NATIONAL SECURITY AGENCY

OFFICE OF THE INSPECTOR GENERAL

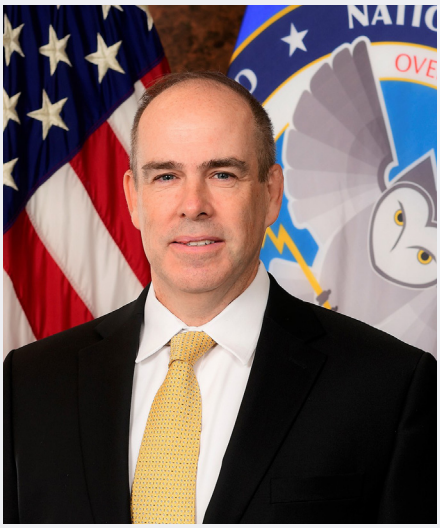
Semiannual Report to Congress

1 April to 30 September 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 audits, evaluations, inspections, and investigations, we detect and deter waste, fraud, abuse, and misconduct, and promote the economy, efficiency, and effectiveness of Agency operations.

NOTE: A classified version of the Semiannual Report (SAR) to Congress formed the basis of this unclassified version. The NSA/CSS OIG has endeavored to make this unclassified version of the SAR as complete and transparent as possible. However, where appropriate, the NSA/CSS OIG has rephrased or redacted information to avoid disclosure of classified information and as required to protect NSA sources and methods and to 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 Acting Inspector General



I am pleased to submit the Semiannual Report (SAR) for the National Security Agency (NSA) Office of the Inspector General (OIG) for the period ending 30 September 2022.

After the reporting period, the Honorable Robert P. Storch was confirmed as the Department of Defense Inspector General (IG). As NSA's first presidentially appointed and Senate-confirmed IG, his legacy will be remembered for years to come. The OIG is deeply indebted to Mr. Storch for his vision, leadership, and passion and wishes him the best in his new role.

As detailed in the pages that follow, the OIG completed a number of important oversight products during this report period from our Intelligence Oversight (IO)—the only such division in the IG community devoted solely to IO—, Inspections, and Audits Divisions, and our Investigations Division managed the Hotline and investigated allegations of fraud, waste, and abuse while also supporting the Department of Justice in criminal prosecutions.

Pursuant to the IG Act, I am pleased to report that the OIG experienced no attempts by the Agency to interfere with our independence and that the Agency fully cooperated with our work and did not refuse to provide or attempt to delay or restrict access to records or other information. Agency management agreed with all OIG recommendations that were made during the reporting period.

Additionally, in this reporting period, the OIG began exploring the potential under Office of Management and Budget memorandum M-22-04, *Promoting Accountability through Cooperation among Agencies and Inspectors General*, issued 3 December 2021, for the OIG to engage more proactively with the Agency to provide input regarding significant new NSA programs or those in which the Agency assumes significant new risks, without limiting our ability or independence in conducting subsequent oversight of such programs. We look forward to being able to provide additional benefits in this new area for engagement as part of the OIG's multi-faceted approach to conducting impactful, independent oversight that improves the integrity and efficiency of operations at this critically important Agency.

KEVIN B. GERRITY
Acting Inspector General

HIGHLIGHTS

Details

The following summaries highlight some of the OIG's audits, evaluations, inspections, and investigations that were issued during this reporting period, which are discussed further in this SAR. As the highlights illustrate, the OIG continues to conduct wide-ranging oversight of NSA programs and operations.

OIG-Wide (issued from 1 April through 30 September 2022)

13
Total Number of OIG Reports[1]

327
Total Number of Recommendations in OIG Reports[2]

19
Total Number of Observations

[1] This figure includes OIG evaluations, inspections, audits, and advisory memoranda issued during the reporting period. It does not include Investigations reports.

[2] This figure includes all recommendations, including those for Agency improvements and dollar-related recommendations, which are recommendations for components to remedy questioned costs and funds to be put to better use.

Intelligence Oversight Division

1
Advisory Memorandum

12
New Recommendations

Inspections Division

3
Field Inspection Reports

119
New Recommendations

11
New Observations

1
Joint Inspection Report

127
New Recommendations

8
New Observations

1
Evaluation Report

26
New Recommendations

1
Advisory Memorandum

4
New Recommendations

Audits Division

5
Audit and Evaluation Reports

39
New Recommendations

1
Attestation (Report)

Investigations Division

671
Processed Contacts from Classified Systems

22
New Investigations Opened

50
Investigations Closed

88
New Inquiries Opened

100
Inquiries Closed

54
Proposed Disciplinary Actions[3]

$708,206
Monetary Recoveries[4]

[3] This number represents employees who resigned or retired prior to proposed disciplinary action, resigned in lieu of removal, or had other disciplinary actions taken, including terminations, suspensions, and reprimands.

[4] This number includes proposed financial recoveries based on substantial fraud.

Contents

This page intentionally left blank.

Significant Problems, Abuses, and Deficiencies and Other Particularly Significant Reports

National Security Agency (NSA)/Central Security Service (CSS)—hereinafter referred to as NSA—Office of the Inspector General (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 NSA/CSS Implementation of the Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act (FISMA) of 2014 establishes an annual review of the effectiveness of agencies' security programs. OIG assessments are completed in accordance with Office of Management and Budget (OMB) guidance that establishes a maturity-model spectrum, ranging from Level 1, Ad Hoc, to Level 5, Optimized.

On 6 December 2021, OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, directing a change in the annual cycle of OIG FISMA assessments to align results of evaluations with the budget submission cycle.[1] In the newly directed three-year cycle, a total of 20 core metrics across the nine identified information technology (IT) security areas are to be assessed annually, and the remaining standards and controls are to be divided and evaluated in either the second or the third year of the cycle. On 13 April 2022, OMB issued *FY22 Core IG Metrics Implementation Analysis and Guidelines*, outlining the 20 core metrics for assessment in FY 2022. The figure below depicts the shift in the number of assessed metrics within the nine security areas from FY 2021 through FY 2022.

[1] Historically, OIG FISMA evaluations were completed in October, limiting agency ability to request resources in the next budget year submissions. This change is intended to reduce the time between issue identification and resource request and allocation.

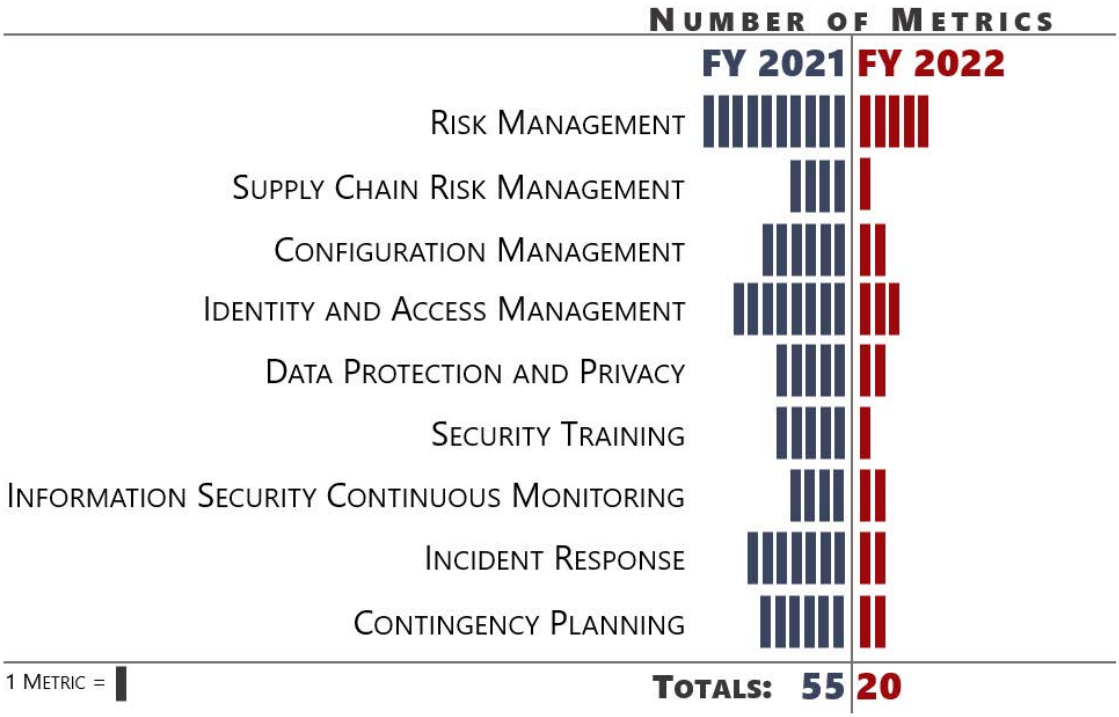


Figure 1: Number of Metrics Assessed in FY 2021 and FY 2022[2]

In FY 2022, because the number of metrics assessed in each security area decreased, each metric had a higher weight in determining the overall maturity level for a given security area. The OIG notes that this may have impacted NSA's overall score in some areas, though we are unable to definitively assess the impact of this change without evaluating the other metrics that were not included this year. Consequently, the overall FY 2022 assessment is not directly comparable to prior years' assessments.

Our evaluation found that NSA had defined policies, procedures, and strategies (Maturity Level 2) for six of nine IT security areas: Risk Management, Supply Chain Risk Management, Configuration Management, Security Training, Information Security Continuous Monitoring, and Contingency Planning. Additionally, NSA had consistently implemented policies, procedures, and strategies (Maturity Level 3) for the remaining three areas: Identity and Access Management, Data Protection and Privacy, and Incident Response. The figure below shows the overall maturity levels for security areas from FY 2020, FY 2021, and FY 2022.

[2] For FY 2021, the FISMA evaluation had 66 metrics, but the OIG evaluated 55 metrics. Two metrics were not applicable to the Agency, and nine were requests to provide additional information that was not otherwise included in the security areas.

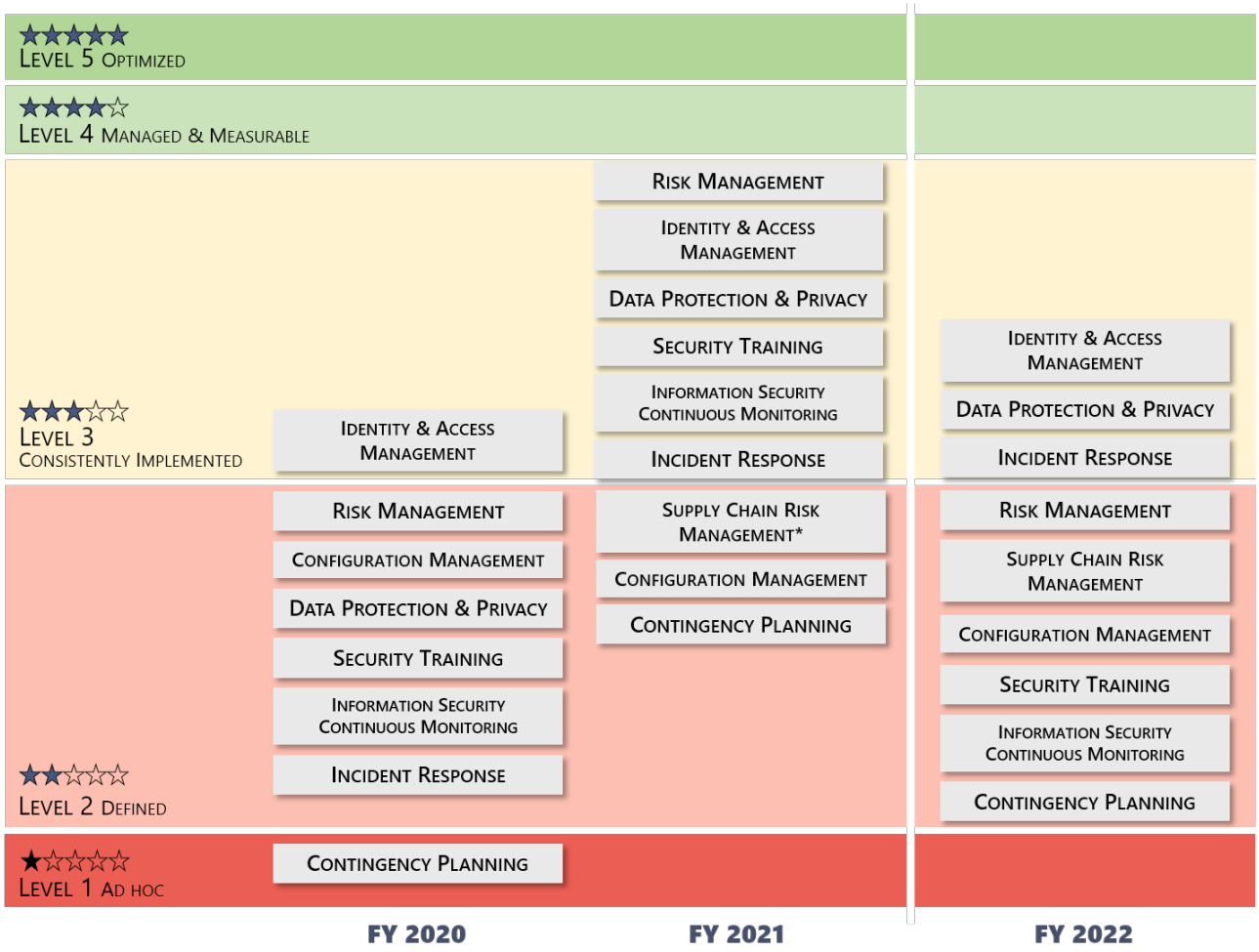


Figure 2: Overall Maturity Levels – Three-Year Overview

*Note: The OIG conducted an initial assessment of the Supply Chain Risk Management security area in FY 2021 to determine the baseline maturity level of the domain in anticipation of its inclusion in future assessments.

The OIG concluded that NSA had defined policies, procedures, and strategies for all FISMA IT security areas and consistently implemented them for three of the nine areas. We noted that NSA continued to make improvements in all IT security areas with additional control implementation, heightened leadership focus, and integration of information system security processes. However, as in past years, none of the security areas were assessed at Level 4, Managed and Measurable, or above, and we noted continued room for improvement in all nine areas. With fewer metrics selected, each was weighted higher than in previous years, which may have impacted the overall scores for these areas. However, we were unable to definitively assess the impact of this change without evaluating the other metrics that were not included this year.

Evaluation of NSA Mission Assurance/Continuity of Operations Program

The NSA OIG evaluated the efficiency and effectiveness of the NSA mission assurance/continuity of operations (MA/COOP) program from May through August 2021, and assessed whether it complied with NSA/CSS Policy 1-4, *NSA/CSS Mission Assurance*, issued 27 March 2014, and all the policies referenced therein. The OIG noted several areas for improvement including but not limited to the following:

- NSA MA/COOP-related policies and guidance are insufficient;
- The MA/COOP program lacks clearly defined roles and responsibilities; and
- The MA/COOP program does not establish training or exercise expectations.

The OIG made 26 recommendations and incorporated 2 recommendations from a prior audit report to assist the Agency in addressing the noted issues.

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.

Compliance With Federal Financial Management Improvement Act of 1996 (FFMIA)

NSA reported that it was not in substantial compliance with FFMIA. NSA's current target completion for remediation is 31 December 2027.

Intelligence Oversight

Oversight Work Completed in the Reporting Period

Advisory Memorandum for the Limited-Scope Evaluation of Mission Correlation Table Data

The OIG conducted this limited-scope evaluation on the effectiveness of controls over mission correlation table (MCT) data, which contains key information used to manage access to data. The OIG found the controls in place for assessing MCT assignments, locations, and segregation of duties in key roles need improvement. The OIG made 12 recommendations to assist the Agency in addressing these issues.

Ongoing Oversight Work

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 Foreign Intelligence Surveillance Act (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 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.

Evaluation of NSA's Controls Related to Certain Publicly Available Information Used for Mission

The objective of the evaluation is to review NSA's internal controls surrounding access to (including querying and auditing), and use, retention, and sharing of certain publicly available data to support foreign intelligence, counterintelligence, and cybersecurity missions, and to provide support to military operations. The evaluation will review adherence to law and policy and the protection of civil liberties and privacy.

INSPECTIONS

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

Evaluation of NSA Mission Assurance/Continuity of Operations Program

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

Inspection of NSA/CSS Representative and Cryptologic Services Group to NORAD and USNORTHCOM

The NSA OIG evaluated the overall climate and the compliance, effectiveness, and efficiency of the NSA/CSS Representative (NCR) to North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM) during a virtual inspection. The OIG interviewed members of the NCR NORAD and USNORTHCOM (N&NC) management and workforce regarding NCR N&NC's operations and functions. NCR leadership and personnel supported the OIG throughout this inspection. We identified several areas for improvement in the following areas:

- **Command topics:** Lack of consistent workforce knowledge of the existing NCR N&NC 2021 strategy, uncertainty regarding the right balance of resources to carry out the NCR's current mission, and a perception among some military assignees that they were not treated as well as the civilians at NCR N&NC.
- **Mission operations:** Incomplete mission documentation, inconsistent use of the Agency's corporate information request portal, not adhering to analytic integrity standards annual training requirements, potential concern about product reporting in support of law enforcement, and incomplete critical information training and evaluation program requirements.
- **Intelligence oversight (IO):** No primary IO lead, inconsistent knowledge of IO guidance sources, outdated and incomplete documentation, inadequate physical mitigations to protect sensitive signals intelligence (SIGINT) in one area, and inconsistent procedures for removing individuals from mission access.
- **Resource programs:** Noncompliant support agreement, lack of required hand receipts for property accountability program, lack of tracking recipients of coins, no designated records management officer, and incorrect supervisory/non-supervisory designations in NSA Human Resources Management System.

- **Information technology (IT) and systems:** Lack of effective document control when using print services, IT equipment space (ITES) racks that were not secured, and N&NC staff personnel functioning as unofficial ITES managers.
- **Safety, facilities, and emergency management:** Lack of recorded safety inspections, lack of emergency phones and refuge areas, lack of a continuity of operations or devolution plan, concerns over the personnel accountability process, and lack of emergency action and emergency destruction plans.
- **Security:** Insufficient program documentation, information security lapses, and lack of required annual operations security activities reports.
- **Training:** Less than 100 percent completion of some mandatory employee and management training, and nepotism and Duty to Act statement noncompliance.

The OIG made a total of 45 recommendations and 1 observation to assist NCR N&NC in addressing the findings identified during the inspection. In addition, the OIG noted one commendable practice regarding the development and use of a project-tracker tool in the area of Mission Operations to guide projects in concert with NSA and NCR N&NC goals. We believe that this tool may warrant replication elsewhere across the NSA enterprise. The OIG closed 35 recommendations on report publication.

Inspection of the NSA/CSS Representative (NCR) and Cryptologic Services Group to U.S. Special Operations Command (SOCOM)

The NSA OIG evaluated the overall climate and compliance, effectiveness, and efficiency of NCR SOCOM during a virtual inspection. The OIG interviewed members of the NCR SOCOM management and workforce with regard to NCR SOCOM's operations and functions in the areas listed below. NCR leadership and personnel supported the OIG throughout this inspection. We identified several areas for improvements in the following areas:

- **Command topics:** A lack of consistent workforce knowledge of the existing NCR SOCOM strategy and uncertainty regarding the right balance of resources to carry out the NCR's current mission.
- **Mission operations:** Incomplete mission documentation; no defined analytic integrity standards program; and lack of documentation supporting knowledge transfer for key NCR SOCOM mission positions.
- **IO:** The IO program needs improvement in light of challenges to sustainability based on key personnel departures, suboptimal program management and documentation, and knowledge gaps in IO operational integration.
- **Resource programs:** Outdated or nonexistent support agreements, no insight into money received from NSA's customers, lack of storage for and protection of vital records, and no on-site contracting officer's representative for the IT contractor.
- **IT and systems:** Inconsistent profile management and lack of data center security.
- **Safety, facilities, and emergency management:** Lack of safety, continuity of operations, and emergency management programs, and questionable personnel accountability procedures.

- **Security:** Insufficient security documentation, lax physical and information security procedures, and no antiterrorism force protection and operations security programs.
- **Training:** Less than 100 percent completion of mandatory and required management training, and difficulty obtaining funding for professional development for some civilian personnel.

The OIG made a total of 42 new recommendations, incorporated 1 additional recommendation carried forward from a previous OIG report, and included 2 observations to assist NCR SOCOM in addressing the findings identified during the inspection. In addition, the OIG noted one commendable training practice that we believe may warrant replication elsewhere across the NSA enterprise whereby adjunct faculty travel to Florida to teach personnel stationed at multiple NCRs across the region, providing needed training while saving money. The OIG closed 19 recommendations on report publication.

Joint Inspectors General Inspection of National Security Agency/Central Security Service Utah

The OIG interviewed members of the NSA Utah (NSA-U) management and workforce regarding NSA-U operations and functions. NSA-U leadership and personnel fully supported the OIG throughout this inspection. We identified several areas for improvement in the following areas:

- **Command topics:** A lack of consistent workforce knowledge of the existing NSA-U strategy and uncertainty across the workforce regarding the right balance of resources to carry out NSA-U current and future endeavors.
- **Mission operations:** The OIG found incomplete and outdated mission documentation, inconsistent adherence to the analytic integrity and standards program, incomplete critical information training and evaluation requirements, and a lack of knowledge transfer processes.
- **IO:** A need for improvement in the areas of program documentation, operational integration, and training.
- **Resource programs:** The OIG identified concerns related to NSA-U's personnel programs, support agreements, and property accountability program.
- **IT and systems:** The OIG identified concerns in information system security, infrastructure, and configuration management.
- **Safety, facilities, and emergency management:** The OIG identified concerns in areas related to safety, accountability, and emergency management.
- **Security:** The OIG found issues in areas related to security.
- **Training:** Less than 100 percent completion of mandatory and required training.

The OIG made a total of 127 new recommendations, incorporated 1 recommendation from an OIG audit report that addressed issues also identified at NSA-U, and made 8 observations to assist NSA-U in addressing the findings identified during the inspection.

Inspection of Special United States Liaison Office Ottawa (SUSLOO)

The OIG interviewed SUSLOO management and its workforce about SUSLOO operations and functions that are listed below. SUSLOO leadership and personnel fully supported the OIG throughout this inspection.

Overall, the OIG found that the SUSLOO workforce expressed positive views about their work and current leaders; however, we identified several areas for improvement in the following areas:

- **Mission operations:** Inaccurate mission ownership documentation and a lack of current documentation supporting knowledge transfer across SUSLOO mission areas.
- **IO:** Inadequate IO program resources and support, and outdated and incomplete IO documentation.
- **Resource programs:** Inconsistent compliance with NSA Talent, Evaluation and Advancement and personnel programs, and no designated records management officer or assigned point of contact for essential records.
- **IT and systems:** Lack of spare tokens for multi-factor authentication for computer access.
- **Safety, facilities, and emergency management:** The OIG identified issues in areas related to safety, facilities, continuity of operations, and personnel accountability.
- **Security:** The OIG found issues in a limited number of security areas.
- **Training:** Less than 100 percent completion of some mandatory employee and management training, and acknowledgement of nepotism and Duty to Act.

The OIG made a total of 32 recommendations and 8 observations to assist SUSLOO in addressing the findings identified during the inspection. In addition, the OIG noted one commendable related to a practice that we believe may warrant replication elsewhere across the NSA enterprise.

Cloud Printing and Secure Printing – Advisory Memorandum

During field and joint inspections, the OIG observed that many NSA personnel do not use cloud printing (i.e., PrintIT) or secure printing (e.g., print-and-hold) services. Specifically, the OIG observed that effective document control procedures were not consistently practiced for shared printers in common areas and made recommendations to address this problem in three inspection reports. Centralized printers pose a challenge to information security, in part because they are frequently located in places where personnel may not be able to maintain line-of-sight to the printer. This can result in a lack of control over sensitive and classified information and/or personally identifiable information.

The OIG made four recommendations to help the Agency address the issues identified.

Ongoing Inspection Work

The OIG continues work on reports for inspections that evaluated the overall climate, compliance, effectiveness, and efficiency of the following organizations:

- Joint Inspection of NSA/CSS Texas,
- Joint Inspection of a Joint Facility,
- Joint Inspection of ADF-C and NSA/CSS Colorado, and
- Inspection of Special United States Liaison Office Canberra.

AUDITS

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

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.

Evaluation of NSA Large-Scale Monitor Purchase

In 2021, the NSA Directorate of Operations (DO) made two purchases totaling approximately $3.8 million for 3,500 large-screen computer monitors in an initiative to boost data analysis and reporting by enabling DO analysts to view more data simultaneously across larger screens. Because the larger monitor models were not included on the Agency's standard IT baseline, DO used the NSA/CSS Enterprise Solution Baseline Exception Request (NES-BER) process to procure the monitors. The NSA Chief Information Officer/Director of Capabilities (CAP) reported to DIRNSA and others in Agency leadership, as well as to the OIG, the concern that the NES-BER process, intended for small lab purchases, had been used inappropriately in an effort to bypass other Agency processes. The overall objective of this evaluation by the OIG was to determine whether DO's large-scale monitor purchases in FY 2021 inappropriately used the NES-BER procurement process, resulting in waste of government resources.

The OIG's evaluation revealed that the Agency's IT procurement processes, including the NES-BER process, and internal controls were insufficient to effectively manage large-scale IT purchases. In addition, these monitors were too large for the dimensions and design of standard NSA workspaces. Further, when CAP requested the monitor locations from DO, it learned that DO did not adequately track the location of the monitors as they were delivered and installed, and DO was unable to fully account for each monitor purchased at that time. After our fieldwork, the Agency reported spending approximately $3.1 million in remediation costs for the monitors. The final remediation cost total was undetermined as of the time of our evaluation.

The findings identified by the OIG in this evaluation indicate that the Agency used IT procurement processes with control deficiencies and had insufficient oversight to purchase 3,500 monitors, leading to numerous challenges. The OIG made 12 recommendations to assist the Agency in addressing these issues.

Evaluation of FY 2021 Application of Classification Markers, Compliance With Declassification Procedures, and the Effectiveness of Declassification Review Processes

The NSA OIG conducted an evaluation of NSA's application of classification markers and compliance with declassification procedures, and the effectiveness of its declassification review processes. This review is the second of three annual congressionally directed actions. We found that:

- Agency classification authority blocks on finished reports were not compliant with Executive Order 13526, *Classified National Security Information*, issued 5 January 2010; NSA/CSS Policy Manual 1-52, *NSA/CSS Classification Guide*, issued 10 January 2018; or other Intelligence Community (IC) and Department of Defense (DoD) requirements.
- NSA did not complete all Mandatory Declassification Review requests within the timeframe established by 32 Code of Federal Regulations (CFR) Parts 2001 and 2003, *Classified National Security Information*, issued 28 June 2010.

These are repeat findings from the previous *Evaluation of NSA's FY 2020 Application of Classification Markers, Compliance With Declassification Procedures, and the Effectiveness of Declassification Review Process*, issued in September 2021. As of the issuance of the current report, 7 of the 13 recommendations issued in the previous report have been closed by the OIG based on Agency action sufficient to meet the intent of the recommendations.

FY 2022 Statement of Standards for Attestation Engagement 18, NSA's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Controls

We contracted with an independent public accounting firm to perform an examination of NSA's description of its system supporting the performance of financial processing services on behalf of another USG organization from 1 October 2021 through 30 June 2022, and of the suitability of design and operating effectiveness of controls to achieve the related control objectives stated in the description. The examination noted that NSA's description fairly presented the system that was designed and implemented and that controls were suitably designed and operated effectively to provide reasonable assurance that the control objectives were achieved.

Audit of NSA's Fiscal Year 2021 Compliance with the Payment Integrity Information Act of 2019

The OIG *Audit of NSA's Fiscal Year 2021 Compliance with the Payment Integrity Information Act of 2019* (PIIA) determined that NSA was in compliance with PIIA. Using the procedures outlined in OMB Circular A-123, Appendix C, "Requirements for Payment Integrity Improvement," issued 5 March 2021, the OIG found that the Agency complied with all 10 statutorily required improper payment reporting requirements for the fiscal year that ended on 30 September 2021.

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 (CRP)

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 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 generally accepted accounting principles. The audit will consider and report on internal control over financial reporting and compliance with certain laws, regulations, and other matters.

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 SCRM controls.

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 the proper use of such funding and the accurate reporting of the status of such activities to the foreign trading partners.

Audit of the Agency's Talent Identification and Acquisition Processes

The overall objective of this audit is to assess whether NSA's talent identification and acquisition processes from recruitment to issuance of a conditional job offer are effective and efficient in positioning the Agency to achieve its goal of hiring an expert and diverse workforce with the skills it needs now and in the future.

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 United States Code (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 activities such as false statements, contractors submitting false labor charges, and ethics violations. The OIG anticipates at this time that these cases are likely to be handled administratively.

The Investigations Division referred 25 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 54 employees based on OIG reports: 3 employees were removed, 14 employees retired or resigned in lieu of removal, 4 employees received a suspension of 30 days or more, 12 employees received a suspension of fewer than 30 days, 19 employees received written reprimands or counseling, 1 employee was issued a "last chance agreement," and 1 employee was removed due to prior performance failures. A total of nine cases referred by the OIG to ER were pending action at the end of the reporting period.

OIG Referrals to ER From 1 April – 30 September 2022	Employment Actions Reported to the OIG From 1 April – 30 September 2022	OIG Referrals Pending ER Action as of 30 September 2022
25	54	9

OIG Hotline Activity

The Investigations Division fielded 671 contacts through the internal OIG hotline. The OIG received 4,443 submissions on the external OIG hotline.

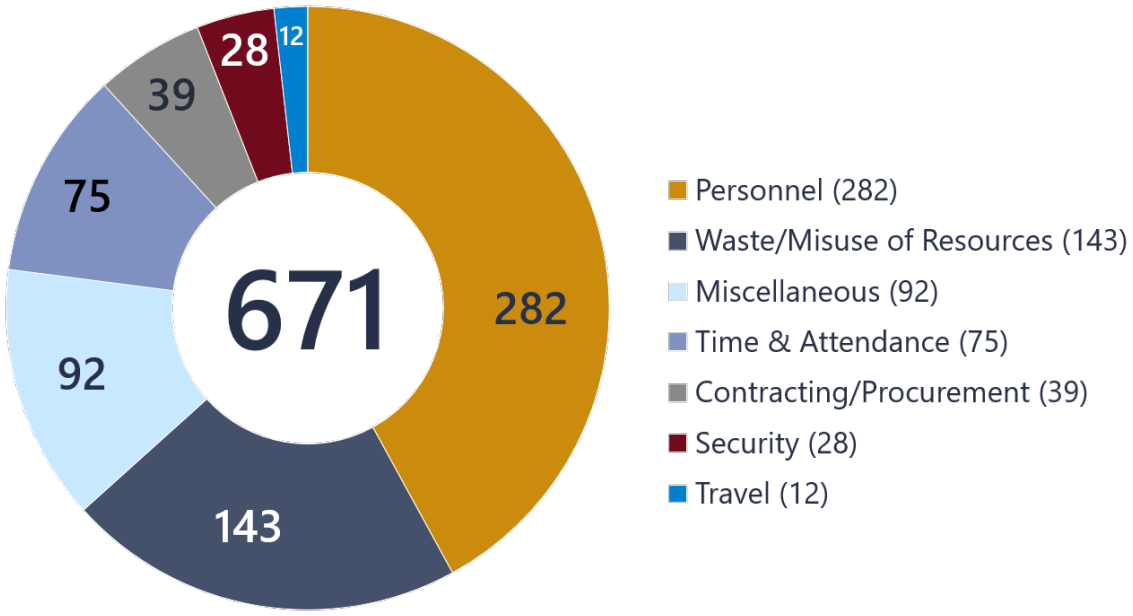


Figure 3: OIG Hotline - Contacts Opened

During this reporting period, the OIG enhanced our engagement across the enterprise by opening our first Investigations office outside of NSA Washington. We chose to open this office at NSA Hawaii in order to enable the OIG to significantly expand the time that our Hotline is actively staffed and our personnel are available to speak with Agency affiliates across the enterprise, as well as to provide a jumping-off point for our personnel at other sites in the region.

Significant Investigations

Former Senior Executive: Personal Services Contract, Preferential Treatment

An OIG investigation determined that a former Agency Senior Executive created the perception of a personal services contract by using an Agency contractor as an Executive Assistant. Further, they did not perform their duties impartially and gave preferential treatment. (Federal Acquisition Regulation 37.104; 5 CFR § 2635; NSA/CSS Personnel Management Manual [PMM], Chapter 366, §1-3; and DoD Joint Ethics Regulation [JER] 5500.7-R).

Based on the subject's status as a former Senior Executive, the investigative findings were forwarded to the DoD OIG. The findings were also forwarded to ER, the Office of Personnel Security, the Business Management and Acquisition (BM&A) Directorate, and the subject's supervisor.

The case did not meet the requirements for reporting to DOJ.

Former Senior Executive and Two GG-15s: Whistleblower Reprisal

An OIG investigation determined that three Agency supervisors did not reprise against Agency employees 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).

The investigative findings were forwarded to DoD OIG.

The cases did not meet the requirements for reporting to DOJ.

GG15: False and Inaccurate Timesheets

An OIG investigation determined that an Agency employee submitted false and inaccurate timesheets totaling 48.5 hours, resulting in a loss of approximately $4,039 to the government (NSA/CSS PMM Chapters 360 and 366).

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor. The Agency issued the subject a Letter of Reprimand on 11 July 2022.

The case was reported to DOJ on 1 June 2022 and declined on 15 June 2022.

GG15: Inappropriate Physical Contact, Preferential Treatment, Misuse of NSA/CSS Information System (IS), and Lack of Candor

An OIG investigation determined that an Agency employee engaged in inappropriate physical contact with another employee, created the appearance of preferential treatment of an employee, misused NSA/CSS IS, and lacked candor and failed to give the OIG full and complete cooperation during the investigation (DoD JER 5500.7-R; 5 CFR 2635; NSA/CSS PMM, Chapter 366; and NSA/CSS Policies 6-8 and 1-60).

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor. Agency disciplinary action, if any, is pending.

The case was reported to DOJ on 27 July 2022 and declined on 10 August 2022.

GG15: Failure to Exercise Courtesy and Respect, Inappropriate Physical Contact, Preferential Treatment, Misuse of NSA/CSS IS, Attempt to Influence an OIG Investigation, and Lack of Candor

An OIG investigation determined that an Agency employee failed to exercise courtesy and respect in their interactions with fellow workers, engaged in inappropriate physical contact, afforded preferential treatment to two subordinate employees, misused NSA/CSS IS in a manner that served no legitimate public interest, attempted to impede and influence an OIG investigation, and knowingly provided a false sworn statement to the OIG (NSA/CSS PMM, Chapter 366; DoD JER 5500.7-R; 5 CFR § 2635; and NSA/CSS Policies 6-8 and 1-60).

The investigative findings were forwarded to ER, the Office of Personnel Security, and the subject's supervisor. Agency disciplinary action, if any, is pending.

The case was reported to DOJ on 14 January 2022 and declined on 1 February 2022.

GG15: Procurement Integrity Act Violations

An OIG investigation determined that an Agency employee disclosed contractor bid or proposal/source selection information along with unclassified sensitive information to a contractor, failed to perform their duties impartially, and gave preferential treatment to a contractor and company (41 U.S.C. § 2102; 5 CFR § 2635.703; NSA/CSS PMM, Chapter 366; 18 U.S.C. § 1905; and DoD JER 5500.7-R).

The investigative findings were forwarded to ER, the Office of Personnel Security, BM&A, and the subject's supervisor. Agency disciplinary action, if any, is pending.

The case was reported to DOJ on 2 December 2021 and declined on 16 December 2021.

GG15: Government Travel Credit Card (GTCC) Misuse

An OIG investigation determined that an Agency employee did not misuse their GTCC for unofficial purposes (DoD Instruction [DoDI] 5154.31, NSA/CSS Corporate TravelGram Issue 01-2008, and Statement of Understanding/Cardholder agreement).

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 April through 30 September 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 $708,206 based on substantiated fraud, and the Agency reported total actual recoveries of approximately $39,219 from current and prior referrals.

Summary of Additional Investigations

The OIG opened 22 investigations and 88 inquiries while closing 50 investigations and 100 inquiries during the reporting period. The new investigations are related to various allegations including acquisition fraud, violations of standards of conduct, waste/misuse of resources, computer misuse, hostile work environment, harassment, contractor labor mischarging, time and attendance fraud, and reprisal.

False and Inaccurate Timesheets

Two OIG investigations and 10 inquiries determined that Agency employees submitted false and inaccurate timesheets resulting in a loss of approximately $30,400 to the Government (NSA/CSS PMM, Chapters 360 and 366).

Contractor Labor Mischarging

Five OIG investigations and five inquiries determined that Agency contractor employees submitted false and inaccurate invoices against Agency contracts, resulting in a loss of approximately $677,806 to the Government (31 U.S.C. § 3802).

Misuse of NSA/CSS IS

An OIG investigation determined that two Agency employees misused NSA/CSS IS for personal use, using Agency assets for private gain. In doing so they misused their position, creating at least an appearance of use of public office for private gain, and they misused non-public information to further their own private interest (5 CFR § 2635 and NSA/CSS Policy 6-80).

Two OIG investigations and two inquiries determined that Agency contractors misused NSA/CSS IS for activities that were not work related (NSA/CSS Policies 6-4 and 6-8).

GTCC Misuse

Two OIG investigations determined that two Agency employees knowingly misused their GTCCs by using the cards to take cash advances to engage in gambling and by failing to pay the monthly GTCC debt in full on numerous occasions (Government Travel Card Regulation and NSA/CSS Corporate TravelGram Issue 01-2008). One investigation determined an Agency employee did not misuse their GTCC for unofficial purposes.

Harassment

An OIG investigation determined that an Agency employee sexually harassed others by creating a work environment perceived by the recipients of the behavior as pervasive and offensive, failed to exercise courtesy and respect with interactions with fellow workers, and misused NSA/CSS IS (NSA/CSS PMM, Chapter 366; NSA/CSS Policy 6-8; and DoD JER 5500.7-R).

Investigations Summary

Total Number of Investigative Reports Issued	50
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 the NSA OIG Electronic Information Data Management System.

Investigations Opened

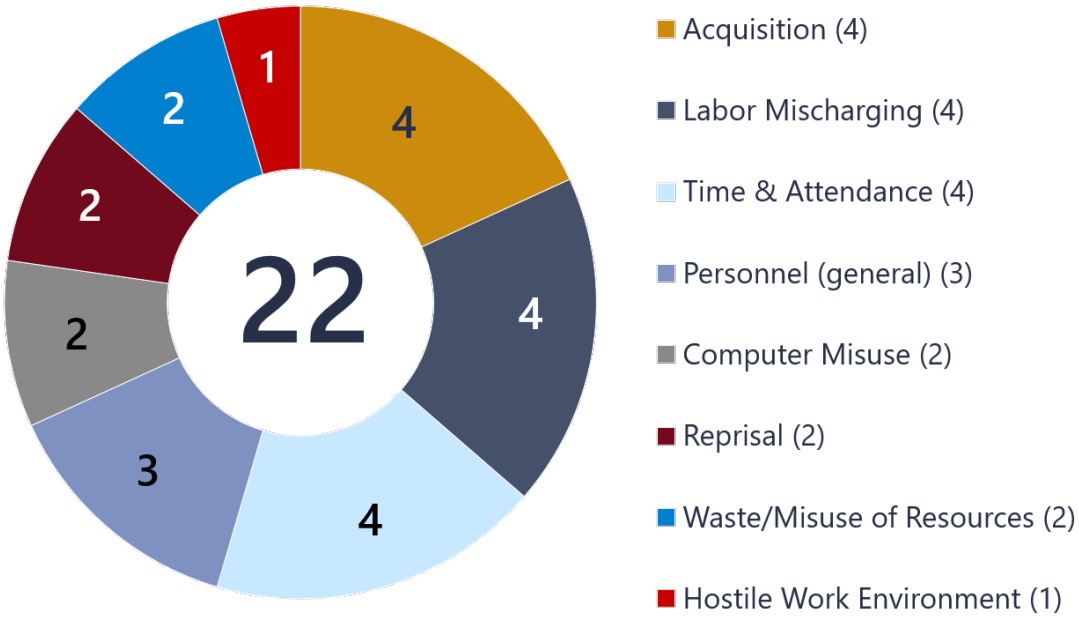


Figure 4: OIG Investigations Opened

Top Management and Performance Challenges

In accordance with the Reports Consolidation Act of 2000, the NSA IG annually submits to Congress what the IG believes are the top management and performance challenges (TMPC) facing NSA. As required by the Act, the TMPC is included in NSA's *Agency Financial Report* (AFR). The OIG has continued its efforts to enhance and refine the TMPC document to have greater impact and to assist in identifying areas for future OIG oversight work. This has been accomplished through the extensive 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 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 TMPC topics that will be included in NSA's *FY 2022 AFR*, which will be submitted to Congress in November 2022:


Recruiting and Sustaining a Diverse, Equitable, and Inclusive Expert Workforce;


NSA's Intelligence Mission in an Era of Strategic Competition;


Addressing Strategic Competition in the Cybersecurity Mission;


Enhancing Financial and Physical Resource Management;


Protecting the Agency from Insider Threats and Promoting Integrity Across the Agency; and


Posturing for Success in the Wake of Natural and Man-Made Events.

Peer Review

Peer Reviews Conducted by Other OIGs

No peer reviews of the NSA OIG were completed during this reporting period. The last peer review conducted was an IC OIGs (National Reconnaissance Office, Defense Intelligence Agency and IC)-led review of the NSA OIG Audits Division that covered the three-year period ending 31 March 2021. There are no outstanding recommendations from that peer review.

Peer Reviews Conducted by NSA OIG

The NSA OIG did not complete a final peer review during this 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 went through the important process of developing the first *DEC Strategic Plan*, covering FY 2023 through FY 2026, to advance DEIA initiatives in the OIG. Based on the *Strategic Plan*, the DEC developed tasks for a *Plan of Action and Milestones*, with quarterly status reporting to OIG senior leadership. We continue to be an active participant in the IG community-wide Council of the Inspectors General on Integrity and Efficiency (CIGIE) DEIA Work Group, partnering with other OIGs from across the oversight community to share best practices and learning in this critically important area.

Whistleblower Coordinator Program

The OIG has continued to make whistleblower protection a priority. Our guiding principles are clear: 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 from the front lines 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 of 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. As referenced in the "Investigations" section of this SAR, the OIG opened its first branch Investigations office during this reporting period, expanding the availability of our personnel to respond to Hotline complaints and speak with affiliates across the NSA enterprise.

Given the importance of whistleblowers to the Agency and the OIG, we have taken steps to help ensure that Agency employees and others are fully informed about whistleblower rights and protections. To that end, the OIG has worked with the Agency to develop and refine an online whistleblower training, which continues to be mandatory for all NSA employees. The OIG's Whistleblower Coordinator continues to serve as a resource through 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 for both employees and contractors.

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

Intelligence Oversight

Advisory Memorandum for the Limited-Scope Evaluation of Mission Correlation Table Data

Inspections

Evaluation of NSA Mission Assurance/Continuity of Operations Program

Inspection of NORAD/NORTHCOM

Inspection of NCR SOCOM

Joint Inspectors General Inspection of National Security Agency/Central Security Service Utah

Inspection of Special United States Liaison Office Ottawa

Advisory Memorandum

Cloud Printing and Secure Printing – Advisory Memorandum

Audits

Mission and Mission Support Branch

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

Cybersecurity and Technology Branch

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

Evaluation of NSA Large-Scale Monitor Purchase

Financial Audits Branch

Audit of NSA's Fiscal Year 2021 Compliance with the Payment Integrity Information Act of 2019

FY 2022 Statement of Standards for Attestation Engagement 18, NSA's Description of its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of its Controls

Appendix B: Audit Reports With Questioned Costs and Funds That Could Be Put to Better Use[3]

Audit Reports With Questioned Costs

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	$ 20,700,000	$ 16,400,000
Issued during reporting period	0	$ 0	$ 0
For which management decision was made during reporting period:			
Costs disallowed	0	$ 0	$ 0
Costs not disallowed	1	$ 3,200,000	$ 0
For which no management decision was made by end of reporting period	2	$ 17,500,000	$ 16,400,000

Audit Reports With Funds That Could Be Put to Better Use

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:		
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

[3] Because OIG recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations is often not readily quantifiable.

Appendix C: Recommendations Overview

Recommendations Summary

The OIG made 327 recommendations to NSA management in reports and oversight memoranda issued during this reporting period. The Agency closed 137 of the newly published recommendations and a total of 445 recommendations during the reporting period.

The OIG published 13 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	32	42	22	96
Outstanding Recommendations	104	351	106	561

Outstanding Recommendations Breakdown

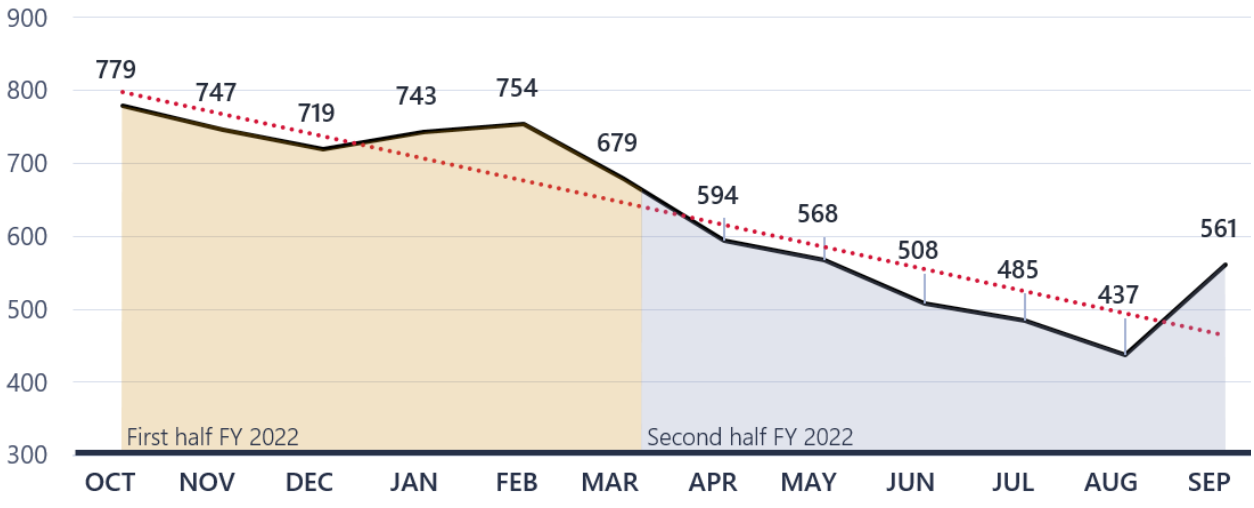


Figure 5: Number of Open Recommendations - October 2021 to September 2022

Days Open Groupings	Intelligence Oversight	Inspections	Audits	Total
Under 1 Year	31	172	26	229
1 – 5 Years	57	168	77	302
Over 5 Years	16	11	3	30
Totals	104	351	106	561

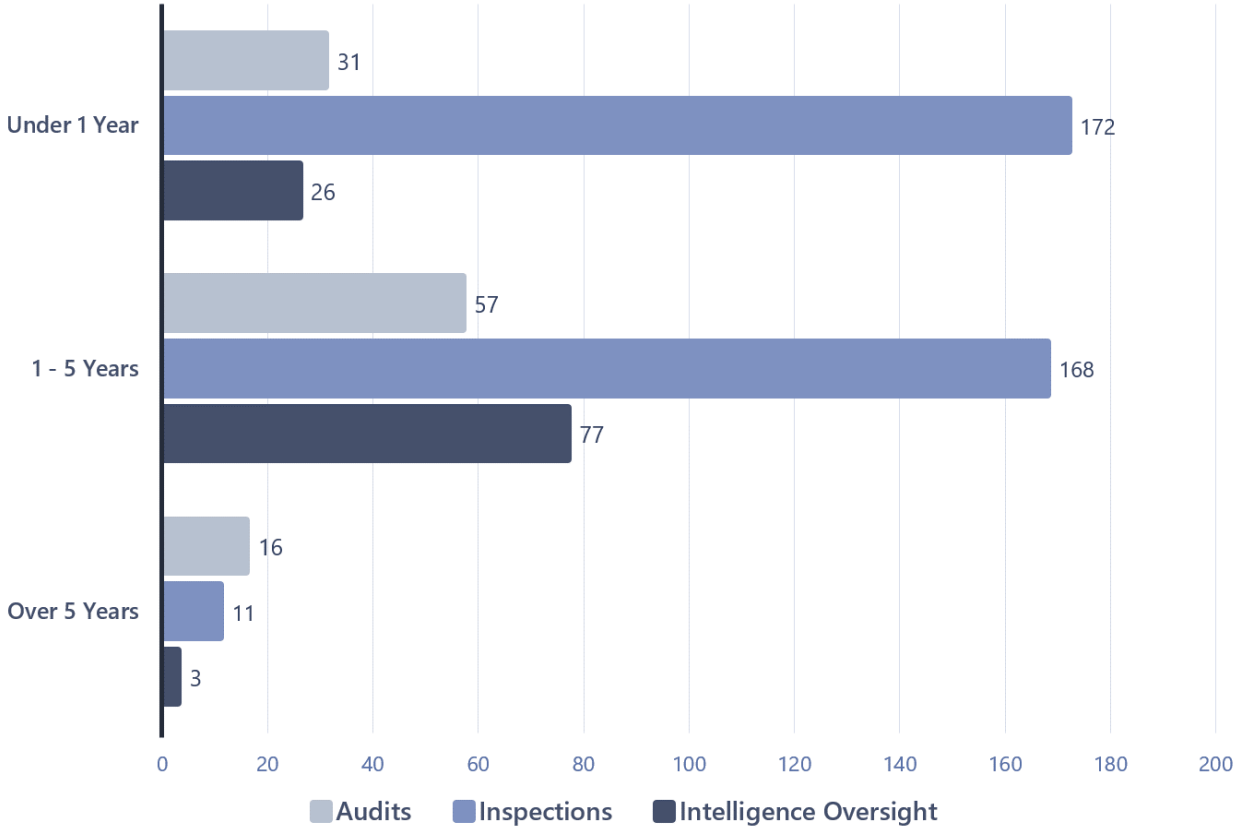


Figure 6: Outstanding Recommendations by Days Open and Source – As of 30 September 2022

Management Policy Referrals

In addition to the recommendations arising from audits, inspections, evaluations, and other oversight products detailed above, the OIG has issued 15 referrals involving policy issues to Agency management since August 2018, including one issued during this reporting period. Fourteen of the prior referrals and the one from this reporting period were closed based on Agency action prior to the end of the reporting period.

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.

On 26 April 2022, NSA and its partner signed a memorandum of agreement which establishes an overarching framework for SIGINT data compliance that emphasizes a risk-managed approach, characterized by what is described as transparent and trusting teamwork. This framework is intended to help resolve outstanding issues associated with the use, handling, and transfer of SIGINT data

identified in the joint OIG report, while also setting the conditions for improved mission responsiveness and efficiency going forward. NSA and its partner have indicated the policy updates and escalation procedures are expected to be completed by 30 June 2023.

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 "Significant Problems, Abuses, and Deficiencies and Other Particularly Significant Reports" section of this report, evaluated the effectiveness and efficiency of this program and determined whether it met all of the requirements of pertinent policies and regulations, and included a number of recommendations for improvement in this critical area.

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.

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.

The OIG issued its most recent report on the *Assessment of NSA's Personnel Accountability Program* in December 2021. The Agency did complete the new recommendation issued with that report during this reporting period; however, it still has not issued formal guidance and procedures—as previously recommended to account for all personnel—which could impact the ability to achieve prompt continuation of operations following an incident or in a similar situation in the future.

The ability of the Agency to account for affiliated personnel remains critical following a natural or man-made disaster, including events like the COVID-19 global pandemic, as highlighted in the "Top Management and Performance Challenges" section in this SAR.

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 NES/BER 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. The OIG is reviewing and testing the actions taken.

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 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

ADF-C	Aerospace Data Facility – Colorado
AFR	Agency Financial Report
BM&A	Business Management & Acquisition
CAP	Capabilities Directorate
CFR	Code of Federal Regulations
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSS	Central Security Service
DEC	Diversity and Engagement Committee
DEIA	Diversity, equity, inclusion, and accessibility
DHS	Department of Homeland Security
DIRNSA	Director, NSA
DO	Directorate of Operations
DoD	Department of Defense
DoDI	Department of Defense Instruction
DOJ	Department of Justice
ER	Employee Relations
FFMIA	Federal Financial Management Improvement Act of 1996
FISA	Foreign Intelligence Surveillance Act
FISMA	Federal Information Security Modernization Act
GTCC	Government travel credit card
IC	Intelligence Community
ICT	Information and communication technology
IG	Inspector General
IO	Intelligence oversight
IS	Information system
IT	Information technology
ITES	IT equipment space
JER	Joint Ethics Regulation
MA/COOP	Mission assurance/continuity of operations
MCT	Mission correlation table
N&NC	NORAD and USNORTHCOM
NCR	NSA/CSS Representative
NDAA	National Defense Authorization Act for Fiscal Year 2020

NES-BER	NSA/CSS Enterprise Solution Baseline Exception Request
NORAD	North American Aerospace Defense Command
NSA	National Security Agency
NSA-U	NSA Utah
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act
PMM	Personnel Management Manual
RF	Radio Frequency
RM	Removable media
SAR	Semiannual Report
SCRM	Supply Chain Risk Management
SIGINT	Signals intelligence
SOCOM	U.S. Special Operations Command
SUSLOO	Special United States Liaison Office Ottawa
TMPC	Top management and performance challenges
U.S.C.	United States Code
USG	U.S. Government
USNORTHCOM	U.S. Northern Command

Appendix E: Index of Reporting Requirements*

IG Act Reference	Reporting Requirements	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	1-4
§5(a)(2)	Recommendations for corrective action	1-4
§5(a)(3)	Significant outstanding recommendations	28-32
§5(a)(4)	Matters referred to prosecutorial authorities	16
§5(a)(5)	Information or assistance refused	i
§5(a)(6)	List of audit, inspection, and evaluation reports	26
§5(a)(7)	Summary of particularly significant reports	1-4
§5(a)(8)	Audit reports with questioned costs	27
§5(a)(9)	Audit reports with funds that could be put to better use	27
§5(a)(10)	Summary of reports for which no management decision was made	4
§5(a)(11)	Significant revised management decisions	4
§5(a)(12)	Significant management decision disagreements	4
§5(a)(13)	Information described under 05(b) of FFMIA of 1996	4
§5(a)(14)	Results of peer review conducted of NSA OIG	23
§5(a)(15)	List of outstanding recommendations from peer review of NSA OIG	23
§5(a)(16)	List of peer reviews and outstanding recommendations conducted by NSA OIG	23
§5(a)(17)	Statistical tables of investigations	16-21
§5(a)(18)	Description of Metrics used in statistical tables of investigations	16-21
§5(a)(19)	Reports concerning investigations of Seniors	17-19
§5(a)(20)	Whistleblower Retaliation	18
§5(a)(21)	Agency interference with IG Independence	i
§5(a)(22)	Disclosure to the public	5; 7-15; 17-19; 26
§5(a)(note)	Final completed contract audit reports	N/A
§5(a)(note)	Outstanding recommendations past 12 months	28-29

* Citations are to the IG Act of 1978, as amended

This page intentionally left blank.

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; are in compliance with federal law, executive orders and directives, and IC, DoD, and NSA policies; and appropriately protect civil liberties and individual privacy. The IO function is grounded in Executive Order 12333, which establishes broad principles for IC activities. IO evaluations are conducted in accordance with the 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, including 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 branches: Cybersecurity and Technology, Financial Audits, and Mission and Mission Support. The Division's audits and evaluations examine the economy, the efficiency, and the effectiveness of NSA programs and operations; assess Agency compliance with laws, policies, and regulations; review the operation of internal information technology and controls; and determine whether the Agency's financial statements and other fiscal reports 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. Investigations are based on submissions made through the classified and unclassified OIG Hotlines; 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

www.oig.nsa.gov