NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

Unclassified Summary

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

12 December 2019

OFFICE OF THE INSPECTOR GENERAL

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

AUDIT

The Audit Division comprises three sections: Cybersecurity and Technology, Financial Audits, and Mission and Mission Support. The Division's audits and evaluations examine the economy, 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 reporting are fairly and accurately presented. Audits are conducted in accordance with auditing standards established by the Comptroller General of the United States.

INSPECTIONS

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

INTELLIGENCE OVERSIGHT

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

INVESTIGATIONS

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

NOTE: A classified version of the Study of NSA Controls to Comply with Signals Intelligence Retention Requirements formed the basis of the unclassified summary.

Overview

The National Security Agency/Central Security Service (NSA) Office of the Inspector General (OIG) conducted this study to determine whether NSA's implementation of controls for aging-off signals intelligence (SIGINT) data is compliant with law and policy.[1] [2] Requirements for retention of SIGINT are established by statutes, minimization procedures, national and NSA policies, and court orders; they vary by authority. Together, these requirements establish data retention limits to protect civil liberties and individual privacy. In order to be compliant, NSA must ensure an adequate system of internal compliance controls has been implemented. Conversely, non-compliance could impact civil liberties and privacy protections and lead to constraints from overseers on NSA SIGINT authorities.

In this study, we focused on the effectiveness of age-off controls implemented in one of NSA's largest SIGINT repositories to ensure data is retained only for the period of time authorized under legal and policy requirements. In summary, we found:

1. NSA's primary content repository has retained a small percentage of the large number of SIGINT data objects beyond legal and policy retention limits in the two data stores tested. NSA has not fully implemented age-off calculations that use the most specific retention requirement with which data objects are labeled.

2. Planned updates to NSA retention policy and legal and policy working aids have been delayed and do not incorporate all current law and policy.

3. Current oversight must be strengthened if it is to ensure compliance with retention requirements.

4. Implementation of age-off for some SIGINT collection authorities in some databases was not in compliance with NSA/CSS Policy Instruction 2-0001, *Early Age-off Decisions for Unevaluated or Unminimized Signals Intelligence*.

The OIG's findings reflect significant risks of noncompliance with legal and policy requirements for retention of SIGINT data. These requirements include established minimization procedures for NSA SIGINT authorities, meaning that the deficiencies we identified have the potential to impact civil liberties and individual privacy. The Agency is making changes to its ingest validation process in an effort to improve its age-off methodology and the accuracy of the information used to determine age-off. The OIG believes implementation of this process for all types of SIGINT data is needed. Overall, the OIG made 11 recommendations to assist NSA in addressing the risks, and ensuring that data retention is conducted in accordance with all applicable requirements and

[1] SIGINT comprises communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, either individually or in combination.

[2] For this study, the OIG reviewed SIGINT data collected pursuant to Executive Order (E.O.) 12333, United States Intelligence Activities, as amended, and the Foreign Intelligence Surveillance Act (FISA) of 1978, including the FISA Amendments Act (FAA) of 2008, as amended.

privacy rights. The Agency agreed with all of the OIG's recommendations. As of the date of this summary, the Agency has taken action sufficient for the OIG to close four of the recommendations, and the OIG has determined that the actions the Agency plans to take meet the intent of the remaining recommendations.

Background

Data Deletion. NSA has established procedures to delete SIGINT data in accordance with applicable laws and policies, which require deletion of SIGINT data in two situations: 1) on or before its authorized retention expiration date (referred to as "age-off"), and 2) on demand (referred to as "purge") when data NSA is not authorized to acquire or retain is discovered.[3]

NSA System Compliance Certification. NSA implemented system compliance certification standards in 2010 to provide reasonable assurance that NSA systems operate in accordance with the laws and policies that address civil liberties and individual privacy. Evidence that the system meets the detailed requirements that support compliant execution of functions (including age-off) is required for certification. To manage age-off, certified systems must:

1. Reliably determine the legal authorities of the SIGINT information stored within the repository;
2. Apply the appropriate retention period to SIGINT data stored within the repository in compliance with the applicable minimization procedures; and
3. Reliably prevent the re-ingestion of previously aged-off SIGINT data, such as from a back-up system.

Certain certified systems are designated by the Agency as Source Systems of Record (SSRs) and are the only repositories authorized to provide source documentation for FISA court applications, SIGINT reports, and some targeting decisions.[4] Using only the data contained in these systems ensures consistency with NSA's legal representations concerning the steps it has taken to prevent use of SIGINT data that is ineligible for retention for these purposes.

The primary SIGINT SSR for content began ingesting data in 2012. The majority of that data is subject to a 5-year legal retention period with age-off commencing in 2017, so OIG testing was performed when the repository had been in place long enough that its age-off process was expected

[3] The OIG is conducting a separate review of the effectiveness and efficiency of the Agency's process to purge non-compliant SIGINT data completely, reliably, and in a timely manner in accordance with legal and policy requirements.

[4] A target is an entity against which intelligence operations are conducted.

to manage 5 years' worth of data. We tested the age-off as calculated by this repository to determine whether raw SIGINT was retained beyond the maximum allowable retention.[5]

Retention Controls. NSA's primary SIGINT content repository has multiple component repositories that perform different functions. For purposes of this study, we reviewed three of these component repositories, identified in this summary as repositories "A," "B," and "C." Each of these repositories performs different functions and, though the intended retention outcomes are the same for all three, each uses one or more age-off mechanisms to manage data retention based on the way it stores data internally. The OIG tested the age-off as calculated by these component repositories to determine whether raw SIGINT was retained beyond the maximum allowable retention. By selecting these three, the OIG believes that it was able to make a comprehensive assessment of the efficacy of the age-off process within NSA's primary SIGINT content SSR for all SIGINT authorities.

Findings

Though the OIG found that NSA is taking steps to improve controls over retention, its study of the Agency's controls over the age-off of raw SIGINT revealed these concerns:

FINDING 1: NSA's Primary Content Repository Has Retained a Small Percentage of a Large Number of SIGINT Data Objects beyond Legal and Policy Retention Limits

The OIG found that NSA has not fully implemented age-off calculations that use the most specific retention requirement with which data objects are labeled, resulting in a small percentage of the large number of SIGINT data objects being retained beyond legal and policy limits.[6]

Because the component repositories selected by the OIG for testing contained large volumes of data, the OIG obtained assistance from the NSA Capabilities Directorate in extracting a representative sample of the data so that retention compliance could be determined. The OIG, with the assistance of the personnel in the NSA Operations Directorate, reviewed a portion of the sampled data from one component repository to verify the sampling approach and confirm that the data would meet the OIG's requirements for testing the repositories.[7]

Our testing found that, though NSA has implemented an improved ingest validation process for 93 percent of the SIGINT data (and about 11 percent of the data feeds) being entered in the primary

---

[5] Raw SIGINT is any SIGINT or associated data that has not been evaluated for foreign intelligence purposes and/or minimized.

[6] The label is an identifier known as the "AuthID" that indicates the legal authority under which the data item is retained.

[7] Age-off control information also was gathered by interviewing subject matter experts within NSA's Operations Directorate, Capabilities Directorate, and the Engagement & Policy Directorate – Compliance Group. We interviewed personnel from NSA's Office of the General Counsel to discuss retention requirements based on legal documents and representations. We also reviewed written processes, procedures, and other documentation pertinent to the areas selected for review.

content repository, the current process to verify the completeness, accuracy, and validity of key elements of SIGINT data objects prior to their ingestion is insufficient, and that implementation of the improved process for all types of SIGINT data is needed.

Because our test results from repositories A and B revealed that a small percentage of the large number of SIGINT data objects were retained beyond legal and policy retention limits, the OIG recommended that additional system controls be implemented to:

1) Validate all elements of the data objects and the relationships among those data elements used to determine age-off prior to ingest in the primary content repository, and

2) Prevent analytic use of data that fails the validation rules. We also recommended NSA complete the process to implement the use of AuthIDs for retention calculations for its content repositories.

The OIG's testing for repository C could not be fully executed because of system performance issues and a software problem that affected the completeness of the query used to extract the test data. The OIG recommended application of the same system controls applied to repositories A and B to repository C once the performance issues with this repository are addressed, followed by verification that age-off is executed in accordance with legal and policy requirements. NSA management agreed with all of the OIG's recommendations in this area, and indicated that it anticipated completion of the recommended actions by 30 September 2020.

FINDING 2: Retention Guidance Is Outdated

Planned updates to NSA retention policy and implementation guidance have been delayed and do not incorporate all current legal and policy requirements. The current retention policy, last revised in March 2015, provides requirements for retention of raw SIGINT but does not incorporate guidelines for retention of evaluated and minimized SIGINT data and disseminated SIGINT. An update to the policy is on hold while interagency coordination of the draft SIGINT Annex to Department of Defense Manual 5240.01 is completed. This guidance will address retention for various types of SIGINT. The OIG also found that, while NSA policy requires that the Agency create and maintain matrices to convey the maximum allowable time period that SIGINT may be retained in accordance with the authority under which it was collected, the matrix summarizing the rules governing the age-off of raw SIGINT has only been made available within the Agency as a draft for informal guidance and informational purposes. Without adequate guidance, NSA is at risk for retaining data past its legal limits.

As a result of this finding, the OIG recommended that NSA complete the update of the retention policy and review, update, and publish the implementing guidance matrix. NSA management agreed and indicated that they anticipate completing implementation by 1 February 2020.

FINDING 3: Oversight Supporting Retention Compliance Is Insufficient

NSA has established an internal compliance standard for verification of age-off activities; however, the OIG found that the Agency's current oversight efforts and controls are insufficient to meet the standard and ensure compliance with data retention requirements.

Specifically, the OIG found that internal compliance controls governing data ingested into NSA's primary SIGINT content repository lack adequate automated support to effectively manage the large data volumes. In addition, the OIG determined that the Agency's existing tools are insufficient to support oversight functions specified in its internal compliance standard to ensure that data in this repository is valid, that age-off calculations are consistently performed in compliance with legal and policy requirements, and that no data remains in the repository beyond its legal/policy retention period.

The OIG recommended the NSA Compliance organization complete a project it previously initiated to verify that compliance standards were fully incorporated in system compliance certification requirements. The OIG also recommended that NSA implement age-off verification controls and tools to support oversight of age-off and commence retention verification oversight activities. NSA management agreed with the recommendations and indicated that they anticipate completing actions in response to these recommendations by 31 December 2020.

FINDING 4: The Policy Instruction for Early Age-Off of Raw SIGINT is Unclear

NSA's internal policy for early age-off of raw SIGINT was established as an internal compliance control to delete SIGINT before it reaches its legal authority retention limit. Implementing guidance lists early age-off decisions that were approved for each SIGINT collection authority. OIG testing found that repositories A and B were not configured in a way that was consistent with this internal guidance.[8] Personnel responsible for applying the guidance to the component repositories tested told the OIG that it was unclear how the early age-off criteria were to be applied. The OIG found that deleting the data earlier than legally required could affect compliance with internal NSA policy; compliance with legal retention requirements is not affected.

The OIG recommended that NSA update its internal policy and clarify the implementing instructions. Management agreed with our recommendations and indicated that the Agency anticipates completing actions responsive to these recommendations by 31 December 2021.

Conclusion

The OIG's findings in this review reflect significant risks for noncompliance with legal and policy requirements governing the retention of SIGINT data. Those requirements include established minimization procedures for NSA SIGINT authorities, meaning that the deficiencies identified in our review have the potential to impact civil liberties and individual privacy. The changes to the Agency's ingest validation process referenced above are an effort to improve its age-off

[8] See discussion above regarding technical issues impacting on our ability to test in repository C.

methodology and the accuracy of the information used to determine age-off. The OIG believes that implementation of this process for all types of SIGINT data is needed. The OIG made a total of 11 recommendations to assist NSA in addressing the risks identified in this review and ensuring that data retention is conducted in accordance with all applicable requirements and privacy rights. The Agency agreed with all of the OIG's recommendations and has taken action sufficient to close four of them. The OIG determined that the actions the Agency plans to take meet the intent of the remaining recommendations.