NATIONAL SECURITY AGENCY

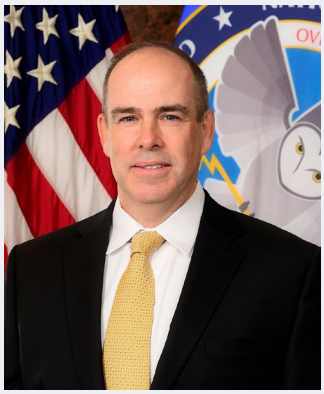
OFFICE OF THE INSPECTOR GENERAL

Semiannual Report to Congress

1 April 2023 to 30 September 2023

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 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.

Message from the Deputy Inspector General



I am pleased to submit the Semiannual Report (SAR) for the National Security Agency (NSA)/Central Security Service (CSS) Office of the Inspector General (OIG) for the period ending 30 September 2023.

The NSA OIG team of extraordinary professionals and subject matter experts performs independent oversight with the goal of producing actionable reports that address the top challenges facing the Agency. As demonstrated in this SAR, our team's oversight touches on multiple areas:

- The Intelligence Oversight Division provides an independent check on critical Agency functions;
- The Inspections Division conducts boots-on-the-ground reviews of the implementation of policies and procedures on multiple topics;
- The Audits Division addresses a wide breadth of areas throughout the Agency—cybersecurity and technology, financial audits, procurement, and mission and mission support;
- The Investigations Division operates our critical Hotline, ensuring whistleblowers have an independent team to whom they can raise any concerns, and investigates criminal matters with our law enforcement partners as well as administrative matters involving employee misconduct, with an emphasis on allegations of whistleblower reprisal.

The incredible work of the team during this reporting period included reports with numerous substantive recommendations to help the Agency perform more efficiently and effectively. The Agency agreed with all the recommendations we issued this period.

The team also focused on outreach to the Agency enterprise wide, with a particular emphasis on whistleblowers. We hosted an Agency event for Whistleblower Appreciation Day and highlighted how a tip to our Hotline led to a recent federal conviction for fraud. The entire OIG team ensures people have a safe place to raise concerns and that we will independently assess their concerns.

It is an honor to be a part of this dedicated team of professionals, and I look forward to reporting the positive impacts of their work.

KEVIN B. GERRITY
Deputy Inspector General

HIGHLIGHTS

REPORTS

6 Audit

3 Evaluation

2 Inspection

304 Total Open Recommendations

INVESTIGATIONS

0
Number of Convictions Resulting From Investigations

6
Investigations Involving Senior Employees

4
Investigations Involving Whistleblower Retaliation

796
Contacts Processed

35
New Investigations Opened

27
Investigations Closed

158
New Inquiries Opened

149
Inquiries Closed

37
Disciplinary Actions

$234,959 (Actual)

$298,383 (Proposed)

Monetary Recoveries

Contents

Information Related to Interference by NSA

The National Security Agency (NSA)/Central Security Service (CSS)—hereinafter referred to as NSA—Office of the Inspector General (OIG) experienced no attempts by NSA to interfere with our independence. The Agency fully cooperated with our work; did not refuse to provide or attempt to delay or restrict access to records or other information; and did not constrain our budget to limit the capabilities of the office.

Audit, Inspection, and Evaluation Reports Issued

Audit Reports

Audit of NSA's Information and Communications Technology Supply Chain Risk Management Controls for Selected Contracts

The overall audit objective was to determine if NSA securely procures information and communications technology equipment for selected contracts and how the Agency mitigates any potential compromises via supply chain controls. Additionally, we assessed if identified supply chain risk management (SCRM) controls were established in accordance with NSA policies, Department of Defense (DoD) directives, DoD instructions, U.S. Intelligence Community guidance, and other applicable criteria. The OIG examined the Agency's SCRM processes for selected contracts, conducted interviews, and evaluated relevant policies and other related documentation.

Audit of the Greenway Program

The OIG performed this audit to determine if the Greenway Program, which provides IT services, was organized and managed economically, efficiently, effectively, and in accordance with applicable policies and requirements. The OIG found the following challenges were caused in part from a lack of detailed specifications in the contracts:

- Performance-based specifications and standard operating procedures for the program were not finalized in a timely manner.
- The Agency had an insufficient program Quality Assurance Surveillance Plan that was not being followed.
- Outsourcing program contractor performance assessments created numerous oversight issues.
- The Agency has not adequately addressed numerous issues with the program's handling of user help desk tickets.
- The pace of the Agency's contract succession planning and decision-making has been inadequate.
- Agency incentives were not effective enough in motivating one of the contractors to provide quality performance.
- Not all performance sites with dedicated contractor support had appointed site contracting officer's representatives.

- The Agency self-reported a potential Antideficiency Act violation of the time statute that warrants further review.

The findings identified by the OIG in this audit reflect that the Agency may not be receiving the benefits expected upon contract awards, ultimately impacting the effectiveness of Agency operations.

Audit of NSA/CSS's Internal Response to Software Vulnerabilities

A software vulnerability was at the center of a large-scale cyber-attack conducted against the Federal Government and private sector. The overall objective of the audit was to determine whether the Agency had reasonable assurance that NSA systems and networks were not compromised by this software vulnerability. Our review did not reveal any compromises of NSA/CSS systems; however, we identified three findings related to the Agency's internal response.

Audit of the Cryptologic Reserve Program (CRP)

The objective of this audit was to determine if the Agency is conducting the Standby Active Reserves and Selective Employment of Retirees (SAR/SER) civilian annuitant programs economically, efficiently, and effectively.

Hiring and retaining a diverse and expert workforce remains a priority for NSA. NSA utilizes the CRP to rehire federal retirees on a temporary basis to provide support to mission. While the OIG recognizes that SAR/SER participants are vital to programs, the OIG found the following issues:

- Multiple internal policy violations and a lack of fully documented justifications of exceptions to time limits for some participants in the program.
- A risk of waste as the OIG could not determine if the grade level of the SAR/SERs were appropriate based on the work being completed. For example, six General Grade (GG) 15/10 CRP participants were assigned to the COVID Call Center to conduct contact tracing.
- Review of administrative functions revealed thousands of hours not properly accounted for due to antiquated procedures.
- Reimbursement of Agency administrative services rendered to U.S. Cyber Command could be affected due to insufficient documentation. This creates an increased risk that the CRP process will not be consistent and repeatable.

The findings identified by the OIG in this audit highlight the need for stronger controls and updated policies and procedures.

Audit of NSA's FY 2022 Compliance With the Payment Integrity Information Act of 2019

The OIG *Audit of NSA's FY 2022 Compliance With the Payment Integrity Information Act of 2019* (PIIA) determined that NSA was compliant with PIIA. Using the procedures outlined in the Office of Management and Budget (OMB) Circular A-123, Appendix C, "Requirements for Payment Integrity Improvement," updated 5 March 2021, the OIG found that the Agency complied with all 10 PIIA reporting requirements for the fiscal year that ended on 30 September 2022.

Audit of the Cryptologic Reserve FY 2023 Statement of Standards for Attestation Engagement 18, NSA's Description of Its System Supporting the Performance of Financial Processing Services and the Suitability of the Design and Operating Effectiveness of Its Controls

The OIG contracted with an independent public accounting firm to perform an examination of NSA's description of its system supporting the performance of financial processing services on behalf of another U.S. Government organization from 1 October 2022 through 30 June 2023 and to perform an examination 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 to effectively provide reasonable assurance that the control objectives were achieved.

Inspection Reports

Recurring Challenges Noted in OIG Inspections January 2021 – December 2022

The OIG routinely inspects NSA enterprise field elements. The OIG identified recurring challenges during 11 inspections from 1 January 2021 through 30 September 2022. This report provides an overview of the most prominent repeat findings to assist leaders across the Agency as they consider their own organizational processes, practices, and structure, and also highlights best practices to help organizations identify how others addressed similar findings with holistic solutions or mitigations. It is important to note that the OIG did not evaluate every area at every site because sites are configured differently, applicable policies and guidance evolved, and some inspections focused on document reviews or were inspected virtually due to the COVID-19 pandemic.

The OIG believes that most of the concerns noted in this report—and in our 2021 Trends Report—can be grouped into four general categories:

- Missing, out-of-date, or inaccurate documentation;
- Failure to follow existing policies, regulations, and/or procedures;
- Lack of accountability or inadequate management oversight; and
- Inconsistent communications from and among site leaders.

Joint Inspectors General Inspection of NSA/CSS Texas

The OIG interviewed members of the NSA Texas (NSAT) management and workforce regarding NSAT's operations and functions. NSAT leadership and personnel fully supported the inspection. We identified challenges related to workforce engagement, outdated or incomplete documentation, and continuity of operations.

Evaluation of Targeting System Control Frameworks

The OIG conducted this evaluation to determine the effectiveness and efficiency of a targeting system's control framework as it relates to external targeting systems and requests. The evaluation examined how NSA prepares certain requests, as well as evaluated 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.

The OIG assessed in general that the control framework was properly functioning to ensure compliance with the laws, directives, and policies that protect civil liberties and individual privacy.

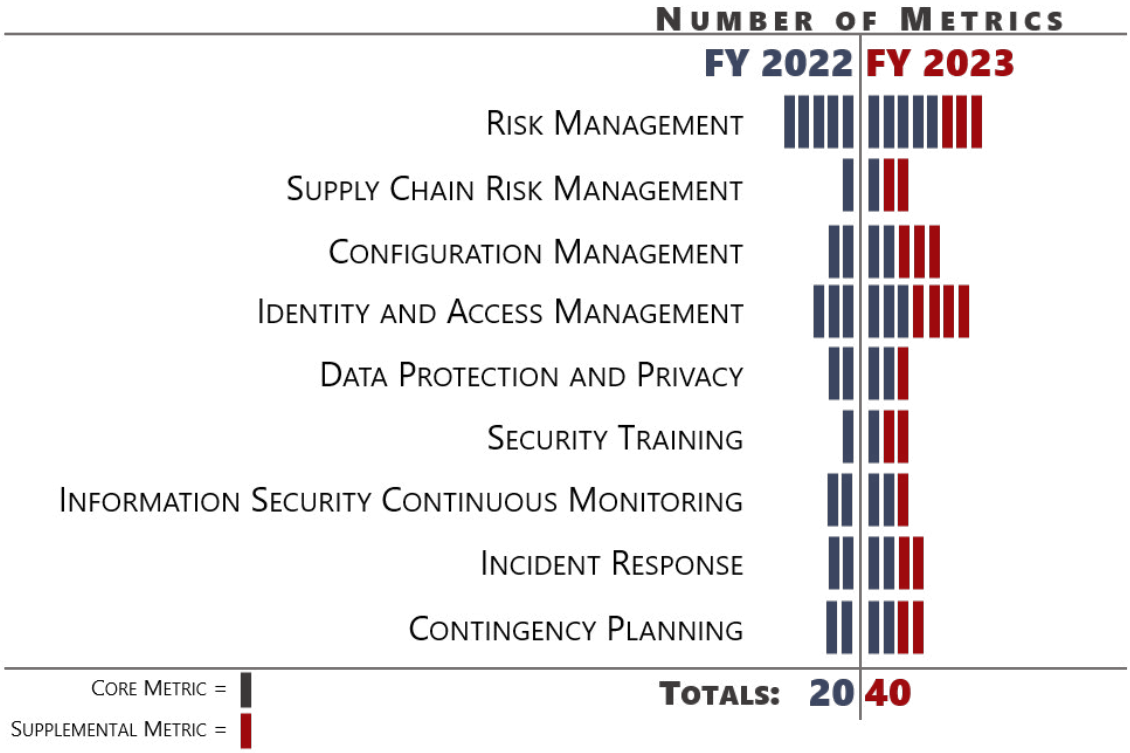
Review Related to Alleged NSA Targeting of a Member of the U.S. Media

The OIG conducted a review related to allegations that NSA improperly targeted the communications of a member of the U.S. news media. The OIG found no evidence that NSA targeted the media member or their communications.

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

The Federal Information Security Modernization Act of 2014 (FISMA) requires OIGs to annually assess the effectiveness of the information security programs of the agencies they oversee. OIG assessments are completed in accordance with 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 three-year assessment cycle in which a total of 20 core metrics are to be assessed annually, and another 40 supplemental metrics are to be divided and evaluated in either the second or third year of the cycle. On 10 February 2023, OMB issued the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, outlining the metrics to be assessed for FY 2023. These metrics align with the five functional areas in the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*: Identify, Protect, Detect, Respond, and Recover. The FY 2023-2024 Reporting Metrics represent a continuation of the work started in FY 2022. The FY 2023 evaluation represents the second year of the three-year evaluation cycle. The figure below depicts the shift in the number of assessed metrics in the nine security areas between FY 2022 and FY 2023.



Number of Metrics Assessed in FY 2022 and FY 2023

In FY 2023, because the number of metrics assessed in each security area increased, each metric had a lesser 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 2023 assessment is not directly comparable to prior years' assessments.

Our evaluation found that NSA had defined policies, procedures, and strategies (Maturity Level 2) for Risk Management, Supply Chain Risk Management, Configuration Management, Security Training, Information Security Continuous Monitoring, and Contingency Planning. Additionally, NSA consistently implemented its policies, procedures, and strategies (Maturity Level 3) for Identity and Access Management, Data Protection and Privacy, and Incident Response.

The OIG concluded that NSA had at least defined policies, procedures, and strategies for all FISMA IT security areas. In addition, NSA had consistently implemented policies, procedures, and strategies for three of the nine areas. 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. Within the context of the maturity model, achieving a Level 4 or above represents an effective level of security.

Total Dollar Value of Questioned Costs and Funds Put to Better Use During the Reporting Period

No questioned costs or funds put to better use were identified in OIG reports during this reporting period.

Information Regarding Management Decisions

The Inspector General Act of 1978, as amended (5 U.S.C. Ch. 4) (IG Act), defines "management decision" as the evaluation by the management of an establishment of the findings and recommendations included in an audit report and the issuance of a final decision by management concerning its response to the findings and recommendations, including actions concluded to be necessary. For NSA OIG audits and evaluations, management's decision to agree or disagree with a recommendation and submission of a corrective action plan occurs prior to issuance of the final report. For NSA OIG inspections, management's decision to agree or disagree with a recommendation occurs prior to issuance of the final report, and their submission of a corrective action plan occurs shortly after issuance of the final report.

Management decisions made in the current reporting period to reverse or change the initial management decision made during a prior reporting period, including changing the organization responsible for the recommendation, are listed below:

Evaluation of Targeting System Control Frameworks

NSA management submitted a request to modify the wording of a corrective action plan for one recommendation to fully meet its intent. The OIG agreed the wording modification aligned with the intent of the recommendation.

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

NSA reported in its *Agency Financial Report* for FY 2022 that it is not in substantial compliance with Section 803(a) of the FFMIA. Specifically, it is not in compliance with federal financial management systems requirements or applicable federal accounting standards. NSA's target for compliance is FY 2028.

INVESTIGATIONS

Summary of Closed Significant Investigations

$377.45 Million Settlement of False Claims Act Allegations

In a settlement announced by the Department of Justice (DOJ), the NSA OIG was recognized for our involvement in this multi-agency investigation and settlement. Investigative partners included the DOJ, the NSA OIG, the Defense Contract Management Agency, the Defense Criminal Investigative Service, the Federal Bureau of Investigations, and numerous OIGs.

Reprisal

The OIG completed four separate investigations into allegations of reprisal. The investigations determined that eight Agency supervisors—which included two Senior Executives and one senior employee—did not reprise against four Agency employees for making protected disclosures and did not engage in any arbitrary or capricious act that adversely affected the rights of the subordinate.

Computer Misuse

An OIG investigation determined that an Agency employee, after being contacted by a potential foreign national, misused NSA information systems and violated the Agency's signals intelligence (SIGINT) authorities and reporting requirements by utilizing a SIGINT tool for non-mission related and unauthorized purposes.

Total Number of Convictions Resulting From Investigations

No convictions resulted from OIG investigations in this reporting period.

Investigative Statistical Tables

Category	Total [a]
Number of Investigative Reports	23
Number of Persons Referred to the Department of Justice for Criminal Prosecution	21
Number of Persons Referred to the State and Local Prosecuting Authorities for Criminal Prosecution	0
Number of Indictments and Criminal Informations That Resulted From Prior Referrals	0

Note: [a] Statistical tables were developed by compiling data from the NSA OIG's internal Investigations Division database.

Investigations Substantiating Misconduct Involving Senior Employees

GG-15: Failure to Exercise Courtesy and Respect

The OIG substantiated that a GG-15 Agency employee failed to treat their subordinates and/or colleagues with courtesy and respect.

GG-15: Failure to Exercise Courtesy and Respect and Harassment

The OIG substantiated that a GG-15 Agency employee failed to treat their subordinates and/or colleagues with courtesy and respect, and harassed them through comments, gestures, and inappropriate nonsexual touching.

GG-15: Nepotism

The OIG substantiated that a GG-15 Agency employee violated nepotism policies by advocating for their child's selection into a supervisory position.

See "Summary of Closed Significant Investigations" section above for other senior employee cases.

Substantiated Investigations of Whistleblower Retaliation

There were no instances of substantiated whistleblower retaliation during this period.

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 2023, the OIG did not open or complete any investigations of disclosures of information that have been determined to be classified.

Audits, Inspections, and Evaluations and Investigations of Senior Government Employees Closed and Not Disclosed to the Public

This SAR discloses to the public all audits, inspections, evaluations, and investigations involving senior government employees closed during the reporting period.

Appendix A: Peer Review

Peer Reviews Conducted by Other OIGs

No peer reviews were performed during this reporting period. The last peer review of the NSA OIG was of the Audits Division, led by the OIG of the Intelligence Community and supported by the National Reconnaissance Office (NRO) and Defense Intelligence Agency OIGs, covering the three-year period from 1 April 2018 through 31 March 2021.

Peer Reviews Conducted by NSA OIG

The NSA OIG did not complete a peer review of another OIG during this reporting period. The last peer review led by the NSA OIG was of the NRO OIG's Investigative Operations Division, for which the report was issued on 1 December 2022. There are no outstanding recommendations from any peer reviews performed by the NSA OIG.

Appendix B: Recommendations Made Before the Reporting Period for Which Corrective Action Has Not Been Completed and All Outstanding Recommendations in the Past 12 Months

Issue Date	Report Number	Recommendation Number[1]
3/31/2011	AU-11-0001	AU-11-0001-1b
3/31/2011	AU-11-0001	AU-11-0001-2
3/31/2011	AU-11-0001	AU-11-0001-3
6/28/2013	AU-13-0004	AU-13-0004-5
6/19/2015	AU-14-0005	AU-14-0005-6
7/23/2015	JT-15-0002	FH-15-1015
3/30/2016	IN-16-0001	MI-16-2009
3/30/2016	IN-16-0001	MI-16-1038
10/4/2016	IG-16-11869	CM-1
2/21/2017	IN-17-0001	SG-17-2503
5/18/2017	IN-16-0009	UT-16-2101
7/14/2017	AD-17-0001	AD-17-0001-1
8/17/2017	ST-16-0003	ST-16-0003-3
9/8/2017	JT-17-0001	TX-17-2005
10/26/2017	AU-17-0005	AU-17-0005a-1
12/20/2017	JT-17-0002	PG-17-0101-S
12/29/2017	AU-16-0018	AU-16-0018-18
1/3/2018	AU-16-0004	AU-16-0004-1
1/3/2018	AU-16-0004	AU-16-0004-6
1/26/2018	IN-18-0001	PA-18-2003
6/29/2018	IN-18-0002	ND-18-2501
8/1/2018	JT-18-0001	FG-18-1302
8/1/2018	JT-18-0001	FG-18-2314
9/21/2018	ST-17-0003	ST-17-0003-19
9/28/2018	ST-17-0001	ST-17-0001-4
9/28/2018	ST-17-0001	ST-17-0001-7
9/28/2018	ST-17-0001	ST-17-0001-8
9/28/2018	ST-17-0001	ST-17-0001-14
9/28/2018	ST-17-0001	ST-17-0001-9
11/6/2018	IN-18-0006	BA-18-2302
11/16/2018	IN-18-0007	KI-18-2402
11/16/2018	IN-18-0007	KI-18-2403
11/16/2018	IN-18-0007	KI-18-2601
11/16/2018	IN-18-0007	KI-18-2506
3/11/2019	JT-18-0002	AK-18-2501
3/11/2019	JT-18-0002	AK-18-1001
3/26/2019	ST-17-0002	ST-17-0002-5
3/26/2019	ST-17-0002	ST-17-0002-10
3/26/2019	ST-17-0002	ST-17-0002-7
7/11/2019	IN-19-0002A	SU-19-2902
7/22/2019	AU-18-0016	AU-18-0016-4
8/16/2019	IN-18-0009	NP-18-2508
8/16/2019	IN-18-0009	NP-18-2001
8/28/2019	JT-18-0003	FH-18-2301
8/28/2019	JT-18-0003	FH-18-2001
8/28/2019	JT-18-0003	FH-18-2501
8/28/2019	JT-18-0003	FH-18-2502
8/28/2019	JT-18-0003	FH-18-1501
8/28/2019	JT-18-0003	FH-18-1507
8/28/2019	JT-18-0003	FH-18-1508
8/28/2019	JT-18-0003	FH-18-1509
8/28/2019	JT-18-0003	FH-18-1704

[1] There are no potential cost savings associated with any of these recommendations.

Issue Date	Report Number	Recommendation Number
9/27/2019	ST-18-0003	ST-18-0003-1
9/30/2019	AU-18-0013	AU-18-0013-18
10/2/2019	AU-18-0002	AU-18-0002-1
10/2/2019	AU-18-0002	AU-18-0002-4
12/18/2019	ST-18-0002	ST-18-0002-3
12/18/2019	ST-18-0002	ST-18-0002-4
12/18/2019	ST-18-0002	ST-18-0002-5
12/18/2019	ST-18-0002	ST-18-0002-6
12/18/2019	ST-18-0002	ST-18-0002-7
12/19/2019	IN-19-0001	TR-19-1504
2/21/2020	EV-20-0001	EV-20-0001-1
3/17/2020	IN-19-0002	SU-19-2103
3/17/2020	IN-19-0002	SU-19-2502
6/16/2020	ST-18-0004	ST-18-0004-1
6/16/2020	ST-18-0004	ST-18-0004-4
6/16/2020	ST-18-0004	ST-18-0004-6
6/18/2020	ST-18-0006	ST-18-0006-18
6/18/2020	ST-18-0006	ST-18-0006-21
6/18/2020	ST-18-0006	ST-18-0006-25
6/18/2020	ST-18-0006	ST-18-0006-17
6/18/2020	ST-18-0006	ST-18-0006-8
6/18/2020	ST-18-0006	ST-18-0006-9
6/18/2020	ST-18-0006	ST-18-0006-12
6/18/2020	ST-18-0006	ST-18-0006-16
6/18/2020	ST-18-0006	ST-18-0006-23
7/1/2020	ST-18-0009	ST-18-0009-21
7/1/2020	ST-18-0009	ST-18-0009-1
7/1/2020	ST-18-0009	ST-18-0009-6
7/1/2020	ST-18-0009	ST-18-0009-23
7/1/2020	ST-18-0009	ST-18-0009-8
7/1/2020	ST-18-0009	ST-18-0009-3
7/1/2020	ST-18-0009	ST-18-0009-25
7/1/2020	ST-18-0009	ST-18-0009-20
7/1/2020	ST-18-0009	ST-18-0009-24
7/1/2020	ST-18-0009	ST-18-0009-15
7/1/2020	ST-18-0009	ST-18-0009-12
7/1/2020	ST-18-0009	ST-18-0009-5
7/14/2020	JT-19-0001	MH-19-1608
7/14/2020	JT-19-0001	MH-19-2504
7/14/2020	JT-19-0001	MH-19-2505
7/14/2020	JT-19-0001	MH-19-2506
7/14/2020	JT-19-0001	MH-19-2601
7/14/2020	JT-19-0001	MH-19-1301
7/14/2020	JT-19-0001	MH-19-1302
9/21/2020	AU-19-0001	AU-19-0001-3
9/30/2020	ST-19-0002	ST-19-0002-3
9/30/2020	ST-19-0002	ST-19-0002-8
9/30/2020	ST-19-0002	ST-19-0002-9
9/30/2020	ST-19-0002	ST-19-0002-12
9/30/2020	ST-19-0002	ST-19-0002-4
9/30/2020	ST-19-0002	ST-19-0002-1
9/30/2020	ST-19-0002	ST-19-0002-2
9/30/2020	ST-19-0002	ST-19-0002-5
9/30/2020	ST-19-0002	ST-19-0002-7
12/17/2020	AU-18-0012	AU-18-0012-5
12/17/2020	AU-18-0012	AU-18-0012-6
2/5/2021	AD-21-0001	SB-21-1402
2/26/2021	AD-20-0004	SJ-20-1501
2/26/2021	AD-20-0004	SJ-20-1502
2/26/2021	AD-20-0004	SJ-20-1603
3/2/2021	JT-19-0003	ET-19-1520
3/17/2021	AD-20-0006	MI-20-1303
3/31/2021	ST-19-0003	ST-19-0003-16
6/1/2021	IN-19-0004	AF-19-2302
6/11/2021	EV-21-0007	EV-21-0007-QRR-2
7/16/2021	IN-21-0001A	FL-21-2901
7/16/2021	IN-21-0001A	FL-21-2902
7/16/2021	IN-21-0001A	FL-21-2904
8/30/2021	EV-19-0002	EV-19-0002-15
8/30/2021	EV-19-0002	EV-19-0002-17
8/30/2021	EV-19-0002	EV-19-0002-1
8/30/2021	EV-19-0002	EV-19-0002-3
8/30/2021	EV-19-0002	EV-19-0002-6
8/30/2021	EV-19-0002	EV-19-0002-2
8/30/2021	EV-19-0002	EV-19-0002-16
8/30/2021	EV-19-0002	EV-19-0002-12
8/30/2021	EV-19-0002	EV-19-0002-9
9/28/2021	JT-20-0001	SL-20-1402

Issue Date	Report Number	Recommendation Number
9/28/2021	JT-20-0001	SL-20-1410 (formerly SL-20-2433)
9/28/2021	JT-20-0001	SL-20-2304
9/28/2021	JT-20-0001	SL-20-1603
9/28/2021	JT-20-0001	SL-20-1605
9/28/2021	JT-20-0001	SL-20-2301
9/28/2021	JT-20-0001	SL-20-1311
9/28/2021	JT-20-0001	SL-20-2402
9/28/2021	JT-20-0001	SL-20-2403
9/28/2021	JT-20-0001	SL-20-2407
9/28/2021	JT-20-0001	SL-20-2413
9/28/2021	JT-20-0001	SL-20-2414
9/28/2021	JT-20-0001	SL-20-2416
9/28/2021	JT-20-0001	SL-20-2417
9/28/2021	JT-20-0001	SL-20-2418
9/28/2021	JT-20-0001	SL-20-2419
9/28/2021	JT-20-0001	SL-20-2420
9/28/2021	JT-20-0001	SL-20-2422
9/28/2021	JT-20-0001	SL-20-2430
9/28/2021	JT-20-0001	SL-20-2437
9/28/2021	JT-20-0001	SL-20-2426
9/28/2021	JT-20-0001	SL-20-1502
9/28/2021	JT-20-0001	SL-20-1503
9/28/2021	JT-20-0001	SL-20-1504
9/28/2021	JT-20-0001	SL-20-1514
9/28/2021	JT-20-0001	SL-20-1515
9/28/2021	JT-20-0001	SL-20-1521
9/28/2021	JT-20-0001	SL-20-1540
9/28/2021	JT-20-0001	SL-20-2109
9/29/2021	EV-21-0002	EV-21-0002-4
9/29/2021	EV-21-0002	EV-21-0002-2
9/29/2021	EV-21-0002	EV-21-0002-11
9/29/2021	EV-21-0002	EV-21-0002-5
9/30/2021	AU-20-0007	AU-20-0007-12
9/30/2021	AU-20-0007	AU-20-0007-7
9/30/2021	AU-20-0007	AU-20-0007-6
9/30/2021	AU-20-0007	AU-20-0007-15
9/30/2021	AU-20-0007	AU-20-0007-2
9/30/2021	AU-20-0007	AU-20-0007-3

Issue Date	Report Number	Recommendation Number
1/21/2022	IN-21-0001	FL-21-2309
1/21/2022	IN-21-0001	FL-21-2301
1/21/2022	IN-21-0001	FL-21-1301
1/21/2022	IN-21-0001	FL-21-1402
1/21/2022	IN-21-0001	FL-21-2506
1/21/2022	IN-21-0001	FL-21-2603
2/9/2022	EV-20-0005	EV-20-0005-2
2/9/2022	EV-20-0005	EV-20-0005-3
2/9/2022	EV-20-0005	EV-20-0005-8
2/9/2022	EV-20-0005	EV-20-0005-10
2/9/2022	EV-20-0005	EV-20-0005-9
2/9/2022	EV-20-0005	EV-20-0005-7
2/9/2022	IN-21-0003	NC-21-1301
3/25/2022	AU-20-0008	AU-20-0008-3
3/25/2022	AU-20-0008	AU-20-0008-4
5/20/2022	IN-21-0002	SO-21-2103
5/20/2022	IN-21-0002	SO-21-2501
6/30/2022	AD-21-0006	AD-21-0006-2
6/30/2022	AD-21-0006	AD-21-0006-4
9/14/2022	EV-21-0005	EV-21-0005-1
9/14/2022	EV-21-0005	EV-21-0005-2
9/14/2022	EV-21-0005	EV-21-0005-3
9/14/2022	EV-21-0005	EV-21-0005-4
9/14/2022	EV-21-0005	EV-21-0005-5
9/14/2022	EV-21-0005	EV-21-0005-6
9/14/2022	EV-21-0005	EV-21-0005-8
9/14/2022	EV-21-0005	EV-21-0005-9
9/14/2022	EV-21-0005	EV-21-0005-11
9/14/2022	EV-21-0005	EV-21-0005-12
9/14/2022	EV-21-0005	EV-21-0005-17
9/14/2022	EV-21-0005	EV-21-0005-18
9/14/2022	EV-21-0005	EV-21-0005-19
9/14/2022	EV-21-0005	EV-21-0005-20
9/14/2022	EV-21-0005	EV-21-0005-23
9/14/2022	EV-21-0005	EV-21-0005-24
9/14/2022	EV-21-0005	EV-21-0005-25
9/14/2022	EV-21-0005	EV-21-0005-26
9/14/2022	EV-21-0005	EV-21-0005-7
9/14/2022	EV-21-0005	EV-21-0005-16
9/14/2022	EV-21-0005	EV-21-0005-21

Issue Date	Report Number	Recommendation Number
9/14/2022	EV-21-0005	EV-21-0005-22
9/19/2022	JT-21-0002	UT-21-2210
9/19/2022	JT-21-0002	UT-21-2214
9/19/2022	JT-21-0002	UT-21-2301
9/19/2022	JT-21-0002	UT-21-2302
9/19/2022	JT-21-0002	UT-21-2304
9/19/2022	JT-21-0002	UT-21-1304
9/19/2022	JT-21-0002	UT-21-1310
9/19/2022	JT-21-0002	UT-21-2404
9/19/2022	JT-21-0002	UT-21-1516
9/19/2022	JT-21-0002	UT-21-1522
9/19/2022	JT-21-0002	UT-21-1609
9/19/2022	JT-21-0002	UT-21-2602
9/23/2022	EV-19-0003	EV-19-0003-1
9/23/2022	EV-19-0003	EV-19-0003-4
9/27/2022	EV-22-0003	EV-22-0003-1
9/27/2022	EV-22-0003	EV-22-0003-2
9/27/2022	EV-22-0003	EV-22-0003-3
9/27/2022	EV-22-0003	EV-22-0003-4
9/27/2022	EV-22-0003	EV-22-0003-5
9/27/2022	EV-22-0003	EV-22-0003-7
9/27/2022	EV-22-0003	EV-22-0003-9
9/27/2022	EV-22-0003	EV-22-0003-6
9/27/2022	EV-22-0003	EV-22-0003-10

Outstanding Recommendations in the Past 12 Months		
Issue Date	Report Number	Recommendation Number
10/17/2022	EV-21-0011	EV-21-0011-A.1.a
10/17/2022	EV-21-0011	EV-21-0011-A.1.b
11/17/2022	AD-23-0002	AD-23-0002-01
11/17/2022	AD-23-0002	AD-23-0002-02
11/17/2022	AD-23-0002	AD-23-0002-03
11/17/2022	AD-23-0002	AD-23-0002-04
11/17/2022	AD-23-0002	AD-23-0002-05
4/7/2023	JT-22-0001	TX-22-2001
4/7/2023	JT-22-0001	TX-22-2402
4/7/2023	JT-22-0001	TX-22-1514
4/7/2023	JT-22-0001	TX-22-1702
4/7/2023	JT-22-0001	TX-22-2701
4/7/2023	JT-22-0001	TX-22-2702
5/2/2023	AU-22-0001	AU-22-0001-3
5/2/2023	AU-22-0001	AU-22-0001-4
5/2/2023	AU-22-0001	AU-22-0001-11
5/8/2023	AU-23-0010	AU-23-0010-2
5/8/2023	AU-23-0010	AU-23-0010-3
5/8/2023	AU-23-0010	AU-23-0010-1
5/22/2023	AU-22-0006	AU-22-0006-2
5/22/2023	AU-22-0006	AU-22-0006-3
5/22/2023	AU-22-0006	AU-22-0006-4
5/22/2023	AU-22-0006	AU-22-0006-5
5/22/2023	AU-22-0006	AU-22-0006-6
5/22/2023	AU-22-0006	AU-22-0006-7
5/22/2023	AU-22-0006	AU-22-0006-8
5/22/2023	AU-22-0006	AU-22-0006-9
5/22/2023	AU-22-0006	AU-22-0006-10
5/22/2023	AU-22-0006	AU-22-0006-11
5/22/2023	AU-22-0006	AU-22-0006-12
5/22/2023	AU-22-0006	AU-22-0006-14
5/22/2023	AU-22-0006	AU-22-0006-15
5/22/2023	AU-22-0006	AU-22-0006-16
5/26/2023	EV-20-0009	EV-20-0009-2
5/26/2023	EV-20-0009	EV-20-0009-3
5/26/2023	EV-20-0009	EV-20-0009-7
5/26/2023	EV-20-0009	EV-20-0009-8
5/26/2023	EV-20-0009	EV-20-0009-10

Issue Date	Report Number	Recommendation Number
5/26/2023	EV-20-0009	EV-20-0009-11
5/26/2023	EV-20-0009	EV-20-0009-14
5/26/2023	EV-20-0009	EV-20-0009-20
5/26/2023	EV-20-0009	EV-20-0009-22
5/26/2023	EV-20-0009	EV-20-0009-23
5/26/2023	EV-20-0009	EV-20-0009-25
5/26/2023	EV-20-0009	EV-20-0009-21
5/26/2023	EV-20-0009	EV-20-0009-24
5/26/2023	EV-20-0009	EV-20-0009-26
6/15/2023	EV-21-0010	EV-21-0010-1
6/15/2023	EV-21-0010	EV-21-0010-2
7/6/2023	AU-22-0003	AU-22-0003-5
7/6/2023	AU-22-0003	AU-22-0003-6
7/6/2023	AU-22-0003	AU-22-0003-7
7/27/2023	AU-22-0002	AU-22-0002-4
7/27/2023	AU-22-0002	AU-22-0002-5
7/27/2023	AU-22-0002	AU-22-0002-6
7/27/2023	AU-22-0002	AU-22-0002-7
7/27/2023	AU-22-0002	AU-22-0002-8
7/27/2023	AU-22-0002	AU-22-0002-9
7/27/2023	AU-22-0002	AU-22-0002-10
7/27/2023	AU-22-0002	AU-22-0002-16
7/27/2023	AU-22-0002	AU-22-0002-17
7/27/2023	AU-22-0002	AU-22-0002-18
7/27/2023	AU-22-0002	AU-22-0002-19
7/27/2023	AU-22-0002	AU-22-0002-21
7/27/2023	AU-22-0002	AU-22-0002-22
7/27/2023	AU-22-0002	AU-22-0002-23
7/27/2023	AU-22-0002	AU-22-0002-26
7/27/2023	AU-22-0002	AU-22-0002-28
7/27/2023	AU-22-0002	AU-22-0002-3
7/27/2023	AU-22-0002	AU-22-0002-13
7/27/2023	AU-22-0002	AU-22-0002-25
7/27/2023	AU-22-0002	AU-22-0002-27

Appendix C: Abbreviations List

CIGIE	Council of the Inspectors General on Integrity and Efficiency
CRP	Cryptologic Reserve Program
CSS	Central Security Service
DoD	Department of Defense
DOJ	Department of Justice
FFMIA	Federal Financial Management Improvement Act of 1996
FISMA	Federal Information Security Modernization Act of 2014
GG	General Grade
IC	Intelligence Community
IG Act	Inspector General Act of 1978, as amended (5 U.S.C. Ch. 4)
IO	intelligence oversight
IT	information technology
NDAA	National Defense Authorization Act for Fiscal Year 2020
NRO	National Reconnaissance Office
NSA	National Security Agency
NSAT	National Security Agency, Texas
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIIA	Payment Integrity Information Act of 2019
SAR	Semiannual Report
SAR/SER	Standby Active Reserves and Selective Employment of Retirees
SCRM	supply chain risk management
SIGINT	signals intelligence

Appendix D: Index of Reporting Requirements

IG Act Reference [a]	Reporting Requirements	Page
§405(a)(1)[b]	Significant problems, abuses, and deficiencies	2-6
§405(a)(2)	Recommendations made before the reporting period for which corrective action has not been completed	13
§405(a)(3)	Summary of significant investigations closed during the reporting period	9
§405(a)(4)	Identification of the total number of convictions during the reporting period resulting from investigations	9
§405(a)(5)(A)	Listing of each audit, inspection, or evaluation	2-6
§405(a)(5)(B)	Total dollar value of questioned costs and the dollar value of recommendations that funds be put to better use	6
§405(a)(6)	Information regarding any management decisions	7
§405(a)(7)	Information described under section 804(b) of the Federal Financial Management Improvement Act of 1996	8
§405(a)(8)	(A) Results of any peer review conducted by another Office of Inspector General during the reporting period; or (B) A statement identifying the date of the last peer review conducted by another Office of Inspector General	12
§405(a)(9)	List of any outstanding recommendations from any peer review conducted by another Office of Inspector General that have not been fully implemented	12
§405(a)(10)	List of any peer reviews conducted by the Inspector General of another Office of the Inspector General during the reporting period	12
§405(a)(11)	Investigative statistical tables	9
§405(a)(12)	Description of metrics used for statistical tables of investigations	9
§405(a)(13)	Each investigation conducted by the Office where allegations of misconduct were substantiated involving a senior Government employee or senior official	10
§405(a)(14)	Detailed description of any instance of whistleblower retaliation	10
§405(a)(15) (A) and (B)	Information related to interference by the establishment including attempts to interfere with independence of the Office and a summary of each report made to the head of the establishment (if interference occurred)	1
§405(a)(16)	(A) Detailed descriptions of each inspection, evaluation, and audit conducted that is closed and was not disclosed to the public; and/or (B) Detailed descriptions of each investigation involving a senior Government employee that is closed and was not disclosed to the public	11
§405(a)(note)	P.L. 110-181 §845, Final, completed contract audit reports	NA
§405(a)(note)	P.L. 103-355 (as amended), Outstanding recommendations past 12 months	13

Note: [a] Citations are to the IG Act of 1978, as amended (5 U.S.C. Ch 4).
[b] Requirement covered by §405(a)(5)(A).

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, efficiency, and 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 Intelligence Community (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*.

AUDIT

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, efficiency, and 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

963.5023 (s) | 301.688.6327 (b)

FAX: 443.479.0099