other 10 systems. The Agency agreed with both recommendations and submitted action plans that met the intent of the recommendations.

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

The OIG conducted this evaluation to assess the effectiveness and efficiency of NSA's process to purge unauthorized or otherwise noncompliant signals intelligence (SIGINT) data completely, reliably, and in a timely manner in accordance with legal and policy requirements, and whether actions taken

ensure that data subject to purge is not used in SIGINT reporting or other dissemination, in FISA applications, or to support FISA Section 702 targeting. For purposes of this evaluation, purge is the on-demand, retroactive removal of data items from NSA mission systems and SIGINT Collection Source Systems of Record, in accordance with NSA's procedures.

The evaluation revealed that the purge procedures, as executed by Corporate Purge Oversight and Performance (CPOP), were generally effective and efficient. However, the OIG also found procedural and systems deficiencies beyond the confines of CPOP's procedures that impacted NSA's accurate, timely, and complete purging of data from its repositories. The evaluation revealed the following concerns:

- **Purge upon recognition was used for reasons unrelated to purge.**

  In addition to the intended purpose of supporting the removal of data from NSA repositories in accordance with NSA standard minimization procedures, analysts used purge upon recognition to delete non-reportable information or to clear their queues. The OIG assessed that inconsistent direction on the approved application of purge upon recognition was the likely reason NSA analysts used it for these additional purposes. The misuse contributed to the overburdening of systems and human resources necessary for processing of purge upon recognition requests. Additionally, the improper application of purge upon recognition impacted the availability of information for legitimate mission use. The OIG assessed that NSA's procedural changes are good first steps in aligning a purge upon recognition method across NSA analytic tools and improving the overall efficiency of the purge process.

- **Delays in the resolution of tainted reports impacted the completion of purge.**

  The completion of "tainted report" mitigation procedures delayed the timely purging of data from NSA repositories. A tainted report is an NSA report sourced from data that had been identified as needing to be purged. While the identification of a tainted report is accomplished per CPOP purge procedures, the resolution of a tainted report is handled through a separate process managed by the Compliance Group's Dedicated Support for Cyber and Operations. The OIG found that the delays were likely the result of a tainted report process that relied on manual processes, cross-organizational collaboration, and systems and guidance shortcomings. Even though NSA safeguards prohibited the further use of a tainted report's underlying data as sources to NSA reports, FISA applications, and targeting requests, the OIG assessed that a protracted purge completion may have presented a risk that data subject to purge remained in NSA repositories and was available for analysts to exploit.

- **Inconsistent management of data elements critical to the purge process affected purge completeness.**

  NSA's inconsistent management of compliance critical identifiers (CCIs) throughout the SIGINT data lifecycle had repercussions that resulted in incomplete purge of data from its repositories. When CCIs were not managed consistently the ability of the purge process to find and purge data objects was thwarted and resulted in incomplete and delayed purge of data from NSA repositories. The OIG assessed that this poor data governance increased the likelihood of incomplete purges resulting in unauthorized data being kept in NSA's repositories and therefore, available for use by NSA analysts.

The OIG made 10 recommendations to assist NSA in addressing these issues. None of the recommendations have been closed, but the actions planned by management partially meet the intent of the recommendations.

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

Following the receipt of several hotline complaints the Office of the Inspector General of the Intelligence Community (IC IG) and the NSA OIG conducted a joint review of the IC ACC from 12 November 2019 through 31 May 2021. The objective of the joint review was to determine whether management and intelligence oversight of the IC ACC ensured that processes and procedures were in place to conduct operations that comply with laws and IC and Department of Defense (DoD) policies. The OIGs identified inconsistencies in oversight of the IC ACC and exceptions to existing processes and procedures to ensure data was handled in compliance with IC and DoD policies.

The joint review resulted in 18 recommendations. However, based on an Office of the Director of National Intelligence recommendation, the IC ACC was closed on 31 December 2021. Therefore, the recommendations in the report were provided for informational and guidance purposes and, if the IC ACC is reopened, the recommendations will be opened for action.

Ongoing Intelligence Oversight Work

Limited-Scope Evaluation of Mission Correlation Table Data

The objective of this 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 SIGINT data in NSA repositories; and administering MCT roles and responsibilities.

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

The objective of this 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 this 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 this 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.

Evaluation Related to Alleged NSA Targeting of a Member of the U.S. Media

This review relates to recent allegations that NSA improperly targeted the communications of a member of the U.S. news media. The OIG is examining NSA's compliance with applicable legal authorities and Agency policies and procedures regarding collection, analysis, reporting, and dissemination activities, including unmasking procedures, and whether any such actions were based on improper considerations. If circumstances warrant, the OIG will consider other issues that may arise during the review.

Joint Department of Homeland Security (DHS)/NSA OIG Evaluation of Cyber Intrusion Prevention Efforts

The objective of this joint evaluation is to assess the actions taken by NSA and DHS in advance of, or in connection with, recent intrusions into U.S. Government (USG) and private sector networks. The evaluation team will use the SolarWinds Orion and related intrusions as use cases to identify relevant authorities NSA and DHS used and determine if the agencies executed activities in accordance with those authorities. The team will also assess the efficacy of the policies, procedures, and mechanisms used to address threats and share information with appropriate stakeholders.

INSPECTIONS

Inspection Reports, Evaluations, and Oversight Memoranda Completed in the Reporting Period

Inspection of NSA/CSS Representative to U.S. Central Command

The NSA OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the NSA/CSS Representative (NCR) to U.S. Central Command (CENTCOM) during a virtual inspection. The OIG interviewed members of the NCR CENTCOM management and workforce with regard to NCR CENTCOM's operations and functions in the areas listed below. NCR leadership and personnel supported the OIG throughout this inspection. We identified a number of concerns, including:

- **Command topics:** A lack of consistent workforce knowledge of the existing NCR CENTCOM 2021 strategy; uncertainty regarding the right balance of resources to carry out the NCR's current mission; and the NCR's continued uncertainty about the future U.S. CENTCOM strategy, causing an inability to plan for future resource needs.
- **Mission operations:** Incomplete mission documentation, no defined analytic integrity standards program, no standard operating procedures for most positions, and a lack of documentation supporting knowledge transfer for key NCR CENTCOM positions.
- **Intelligence oversight:** A need for improvement in the areas of governance, operational integration, training, and foundational intelligence oversight knowledge.
- **Resource programs:** Outdated support agreements, the lack of designated records management officers and up-to-date file plans, and noncompliant Civilian Welfare Fund (CWF) processes.
- **IT and systems:** Concerns regarding infrastructure and IT end-user support, including the lack of spare parts.
- **Safety and emergency management:** Concerns regarding continuity of operations (COOP) and emergency management programs.
- **Security:** Concerns about security documentation and operations security programs.
- **Training:** Less than 100 percent completion of mandatory training and difficulty obtaining funding for professional development for both civilian and military personnel.

The OIG made a total of 46 new recommendations, incorporated 2 recommendations from other inspections that address issues also identified at NCR CENTCOM, and made 4 observations to assist NCR CENTCOM in addressing the findings identified during the inspection. The OIG closed eight of these recommendations at report publication.

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

The NSA OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the NCR and Cryptologic Services Group (CSG) to U.S. Southern Command (SOUTHCOM) during a virtual inspection. The OIG interviewed members of the NCR SOUTHCOM management and workforce with regard to NCR SOUTHCOM's operations and functions in the areas listed below. NCR leadership and personnel supported the OIG throughout this inspection. We identified a number of concerns, including:

- **Command topics:** The OIG identified a lack of consistent communication, which had a cascading effect on the governance of the NCR SOUTHCOM organization, including a lack of adherence to strategy, uneven morale, unclear staffing needs, and negative impact on customer support.
- **Mission operations:** The OIG found incomplete mission delegation documentation, a lack of a defined analytic integrity standards program, and a lack of standard operating procedures and knowledge management processes.
- **Intelligence oversight:** The OIG assessed that the NCR SOUTHCOM intelligence oversight program was effective but required improvement in the specific areas of training, oversight program and SIGINT access documentation.
- **Resource programs:** The OIG identified concerns related to support agreements, the NCR SOUTHCOM property accountability program, and records management.
- **Information technology and systems:** The OIG identified concerns in the areas of information system security and infrastructure.
- **Safety and emergency management:** The OIG found issues in areas related to safety, COOP, personnel accountability, and emergency action plans.
- **Security:** The OIG noted issues in several security areas.
- **Training:** The OIG identified concerns in the areas of mandatory training and funding for professional development for both civilian and military personnel.

The OIG made a total of 79 recommendations, 2 of which have been carried forward from previous OIG inspections, to assist NCR SOUTHCOM in addressing the findings identified during this inspection. In addition, the OIG noted one commendable practice in the intelligence oversight program that we believe may warrant replication elsewhere across the NSA enterprise.

Reimbursable Support Agreements—Advisory Memorandum

NSA/CSS Policy 1-38, *Intra-Agency and Interagency Reimbursable Support Agreements*, issued 29 July 2016, assigns responsibilities for entering into reimbursable support agreements with USG agencies. The policy states that "NSA/CSS elements shall use support agreements to document terms and conditions of any agreement through which NSA/CSS supports or is supported by another DoD Component or Federal agency and reimbursement (or payment) for said support is required." The policy also requires that NSA elements coordinate support agreement preparation and signature approvals with the Support Agreements Manager (SAM) regardless of whether NSA is the supplying or receiving activity.

A division in Business Management & Acquisition (BM&A) serves as the SAM for all of NSA's reimbursable support agreements, and the division provides corporate oversight of all reimbursable support agreements executed in NSA. This division oversees the reimbursable support agreement process, facilitates coordination and approvals, and maintains NSA's repository of reimbursable support agreements.

While conducting three inspections over the past two years, the OIG determined that NSA's repository of reimbursable support agreements was incomplete and that BM&A does not consistently verify that reimbursable support agreements are in the repository before processing orders. The OIG made two recommendations to address these concerns; the Agency agreed with both.

Ongoing Inspections Work

In addition to the above, the OIG continues to work on reports for three field inspections and two joint inspections that evaluated the overall climate and the compliance, effectiveness, and efficiency of the following organizations:

- Inspection of NSA/CSS Representative and Cryptologic Services Group to U.S. Special Operations Command;
- Inspection of NSA/CSS Representative and Cryptologic Services Group to North American Aerospace Defense Command/U.S. Northern Command;
- Inspection of NSA Utah;
- Inspection of Special United States Liaison Office Ottawa; and
- Joint Inspection of NSA/CSS Texas.

During the current reporting period, the Inspections Division also continued to work on the following evaluation:

Evaluation of Mission Assurance/Continuity of Operations

The OIG has noted COOP program concerns across the last several years of inspections and has cited this topic in the Semiannual Report to Congress as a significant outstanding recommendation to elevate the importance for the Agency to address the continuing challenge. The COVID-19 pandemic has reinforced the need to evaluate the effectiveness and efficiency of NSA's Mission Assurance/COOP program and to determine whether the program meets all of the requirements of pertinent policies and regulations.

AUDITS

Audit Reports, Evaluations, and Oversight Memoranda Completed in the Reporting Period

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

On 27 March 2020, Congress enacted the Coronavirus Aid, Relief, and Economic Security (CARES) Act in response to the COVID-19 national emergency. The CARES Act, Section 3610 provides agencies the discretion to reimburse paid leave to federal contractors confronted with the inability of their employees or subcontractors to perform work at a federal government-approved work site due to facility closures or restrictions when their job duties could not be performed remotely. Reimbursement under the CARES Act, Section 3610 has several limitations related to contractor status, billing rates, hours, and whether the contractor has received other COVID-19 relief. The overall objective of our audit was to determine whether NSA has economically, effectively, and efficiently implemented Section 3610 of the CARES Act.

The OIG found that NSA had significant issues implementing the CARES Act, including insufficient invoice reviews. Evolving guidelines, reduced contract oversight staffing during the COVID-19 pandemic, an over-reliance on contractor-provided information, and the absence of clear and comprehensive Contracting Officer Representative oversight procedures for CARES invoices caused the OIG to question more than $16.4 million, or 40 percent of the sampled CARES invoice charges. The questionable costs were due to the status of contractor employees, differences in invoice documentation, and questionable billing rates, hours, and timeframes.

The findings identified by the OIG in this audit increase the risk of the Agency being overcharged for CARES paid leave and of potential fraud by contractors. Because the Agency did not receive separate CARES funding, it used current contract funding, which, extrapolated to the full amount of CARES invoices, could impact current and future contract work and mission requirements. The OIG made four recommendations in the report. One recommendation was closed prior to issuance, and the actions planned by management meet the intent of the other recommendations.

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

The overall objective of this 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 CWF as of and for the fiscal years ended 30 September 2020 and 2019 were performed in accordance with U.S. generally accepted government auditing standards (GAGAS) and the terms of the contract for non-appropriated fund instrumentalities audit services. In its audit, the IPA firm reported that the

financial statements were fairly presented, in all material respects, in accordance with GAAP; that there were no material weaknesses in internal control over financial reporting; and that 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. The OIG found that the IPA firm's audit procedures and quality control review were not sufficient to identify a material misstatement on the CWF cash flow statement with regard to the initial disposition of funds received under the CARES Act. Additionally, the OIG found that the Restaurant Fund and CWF financial statements were not comparable and did not include adequate disclosures that would enable an intended user to understand the effects of material transactions and events regarding these funds. Because the IPA firm issued an unmodified opinion on the financial statements that contained a material misstatement and were not comparable, the NSA OIG concluded that the audit was not conducted in accordance with either GAGAS or GAAP.

As reflected in the IPA firm's *Independent Auditors' Report*, Agency management is responsible for the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States. This includes the design, implementation, and maintenance of internal controls relevant to the preparation and fair presentation of financial statements that are free from material misstatement. The OIG concluded that Agency management's review of the prepared financial statements was not sufficient to prevent, detect, and correct the material misstatement that we identified. The OIG made two recommendations to assist the Agency in addressing these findings.

Audit of NSA's FY 2021 Financial Statements

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

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

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

Ongoing Audits Work

Joint Evaluation of the National Security Agency Integration of Artificial Intelligence

The overall objective of the evaluation is to assess NSA's integration of artificial intelligence into SIGINT operations in accordance with DoD and IC guidance for artificial intelligence.

Audit of the Cryptologic Reserve Program

The objectives of this audit are to determine if the Agency is using civilian annuitants assigned and used as Selective Employment of Retirees and Standby Active Reserves economically, efficiently, and effectively. The scope of the audit includes a review of policies and procedures, interviews with stakeholders, a review of documentation from a sample of program participants, and benchmarking with similar programs used in the IC.

Audit of the Greenway Program

The Greenway Program provides IT services across the NSA enterprise. The objective of this audit is to determine if NSA's Greenway Program is organized and managed economically, efficiently, effectively, and in accordance with applicable policies and requirements.

Audit of NSA's SolarWinds Orion Internal Response

SolarWinds Inc. is an American company that develops software for businesses to help manage their networks, systems, and IT infrastructure. A SolarWinds product, Orion, used by about 33,000 public and private sector customers, was the focus of a large-scale cyber-attack. The attack was disclosed in December 2020 but occurred undetected months earlier. The overall objective of the audit (which is separate from the ongoing *Joint Evaluation of Cyber Intrusion Prevention Efforts* referenced in the "Intelligence Oversight" section of this report) is to determine whether the Agency has reasonable assurance that NSA systems and networks were not compromised by the SolarWinds Orion software vulnerabilities.

Audit of NSA's Management of Programs that Protect Especially Sensitive Classified Information

The overall objective of this audit is to determine if NSA is managing the programs that protect especially sensitive classified information efficiently, effectively, and in accordance with applicable policies.

Audit of NSA's FY 2021 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 FY 2022 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 GAAP. The audit will consider and report on internal control over financial reporting and compliance with certain laws, regulations, and other matters.

Evaluation of NSA's FY 2021 Application of Classification Markers, Compliance with Declassification Procedures, and the Effectiveness of Declassification Review Processes

In accordance with the National Defense Authorization Act for FY 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 FY 2021:

- 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; and
- The effectiveness of processes for identifying topics of public or historical importance that merit prioritization for declassification review.

NSA's Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Controls for Certain Contracts

The objective of the audit is to determine whether NSA securely procures ICT equipment under certain contracts via supply chain controls.

Evaluation of the NSA/CSS Implementation of the Federal Information Security Modernization Act

The OIG will conduct an evaluation of the NSA/CSS Implementation of FISMA. The overall objective of the evaluation will be to review the Agency's information security program and practices. In accordance with OMB guidance, we will assess the overall effectiveness of the Agency's information security policies, procedures, and practices.

Audit of Foreign Trading Partner Activity

The overall objective of this audit is to determine whether NSA effectively and efficiently manages foreign trading partner funding and execution through the Accommodation Buy process, including whether the Agency has internal controls sufficient to ensure proper use of such funding and accurate reporting of the status of such activities to the foreign trading partners.

INVESTIGATIONS

Criminal Prosecutions

The OIG continues to provide support for ongoing criminal cases the OIG referred to the Department of Justice (DOJ).

OIG Referrals

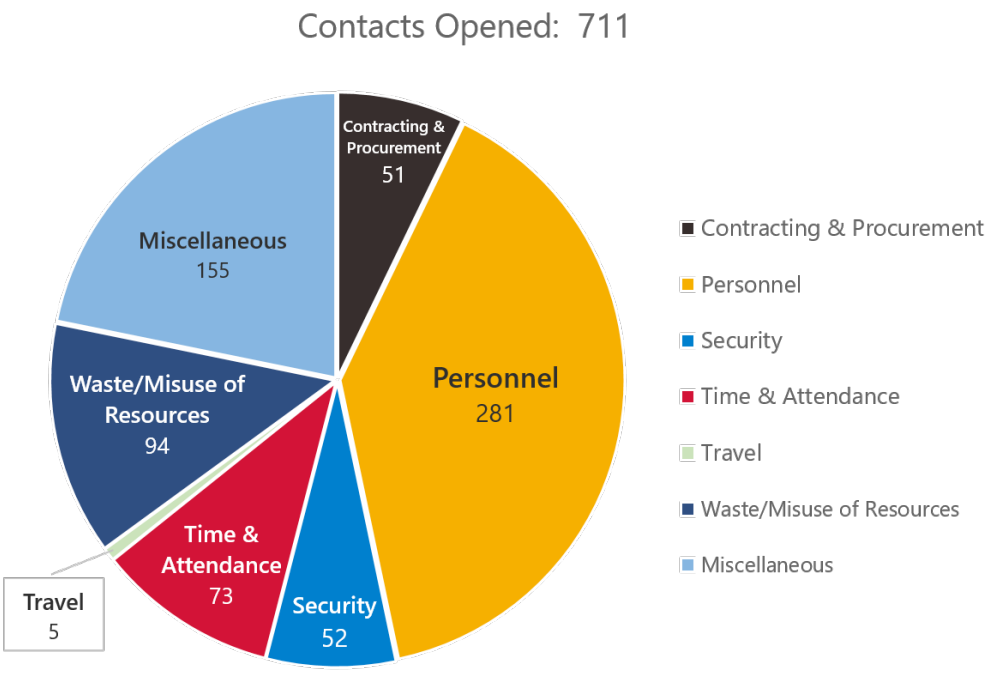
In accordance with section 4(d) of the IG Act and 5 U.S.C. appendix, the Investigations Division reported 14 cases to DOJ during the reporting period. In each case, the OIG had reasonable grounds to believe that a violation of federal criminal law had occurred. The allegations referred included activity such as false statements, civilians submitting false timesheets, providing source selection and nonpublic information to an Agency contractor, and contractors submitting false labor charges. The OIG anticipates at this time that these cases are likely to be handled administratively.

The Investigations Division referred 32 new cases involving Agency personnel to NSA Employee Relations (ER) for potential disciplinary action. During the reporting period, the Agency notified the OIG of disciplinary decisions for four employees based on OIG reports: one employee resigned prior to ER action; one employee received a suspension of 14 days or more; and two employees received written reprimands or counseling. A total of 49 cases referred by the OIG to ER are pending action at the end of the reporting period.

OIG Referrals to ER from 1 Oct 2021 – 31 Mar 2022	Employment Actions Reported to the OIG from 1 Oct 2021 – 31 Mar 2022	OIG Referrals Pending ER Action as of 31 Mar 2022
32	4	49

OIG Hotline Activity

The Investigations Division fielded 711 contacts through the internal OIG Hotline. The OIG received 3,716 submissions on the external OIG hotline.



Significant Investigations

Senior Executive and GG15: Whistleblower Reprisal

An OIG investigation determined that a senior official and an Agency supervisor did not reprise against a subordinate with regard to the employee's non-promotion (50 U.S.C. § 3234) and did not engage in any abuse of authority with respect to the subordinate (NSA/CSS PMM, Chapter 366).

Senior Executive: Hostile Work Environment

An OIG investigation determined that a senior official did not create a hostile work environment (DoDI 1020.04 and NSA/CSS PMM, Chapter 366) and did not fail to exercise the ethical values of "caring" and "respect" (DoD 5500.07-R and NSA/CSS PMM, Chapter 366).

Senior Executive and GG15: Whistleblower Reprisal

An OIG investigation determined that a senior official and a Contracting Officer did not reprise against an employee for changing their work location or terminating their Contracting Officer Representative-Technical appointment (50 U.S.C. § 3234) and did not engage in any abuse of authority with respect to the employee (NSA/CSS PMM, Chapter 366).

Senior Executive: Whistleblower Reprisal

An OIG investigation determined that a former senior official reprised against a subordinate by denying a cash award subsequent to the subordinate making a protected disclosure (50 U.S.C. § 3234). The investigation also determined that a different senior official did not reprise against the subordinate for the same action, as the senior official was not the responsible management official for the cash award.

Senior Executive and GG15: Whistleblower Reprisal

An OIG investigation determined that three supervisors did not reprise against an Agency employee for making protected disclosures (50 U.S.C. § 3234). The investigation also determined that the supervisors did not create a hostile work environment (DoDI 1020.04 and NSA/CSS PMM, Chapter 366) or engage in unfair treatment, harassment, or discrimination.

GG15: Whistleblower Reprisal

An OIG investigation determined that two Agency supervisors did not reprise against an Agency employee for making protected disclosures and did not engage in any arbitrary or capricious act that adversely affected the rights of the subordinate (NSA/CSS PMM, Chapter 366).

Senior Executive: Abuse of Authority and Harassment

An OIG investigation determined that a senior official failed to act impartially in that the senior official provided preferential treatment to a subordinate employee (5 CFR § 2635 and NSA/CSS PMM, Chapter 366).

Senior Executive: Hostile Work Environment

An OIG investigation did not substantiate that a senior official created a hostile work environment but did find that they failed to treat their subordinates with courtesy and respect, and misused their position (NSA/CSS PMM, Chapter 366, and 5 CFR § 2635.705).

All of the above 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 a new section: "Section 1105 – Semiannual Reports on Investigations of Unauthorized Disclosures of Classified Information." This section requires the NSA OIG to submit to the congressional intelligence committees a report on investigations of unauthorized public disclosures of classified information and to do so no less frequently than once every six months.

During the period from 1 October 2021 through 31 March 2022, the OIG has not opened or completed any investigations of disclosures of information that have been determined to be classified.

Recoveries

During the reporting period, the OIG referred to the Agency proposed financial recoveries of approximately $221,600 based on substantiated fraud, and the Agency reported total actual recoveries of approximately $421,190 from current and prior OIG referrals.

Summary of Additional Investigations

The OIG opened 17 investigations and 89 inquiries while closing 31 investigations and 115 inquiries during the reporting period. The new investigations are reviewing various allegations including whistleblower reprisal, computer misuse, misuse of government travel credit cards, standards of conduct, hostile work environment, violations of time and attendance, and contractor labor mischarging.

Contractor Labor Mischarging

The OIG opened one new contractor labor mischarging investigation and substantiated one case. The substantiated case closed during the reporting period resulted in the proposed recoupment of approximately $4,800. Three investigations remain open.

Time and Attendance Fraud

The OIG opened four new investigations into employee time and attendance fraud and substantiated two cases during the reporting period. The substantiated cases resulted in the proposed recoupment of approximately $47,500. Disciplinary action against eight employees for time and attendance fraud is pending with the Agency. Three investigations remain open.

Computer Misuse

The OIG opened two new investigations involving allegations of computer misuse and substantiated one case during the reporting period. Disciplinary action against two employees for computer misuse is pending with the Agency. Two investigations remain open.

Government Travel Credit Card Misuse

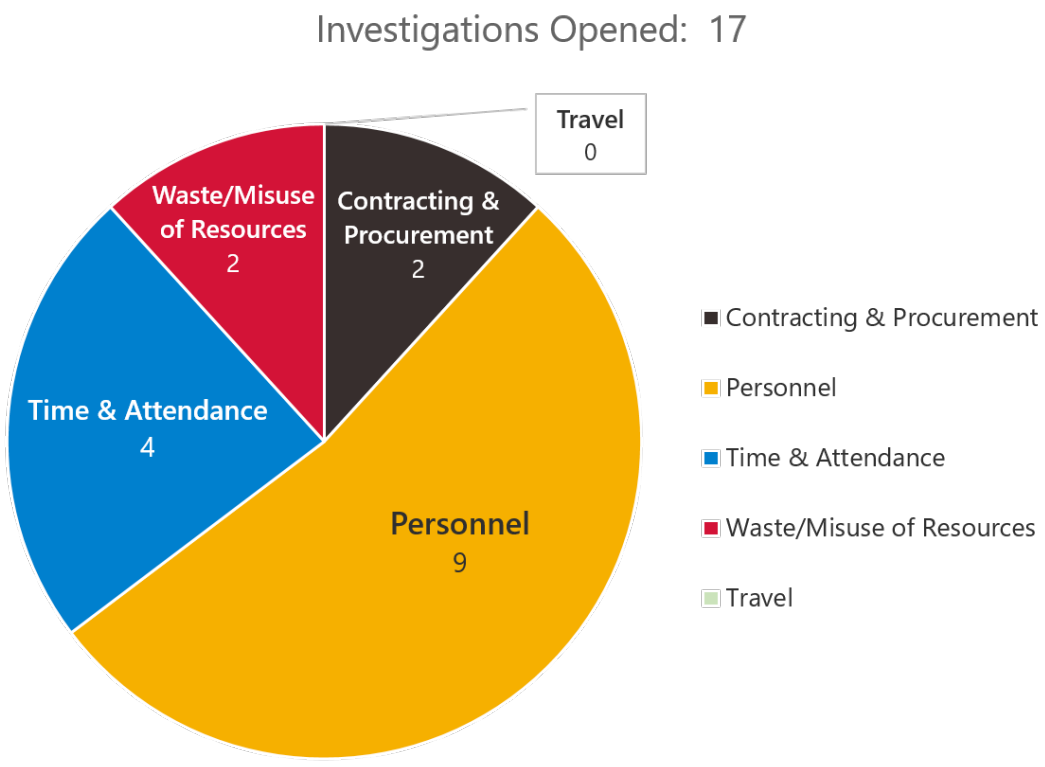
The OIG opened one new investigation involving allegations of government travel credit card misuse and substantiated four cases during the reporting period. The misuse for the substantiated cases totaled approximately $90,079 for non-sanctioned government purchases. Disciplinary action against eight employees for government travel credit card misuse is pending with the Agency. One investigation remains open.

Investigations Summary

Total number of investigative reports issued	31
Total number of persons reported to DOJ for criminal prosecution	14
Total Number of Persons Referred to State and Local Authorities for Criminal Prosecution	0
Total Number of Indictments	0

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

Investigations Opened



Top Management and Performance Challenges

In accordance with the Reports Consolidation Act of 2000, the NSA IG submits annually to Congress what the IG believes are the top management and performance challenges (TMPC) facing NSA. Per direction of the Act, the TMPC is included in NSA's *Agency Financial Report*. Over the past few years, the OIG made a concerted effort to enhance the TMPC document to have greater impact and to assist in identifying areas for future OIG oversight work. This has been accomplished through the efforts of a cross-divisional OIG working group, operating annually, that is dedicated to researching, interviewing, and crafting a robust, independent assessment. Additionally, the TMPC report design has been enriched to enhance its readability, accessibility, and professional appearance. These efforts have helped ensure greater awareness of the report in NSA and with Congress.

The OIG identified the following TMPCs that were included in NSA's FY 2021 *Agency Financial Report* that was submitted to Congress in November 2021:

- Recruiting and Retaining a Diverse, Equitable, and Inclusive Expert Workforce;
- Achieving Success in the Strategic Competition on Cybersecurity;
- Using and Addressing Adversary Use of Emerging Technologies;
- Protecting the Agency from Insider Threats;
- Enhancing Financial Management; and
- Responding to Unforeseen Events.

Peer Review

No peer reviews were performed during the current reporting period.

Diversity and Engagement

Established in February 2018, the OIG Diversity and Engagement Committee's (DEC) mission is as follows: "We foster a culture that embodies teamwork, emphasizes professional development, and values DEIA [diversity, equity, inclusion, and accessibility] in the OIG. We encourage all employees to use their unique experiences and perspectives to enhance the OIG's mission, and we work to identify and eliminate barriers to equal opportunity in the OIG."

During this reporting period, the DEC held a week-long virtual diversity event for OIG staff and management, focused on professional development and expanding diversity, equity, inclusion, civility, and mental health awareness. At close of the event, the OIG presented its Ralph Adams, Jr. Memorial DEIA Award, established in July 2021, to its first recipient.

The awardee was recognized for their sustained, innovative, and forward-thinking efforts in the promotion and advancement of DEIA in the OIG and for support of such efforts in the broader IG community.

Whistleblower Coordinator Program

The OIG has continued to make whistleblower protection one of its highest priorities. As we often say, whistleblowers perform an important service to 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. We at the OIG consider whistleblowers to be a vital source of information that helps us accomplish our mission by providing information that is critical to our ability to detect and deter waste, fraud, abuse, and misconduct throughout this extensive Agency and related to its diverse programs and operations.

To facilitate such disclosures, the OIG operates a Hotline, staffed by experienced and knowledgeable investigators, to receive and process complaints from inside and outside the Agency. Individuals may submit complaints anonymously; if the complainant elects to identify themselves, the OIG will maintain their confidentiality unless the complainant consents or disclosure is unavoidable. The OIG's Investigations Division examines all credible claims of reprisal.

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 that end, the OIG worked with the Agency to develop an online whistleblower training, which continues to be mandatory for all NSA employees, and we have continued to work with the Agency to refine the program based on user feedback and otherwise. The OIG's Whistleblower Coordinator continues to serve as a resource by which Agency employees and others can obtain further information about their rights and protections. Finally, the OIG continues to engage with Congress and other IC entities on legislative initiatives that would afford additional whistleblower protections.

This page intentionally left blank.

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

Oversight Work Involving Multiple Divisions

COVID-19 Pandemic Response Survey Advisory Memorandum

Intelligence Oversight

Quick Reaction Report Regarding NSA's Handling of U.S. Person Information Found in Specific EO 12333 Content Collection

Quick Reaction Report on the Evaluation of NSA's LEGALEAGLE System Enrollment and Data Ingest Processes

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

Evaluation of the Procedures for CONUS Wireless Testing and Training

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

Inspections

Inspection of NSA/CSS Representative to U.S. Central Command

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

Evaluation of NSA's Personnel Accountability Program

Advisory Memorandums

Reimbursable Support Agreements—Advisory Memorandum

Audits

Mission and Mission Support Branch

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

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

Cybersecurity and Technology Branch

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

Financial Audits Branch

Audit of NSA's FY 2021 Financial Statements

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	$231,360,000	$227,226,000
Issued during reporting period	1	$16,400,000	$16,400,000
For which management decision was made during reporting period			
Costs disallowed	2	$2,500	$2,500
Costs not disallowed	1	$227,000,000	$227,000,000
For which no management decision was made by end of reporting period	2	$20,757,500	$16,623,500

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 171 recommendations to NSA management in reports and oversight memoranda issued during this reporting period. The Agency closed 45 of the newly published recommendations and a total of 266 recommendations during the reporting period.

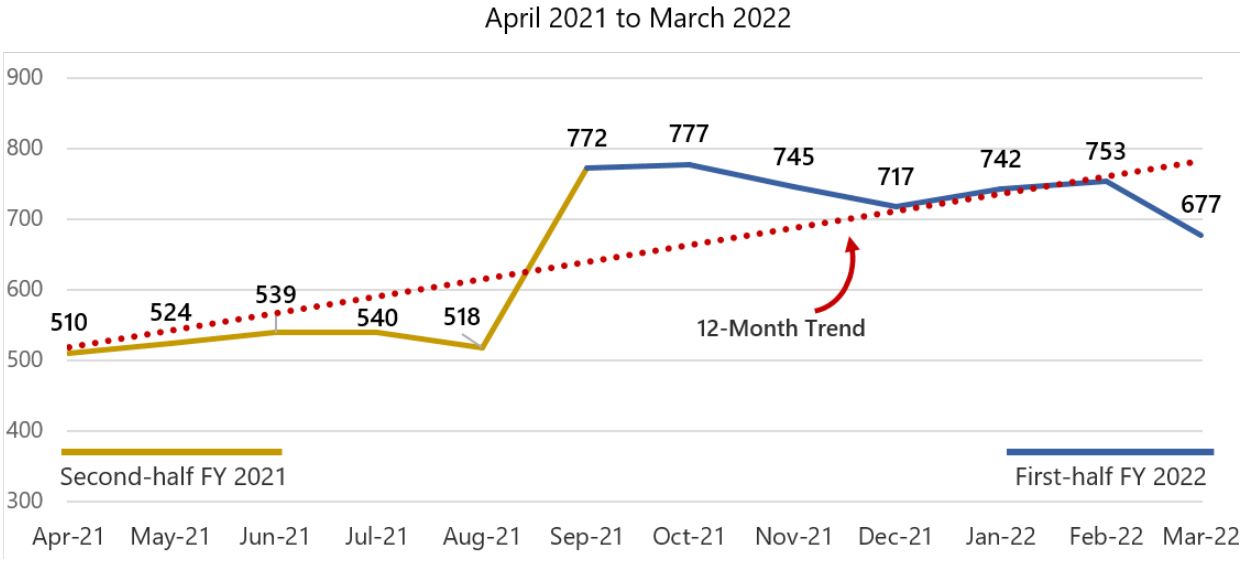
The OIG published 14 reports and other oversight products during this reporting period.

Outstanding Recommendations

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

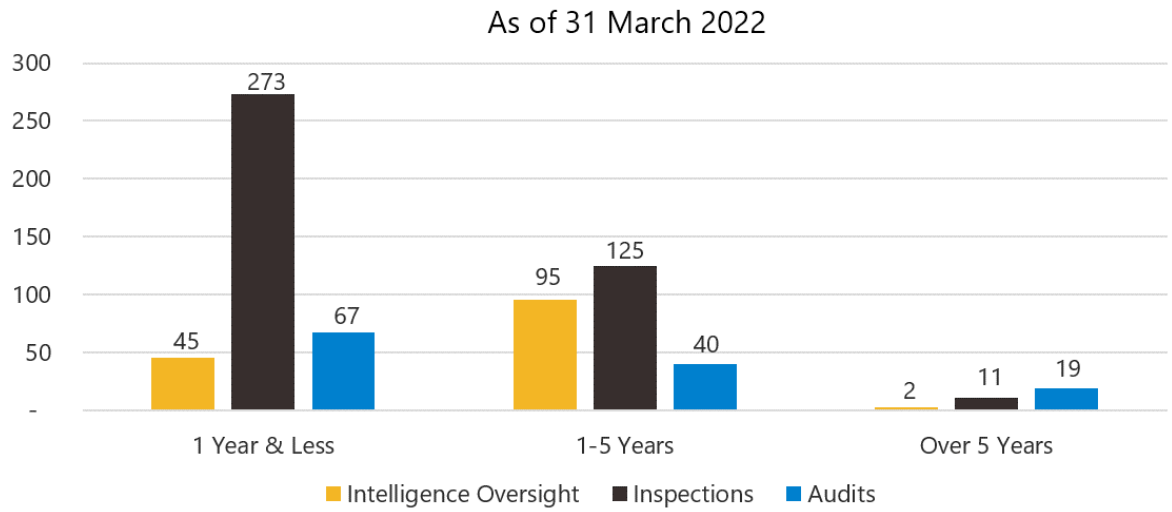
	Intelligence Oversight	Inspections	Audits	Total
Open reports	23	40	34	97
Outstanding recommendations	142	409	126	677

Outstanding Recommendations Breakdown



Days Open Groupings	Intelligence Oversight	Inspections	Audits	Total
1 Year & Less	45	273	67	385
1 – 5 Years	95	125	40	260
Over 5 Years	2	11	19	32
Totals	**142**	**409**	**126**	**677**

Outstanding Recommendations by Days Open and Source



Management Policy Referrals

In addition to the recommendations arising from audits, inspections, evaluations, and reviews detailed above, the OIG has issued a total of 14 referrals involving policy issues to Agency management since August 2018, including 3 issued during this reporting period. All 11 of the prior referrals and 1 of the referrals from this reporting period were closed based upon Agency action prior to the end of the reporting period. The other two referrals remain open.

Significant Outstanding Recommendations – Intelligence Oversight

Special Study of NSA Controls to Comply with FISA Section 702 Targeting and Minimization Procedures

The OIG conducted this study to determine whether select NSA controls are adequate to ensure compliance with FISA 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 FISA 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 FISA 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 February 2023.

Joint Review of Overhead SIGINT Compliance at a Joint Facility

The NSA OIG conducted a joint review of overhead SIGINT compliance at a joint facility. The objectives of this joint review were to assess the application of SIGINT compliance policies and procedures; assess the processes or mechanisms for raising questions and resolving disagreements regarding programs or operations as they relate to SIGINT compliance; and identify any hurdles that may keep SIGINT compliance policies from keeping pace with technological advances in the overhead radio frequency (RF) collection environment.

The OIGs identified a number of hurdles that may hinder the application of SIGINT compliance policies and their ability to keep pace with technological advances in the overhead RF environment. We also found that a process does not exist for raising questions and effectively resolving disagreements, and that there are no jointly accepted operating instructions for partner laboratory activities, which has resulted in what NSA at times has assessed to be noncompliant SIGINT access. As a result, the OIGs jointly made 18 recommendations, including 3 recommendations addressed directly to the Directors, to assist the agencies in addressing the findings detailed in the report.

NSA and its partner agreed with all of the report's recommendations and agreed to take action sufficient to meet their intent. The agencies determined that the three recommendations to the directors had to be resolved before the other recommendations could be addressed. The original target completion date for the three recommendations was March 2021.

The OIGs have been informed that the agencies' leadership have developed a draft framework that leverages definitions in DoD Manual 5240.01 in the context of EO 12333 missions to resolve key topics in the OIGs' joint report and that they intend to update the existing memorandum of agreement (MOA) to formally document the framework. The OIGs have also been told that, in parallel with the development of the updated MOA, both agencies will commence policy updates to identify and review policies, escalation procedures, and other relevant information to achieve the goals laid out by both Directors in their joint statement. The agencies have indicated the policy updates and escalation procedures are expected to be completed by September 2022.

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

The OIG has noted COOP program concerns across the last several years of inspections. The COVID-19 pandemic has reinforced these concerns. The OIG's *Evaluation of NSA's Mission Assurance/Continuity of Operations*, referenced in the "Inspections" section of this report, will evaluate the effectiveness and efficiency of this program and determine whether it meets all of the requirements of pertinent policies and regulations.

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.

Assessment of NSA's Personnel Accountability Program

DoDI 3001.02, *Personnel Accountability in Conjunction with Natural or Manmade Disasters*, issued 3 May 2010, establishes policy and assigns responsibilities for accounting and reporting of DoD-affiliated personnel following a natural or man-made disaster. Since CY 2011, DoDI 3001.02 has required IGs of DoD components to conduct evaluations biennially of the personnel accountability programs in their respective components to ensure compliance with this instruction.

As referenced under "Inspections" above, the OIG issued its most recent report in December 2021, in advance of the February 2022 date required by DoD instruction.

The ability of the Agency to account for affiliated personnel is critical following a natural or man-made disaster, including events like the COVID-19 global pandemic. The lack of pre-planned guidance and procedures to account for all personnel could impact the ability to achieve prompt continuation of operations following an incident or in a similar situation in the future.

Significant Outstanding Recommendations – Audits

Audit of NSA Enterprise Solution and Baseline Exception Request Processes

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

The OIG also recommended that the Agency develop contract provisions to require contractors to comply with NSA/CSS Enterprise Solutions/Baseline Exception Request processes, as NSA/CSS Policy 6-1, *Management of NSA/CSS Global Enterprise IT Assets*, issued 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 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. NSA asserts that it has implemented a combination of technical and administrative controls and is making improvements to the process, scheduled for review by 30 September 2022.

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.

The OIGs recommended that NSA implement procedures to ensure that the transactions associated with joint programs are recorded in accordance with GAAP. 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. These recommendations are significant and outstanding as of the end of the reporting period.

Appendix D: Abbreviations List

ACC	Advanced Campaign Cell
BM&A	Business Management & Acquisition
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CCI	Compliance critical identifier
CENTCOM	U.S. Central Command
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CONUS	Continental United States
COOP	Continuity of operations
CPOP	Corporate Purge Oversight and Performance
CSG	Cryptologic Services Group
CSS	Central Security Service
CWF	Civilian Welfare Fund
DEC	Diversity and Engagement Committee
DEIA	Diversity, equity, inclusion, and accessibility
DHS	Department of Homeland Security
DIRNSA	Director, National Security Agency
DoD	Department of Defense
DoDI	DoD Instruction
DOJ	Department of Justice
EAO	Economy Act Order
EO	Executive order
ER	Employee Relations
FBwT	Fund Balance with Treasury
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Modernization Act
FY	Fiscal year
GAAP	Generally accepted accounting principles
GAGAS	Generally accepted government auditing standards
IC	Intelligence Community
IC IG	Office of the Inspector General of the Intelligence Community
ICT	Information and Communications Technology
IG	Inspector General

IO	Intelligence oversight
IPA	Independent public accounting
IT	Information technology
MCT	Mission Correlation Table
MOA	Memorandum of agreement
NCR	NSA/CSS Representative
NDAA	National Defense Authorization Act
NSA	National Security Agency
NSAW	NSA Washington
OHESS	Occupational Health, Environmental & Safety Services
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PP&E	Property, Plant and Equipment
QRR	Quick reaction report
RF	Radio frequency
RM	Removable media
SAM	Support Agreements Manager
SCRM	Supply Chain Risk Management
SIGINT	Signals intelligence
SOUTHCOM	U.S. Southern Command
TMPC	Top management and performance challenges
UDO	Undelivered Order
USG	U.S. Government
USP	U.S. person

Appendix E: Index of Reporting Requirements*

IG Act Reference	Reporting Requirements	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	1-6
§5(a)(2)	Recommendations for corrective action	N/A
§5(a)(3)	Significant outstanding recommendations	34-36
§5(a)(4)	Matters referred to prosecutorial authorities	21
§5(a)(5)	Information or assistance refused	i-ii
§5(a)(6)	List of audit, inspection, and evaluation reports	31
§5(a)(7)	Summary of particularly significant reports	1-6
§5(a)(8)	Audit reports with questioned costs	31
§5(a)(9)	Audit reports with funds that could be put to better use	31
§5(a)(10)	Summary of reports for which no management decision was made	6
§5(a)(11)	Significant revised management decisions	6
§5(a)(12)	Significant management decision disagreements	6
§5(a)(13)	Information described under 05(b) of FFMIA of 1996	N/A
§5(a)(14)	Results of peer review conducted of NSA OIG	27
§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	21-25
§5(a)(18)	Description of Metrics used in statistical tables of investigations	21-25
§5(a)(19)	Reports concerning investigations of Seniors	22-23
§5(a)(20)	Whistleblower Retaliation	22-23
§5(a)(21)	Agency interference with IG Independence	ii
§5(a)(22)	Disclosure to the public	23
§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	32-33

* 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 OIG conducts independent oversight that promotes the wise use of public resources; adherence to laws, rules, and regulations; and respect for Constitutional rights. Through audits, evaluations, inspections, and investigations, we detect and deter waste, fraud, abuse, and misconduct and promote the economy, the efficiency, and the effectiveness of Agency operations.

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 Intelligence Community (IC) activities. IO evaluations are conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation*.

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 IC entities to jointly inspect consolidated cryptologic facilities. Inspections and evaluations are conducted in accordance with the CIGIE *Quality Standards for Inspection and Evaluation*.

AUDITS

The Audits 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, the equity, the ethics, 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.

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