



NSA Director of Civil Liberties and Privacy Office
Report

**NSA's Civil Liberties and Privacy Protections
for Targeted SIGINT Activities
Under Executive Order 12333**

October 7, 2014

Rebecca J. Richards

Director, NSA Civil Liberties and Privacy Office



EXECUTIVE SUMMARY

This report, from the NSA Civil Liberties and Privacy Office, addresses the general civil liberties and privacy protections employed by the NSA and more specifically documents additional procedures for targeted Signals Intelligence activities under Executive Order (E.O.) 12333. The Fair Information Practice Principles (FIPPs), which are the widely accepted framework of defining principles used by federal agencies to evaluate how systems, processes, or programs affect individual privacy, were used as the basis for assessment.

The report finds that NSA has multiple activities that provide civil liberties and privacy protections for six of the eight FIPPs (*Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing*). These protections are underpinned by NSA's management activities, documented compliance program, and investments in people, training, tools and technology.

Because NSA has a national security mission, the principles of *Transparency* and *Individual Participation* are not implemented in the same manner they are in organizations with a more public-facing mission. NSA cannot offer direct *Transparency* because that would alert foreign intelligence targets that they are under surveillance. NSA can only offer *Individual Participation* in limited instances for the same reason. In many cases, NSA overseers provide surrogate means for these two principles. NSA is interested in exploring ideas with those in government, the public and expert groups on how to strengthen these protections.

The report provides an overview of the signals intelligence lifecycle (Acquire, Analyze, Retain and Disseminate), and describes existing civil liberties and privacy protections that are built into each step. Agency-wide policies, directives, procedures training, and education activities also help protect the civil liberties and privacy of ordinary individuals. All employees also have responsibilities for protecting and upholding laws and policies.



I. INTRODUCTION

This report was prepared by the National Security Agency (NSA) Civil Liberties and Privacy Office (CLPO) as part of its responsibilities to enhance communications and transparency with the public and stakeholders. The Director of this Office is the primary advisor to the Director of NSA for civil liberties and privacy. Created in January 2014, the Office is also charged with ensuring that civil liberties and privacy protection considerations are integrated into NSA's mission activities. NSA published its first paper, April 16, 2014 and addressed NSA's Implementation of Foreign Intelligence Surveillance Act Section 702. The intent of this second report is to continue to build upon a common understanding and foundation for future discussions about NSA's civil liberties and privacy protections.

NSA's mission is to make the nation safer by providing policy makers and military commanders with timely foreign intelligence and by protecting national security information networks consistent with laws, regulations, and policies which frame these activities. NSA collects signals intelligence (SIGINT) for foreign intelligence and counterintelligence purposes based on requirements from the President, the national security team, federal departments and agencies, and their staffs through the National Intelligence Priorities Framework¹. NSA fulfills these national foreign intelligence requirements through the collection, processing, analysis, and dissemination of communications or other data, passed or accessible by radio, wire or other electronic means. NSA conducts its activities in accordance with several legal authorities. This report focuses on targeted SIGINT activities authorized by Executive Order 12333, as amended², and outlines the measures that are currently in place to protect civil liberties and privacy.

This report examines: (1) NSA's **Management Activities** that are generally applied throughout the Agency and (2) **Mission Safeguards** within the SIGINT mission when specifically conducting targeted³ SIGINT activities under E.O.12333. It documents the current civil liberties and privacy protections using the Fair Information Practice Principles (FIPPs)⁴ as a

¹ The National Intelligence Priorities Framework is the primary mechanism of the Director of National Intelligence (DNI) for communicating national intelligence priorities to guide Intelligence Community's (IC) collection and analytic activities.

² Executive Order No, 12333, "*United States Intelligence Activities*," as Amended (July 2008) ("E.O. 12333").

³ In the context of this paper, the phrase "targeted SIGINT activities" does not include "bulk" collection as defined in Presidential Policy Directive (PPD)-28. Footnote 5 states, in part, "References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)."

⁴ The FIPPs are the internationally recognized principles for assessing privacy impacts and are explicitly mentioned by the Privacy and Civil Liberties Oversight Board (PCLOB) Report on the Telephone Records Program Conducted



basis for analysis. This report also addresses questions such as: How is NSA organized and managed to protect civil liberties and privacy? What is already in place within NSA that promotes a culture where employees recognize and operate within the rule of law and policy? What current safeguards are in place which protect civil liberties and privacy within oversight and compliance regimes? What technical means and other activities does NSA perform to verify and give demonstrable assurance to the public and overseers that NSA is compliant with laws, regulations and procedures intended to protect the civil liberties and privacy of U.S. Persons?

The report focuses only on U.S. person protections. PPD-28 states that intelligence community elements shall establish policies and procedures that apply various principles for safeguarding personal information collected from signals intelligence activities equally to the personal information of all persons, regardless of nationality, to the maximum extent feasible consistent with national security. NSA is in the process of developing implementation instructions consistent with PPD-28.

Overall, NSA has multiple activities in place that provide civil liberties and privacy protections for six of the eight FIPPs (*Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, Accountability and Auditing*). Because NSA has a national security mission, the principles of *Transparency* and *Individual Participation* are not implemented in the same manner they are in organizations with a more public facing mission. Instead, NSA satisfies the *Transparency* principle through routine reporting to a variety of entities, including Congress, the Department of Defense (DOD), the Department of Justice (DOJ), the Office of the Director of National Intelligence (ODNI), the President's Intelligence Advisory Board (PIAB) and the Privacy, Civil Liberties Oversight Board (PCLOB). Recently, NSA declassified key historical documents, wrote and released new materials, and made its senior executives available in various public venues to help people in the United States and overseas understand its mission, core values, and value to the nation. Traditionally, the principle of *Individual Participation* in the context of FIPPs means the individual whose information is being collected knows about the collection and has the ability to contest the collection. Because there is a compelling need not to alert foreign intelligence targets that they are under surveillance, NSA can only offer *Individual Participation* in limited instances. The CLPO is engaged with academic community members and civil liberties and privacy advocates to identify potential additional activities that can be undertaken to strengthen the protections related to these two principles.

under Section 215 of the USA Patriot Act and on the operations of the Foreign Intelligence Surveillance Court dated January 23, 2014, E.O. 13636, Improving Critical Infrastructure Cyber security, The National Strategy for Trusted Identities in Cyberspace. These principles are rooted in the United States Department of Health, Education and Welfare's seminal 1973 report, "Records, Computers and the Rights of Citizens."



II. MANAGEMENT ACTIVITIES

NSA's Management Activities considers its structure and management controls that relate to civil liberties and privacy protections. At NSA, these management activities include four main components: (1) Organization and Management; (2) Policy; (3) Training and Education; and (4) Research. The Director of NSA provides strategic direction through consistent communications and routine strategic planning documents. This guidance is further tailored and implemented throughout NSA and has resulted in a work force that respects the law, understands the rules, complies with the rules, and is encouraged to report problems and concerns. All organizations and individuals throughout NSA consider protecting civil liberties and privacy to be part of their responsibility. Accountability further rests with each individual employee to maintain a culture with a strong history of protecting the privacy of U.S. Persons.

NSA takes several steps to ensure that each individual who joins its ranks understands from the first day on the job that civil liberties and privacy protection is a priority and a key personal responsibility. Civil liberties and privacy training is conducted as part of each employee's initial indoctrination, and employees complete additional mandatory training annually. When entering on duty, each employee takes an oath of office to the Constitution that speaks not simply to national security, but to protection of civil liberties and privacy. The importance of civil liberties and privacy protection is also articulated in Agency strategic plans, routine communications and policies.

NSA's current strategy emphasizes a specific goal of "Manifesting Principled Performance - Accomplishing our missions with a commitment to a principled and steadfast approach to performance through compliance, lawfulness, and protection of public trust must be paramount." NSA's published core values include specific calls for lawfulness, integrity and loyalty, all relating to how Agency employees and affiliates must protect privacy and civil liberties. It states in part:

*"We will adhere to the spirit and the letter of the Constitution and the laws and regulations of the United States. We will be loyal to the nation, the mission, and each other, weighing ideas solely on the merits and ensuring that decisions enjoy vigorous debate while being made, followed by unified implementation."*⁵

⁵ NSA Strategy, June 2010



(1) Organization and Management

NSA maintains a centralized policy and oversight management structure with decentralized execution of civil liberties and privacy protections using both staff and line organizations to create policies and programs, execute procedures and oversee these protections. NSA's line and staff organizations also provide input to and help manage routine and ad hoc responses to government entities including oversight by DOD, DOJ and ODNI, PCLOB, Congress, and, in the case of certain other authorities, the Courts.

During a 2013 inspection of NSA's intelligence and intelligence-related activities by the Office of the Assistant to the Secretary of Defense for Intelligence Oversight, NSA's Intelligence Oversight program was commended by inspectors as a model for other agencies to follow, stating that NSA's "program leads the other Defense Intelligence Components in fidelity and rigor" and that "NSA's best practices are ...numerous..."⁶

NSA invests considerable resources in support of protecting civil liberties and privacy. For 2013, its mission compliance program alone was supported by a budget of approximately \$30 million and over 300 personnel across the Agency.⁷

Agency Staff Organizations and Responsibilities

The Director of NSA has six major staff organizations responsible for some facets of civil liberties and privacy responsibilities: the Office of the Inspector General, the Office of General Counsel, the Office of the Director of Compliance, the Authorities Integration Group, the Associate Director for Policy and Records, and now the Civil Liberties and Privacy Office.

The Office of the Inspector General (OIG) – conducts intelligence oversight, inspections, audits and investigations that include reviewing effectiveness of mission safeguards that provide civil liberties and privacy protections. This Office also administers NSA's formal Whistleblower Protection Program.

The Office of General Counsel (OGC) – provides legal advice to NSA to ensure all activities conform to the law, including those designed to protect civil liberties and

⁶ "Report of Intelligence Oversight Inspection," Assistant to the Secretary of Defense/ Intelligence Oversight, 10 April 2013.

⁷ Per the United States House Permanent Select Committee on Intelligence (HPSCI) testimony provided by Mr. John C. "Chris" Inglis, former Deputy Director NSA, October 29, 2013.



privacy. Attorneys are also embedded within key mission elements to provide on-the-spot guidance and interpretation of laws to ensure NSA activities remain lawful.

The Office of the Director of Compliance (ODOC) — develops and directs the implementation of compliance strategies in partnership with each mission’s Directorate Compliance Component (DCC). Compliance activities are designed to achieve reasonable assurance that mission activities are consistent with laws, policies, and minimization procedures designed to protect U.S. Person privacy. NSA’s enterprise-wide compliance program is led by NSA’s Director of Compliance, a position required by statute. Drawn from industry and government best practices, the implementation of the program supports personnel, mission and technology to consistently operate within more than a dozen different regulatory regimes and under distinct external authorizations including, in this case, NSA’s targeted SIGINT activities under E.O. 12333.

The Authorities Integration Group (AIG) – provides a forum for integrating authority-related activities (changes, additions, deletions, etc.) across the NSA enterprise. By integrating five core elements – mission operations, technology, legal, policy, and compliance – the AIG makes fully-vetted mission authorities-related recommendations to NSA senior leaders.

Associate Directorate for Policy and Records (ADPR) – manages the process by which NSA-wide policies are developed, updated and adjudicated, including those related to civil liberties and privacy. ADPR currently acts as the Privacy Advocate. ADPR conducts Privacy Impact Assessments on administrative systems in conjunction with the Technology Directorate (TD). ADPR also is responsible for responding to Privacy Act and Freedom of Information Act (FOIA) requests.

The Civil Liberties and Privacy Office (CLPO) –focuses on systematically building civil liberties and privacy considerations into NSA mission activities in partnership with mission elements while maintaining mission effectiveness. The CLPO is also responsible for appropriately increasing transparency of NSA’s activities, and communicating with external parties on civil liberties and privacy matters to better understand concerns and share best practices. The CLPO reports directly to the Director, NSA and was established in January 2014 at the President’s direction.

Agency Line Organizations and Responsibilities:

In addition to centralized staff functions, NSA line organizations maintain overall accountability for ensuring that their personnel perform specific mission duties to conform with laws, policies and procedures. To help line managers, each of the major NSA mission organizations has established its own Directorate Compliance Component (DCC) to implement internal controls, including training and working aids, compliance monitoring and verification, and compliance improvement.



Several other organizations have compliance elements that support NSA's computers and information systems to make sure they are secure and operating properly. NSA's Technology Directorate (TD) Office of Compliance is responsible for identifying, assessing, tracking and mitigating compliance risks in NSA's mission systems, including U.S. Person privacy concerns. This organization manages the system compliance certification process, continuous compliance monitoring, technical compliance incident management, and also conducts training and awareness for technical personnel. Similarly, the Associate Directorate for Information Security and NSA's Chief Information Security Officer (CISO) are responsible for NSA information and system security risk management, which includes engineering secure solutions and ensuring that evolving threats do not impact NSA mission. Their focus is on strengthening information systems, building in security, and maintaining a desired system security posture and overall continual awareness of NSA networks' security posture.

These dedicated resources help identify and incorporate civil liberties and privacy protections specific to their areas of responsibilities. They also act as an internal check when mission elements consider new activities. Working with ODOC and the DCC's provides the CLPO with an additional opportunity to identify risks and mitigation strategies across the Agency.

(2) Policy

ODNI and DOD policies require NSA to have a civil liberties and privacy program. Prior to January 2014, these functions were managed by NSA operational mission elements, the OGC, and the Associate Director for Policy and Records. With the creation of the NSA CLPO, most of these responsibilities are being consolidated into the new organization to provide a more efficient, effective and coherent leadership focus on civil liberties and privacy. As part of its responsibilities, the CLPO will review whether existing civil liberties and privacy -related policies need to be updated or new policies need to be promulgated.

NSA maintains published policies and procedures that consider civil liberties and privacy as they relate to collection, use, retention, dissemination and destruction of SIGINT mission data. Existing NSA policies describe how the Agency implements specific laws, Executive Orders, and other external policy decisions designed to help protect the civil liberties and privacy of ordinary individuals. For example, the United States Signals Intelligence Directives (USSIDs) contain specific guidance to all personnel in the conduct of SIGINT activities, and include within USSID SP0018⁸ the principles for protecting U.S. Person privacy in accordance with U.S.

⁸ USSID SP0018 prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System are conducted in a manner that safeguards the Constitutional rights of U.S. Persons.



Attorney General approved minimization procedures. In response to PPD-28, NSA is working with the Intelligence Community and the Department of Defense to strengthen privacy protections for ordinary citizens of other nations.

(3) Training and Education

Training and education are also key components of an effective civil liberties and privacy program. As part of NSA's training and education program, each employee completes annual training on the Privacy Act and Intelligence Oversight, which includes guidance on compliance matters. In addition, NSA has a training program designed specifically for all personnel who perform SIGINT missions or have access to SIGINT data. These courses are designed to provide a mission appropriate understanding of applicable laws, regulations and policies associated with the protection of U.S. Person privacy.

Basic level privacy and compliance training is required for all employees. Employees who have access to SIGINT mission data complete a minimum of three training classes in privacy and compliance. Many employees must complete supplementary tailored training. Currently, NSA has several specialized courses in its oversight and compliance and privacy curricula. NSA reviews and updates its training curricula to reflect mission changes.

Specific job requirements, access to SIGINT mission data, and other criteria are used to determine additional training requirements. These requirements rise to advanced levels and/or mission-specific coursework based on employees' responsibilities and accesses. Validation of employee's knowledge of these topics takes place via formal testing and demonstrated knowledge checks. Even after successfully completing this training and testing, employees with access to SIGINT must review and update their understanding of legal, policy and oversight, and compliance requirements at least annually. Course work is verified through NSA's training systems. Access to SIGINT mission data is not granted to employees until their clearances, training records, and mission needs are validated.

New employees also receive on-the-job-training (OJT) which may consist of mission-specific checklists and standard operating procedures (SOPs) that guide daily work. For individuals with access to SIGINT mission data, this may include specific direction to implement tasking, advanced analytics and queries, cautions about sensitive sources and methods, and dissemination guidance and limitations.

Incorporating industry and government best practices into its compliance program, NSA established the Compliance Officer work role in 2010 to provide focus, dedicated education and training, and a development path for its compliance professionals. As part of this initiative, an increasing number of NSA compliance professionals have obtained one or more external professional certifications (e.g., the Certified Compliance and Ethics Professional and the Certified Information Privacy Manager).



(4) Research

Several ongoing research efforts within NSA support enhanced civil liberties and privacy protection and compliance capabilities. Successful results from this research can potentially be transferred to private industry to support the production of commercially available systems and devices with enhanced capability to protect civil liberties and privacy rights.

For example, NSA researchers are pursuing research into Private Information Retrieval (PIR). This area has the potential to improve data security and privacy protection by cryptographically preventing unauthorized users from accessing protected data. Researchers are also developing hardware and software that provide advanced security for data and system protection. More specifically, this research includes: using commercially available microprocessor technology to produce a secure and private computing environment; prototyping systems that validate authorized program execution, querying and auditing; developing tamper-proof hardware and software models; and developing secure failure techniques upon detection of adverse activity.

NSA is also part of a working group that is helping to develop a framework to support coordinated research in privacy-enhancing technologies, under the auspices of the President's Office of Science and Technology Policy.

In addition to these initiatives, CLPO is exploring other potential research opportunities to build upon existing civil liberties and privacy protections in NSA systems. These opportunities will initially focus on: (1) tools and techniques that may help suppress or mask data that constitutes personal information and (2) architectural and engineering techniques to build and augment privacy protections into cloud infrastructures, improve civil liberties and privacy protections when analyzing big data, and for rapid deployment of compliant analytics and tools.

III. MISSION SAFEGUARDS FOR TARGETED SIGINT ACTIVITIES UNDER E.O. 12333

Mission safeguards are the operational activities NSA puts in place to implement civil liberties and privacy protections. Safeguards include programs, procedures, and human-based and technical-based controls that, in combination with Management Activities, provide civil liberties and privacy protections. These protections related to NSA's SIGINT mission are primarily documented in the AG-approved procedures for the protection of U.S. Persons. Having the right policies and rules in place are critical, but it is equally important that they are technically implemented and adhered to within NSA's many complex tasking, collection,



processing and dissemination systems. That is the purpose of the mission safeguards. Most of the mission safeguards described in this section have been in place for several years and continue to evolve as longstanding procedures are reviewed and updated to meet current laws and policy guidelines.

NSA's mission compliance program includes initiatives to achieve reasonable assurance that NSA mission operations are verifiably conducted in accordance with the laws and policies that govern NSA's operations. Many control activities that provide civil liberties and privacy protections are documented by NSA in compliance standards.

System Certifications provide additional systems safeguards and support the privacy principle of Accountability and Auditing. NSA conducts two specific certifications that add technology embedded controls to verify that operational systems adhere to appropriate security and mission compliance requirements. These certifications are designed to help systems remain compliant in handling mission data and minimize the risk of malicious or inappropriate behavior. First, a senior official must authorize the operation of an information system after consideration of risks and mitigating security controls. Secondly, NSA has a specific organization that is responsible for reviewing and issuing compliance certification of designated NSA systems to provide reasonable assurance that the systems are operating in accordance with the legal and policy requirements concerning U.S. Person privacy.

The SIGINT Production Cycle

All SIGINT activities are based on appropriate legal authorities and are conducted for valid foreign intelligence purposes in response to National Intelligence Priorities. The SIGINT activities described in this section are governed by DOD regulation and Attorney General-approved procedures.

The CLPO reviewed the Mission Safeguards in place during each major segment of the SIGINT production cycle for targeted activities under E.O.12333 and used the FIPPs as a basis for analysis. The FIPPs provide a consistent framework for considering civil liberties and privacy risks and safeguards across activities and programs.

While there are a variety of ways to describe the intelligence cycle, this report focuses on the following major components: **Acquire, Analyze, Retain** and **Disseminate**.

ACQUIRE: (Includes Targeting, and Collection and Processing). NSA acquires data using a variety of methods. The processes described below focus on targeted SIGINT collection.

Targeting – Targeting is an overall term for the processes that cause SIGINT collection to occur in response to foreign intelligence requirements levied on NSA. A limited number of NSA personnel who are appropriately trained and authorized are permitted to introduce specific terms (such as a phone number or email address) into NSA collection systems as “selection



terms” for acquiring communications associated with specific foreign intelligence targets. These NSA personnel complete rigorous training on legal and policy constraints, and operate in accordance with focused mission assignments that are documented and controlled by a centralized mission management system. They perform pre-targeting research and two-person review and approval before entering any selection term into NSA’s collection systems, and conduct checks throughout the targeting process to review and validate that the acquired collection is responsive to the documented foreign intelligence need. In addition to initial approvals, selectors are reviewed by a supervisor or senior analyst on an annual basis.

CLPO Analysis: There is a civil liberties and privacy risk that the wrong entity may possibly be targeted. In order to mitigate this risk, NSA has the following **civil liberties and privacy safeguards** in place: (1) the system for targeting only allows properly trained individuals to use the systems – if training is incomplete or out of date, individuals will be denied access to these systems; (2) the targeting must be tied to one of the valid foreign intelligence requirements listed in the National Intelligence Priorities Framework; (3) a supervisor or senior analyst must review the targeting request before collection can begin; (4) the analyst reviews the resulting data after the selector has been targeted to ensure that it contains foreign intelligence on foreign targets; (5) in the event an incorrect entity is targeted, all selectors associated with that entity must be removed from targeting and, if the entity is a U.S. Person, the data must be deleted from NSA systems; and (6) the initial collection and subsequent decisions are all auditable activities. The existing civil liberties and privacy protections fall into the following FIPPs: Transparency (to overseers), Purpose Specification, and Accountability and Auditing.

Collection and Processing – Collection is the means by which NSA obtains SIGINT mission data on targets likely to produce foreign intelligence. Processing refers to the functions necessary to make that data usable for analysis and dissemination. NSA uses a variety of systems to perform collection and processing and takes many steps to assure accuracy and precision. For example, some systems have automated filtering to make the resultant collection more precise. As data is being collected and processed, it is generally not available for reporting purposes.

As data is collected and processed, steps are taken to document the authority under which the SIGINT data was obtained. NSA continues to modernize its architecture and adopt improved methods to provide that identification. Collection activities are approved and managed via several processes, with more scrutiny placed on those activities where there are greater civil liberties and privacy risks.

A combination of trained NSA personnel and use of automated tools provide continual quality assurance testing on collection and processing systems. This allows NSA to sustain collection of SIGINT mission data consistent with its authorities even as evolutionary changes in the world-wide communications infrastructures occur.



CLPO Analysis: The civil liberties and privacy risks associated with collecting SIGINT mission data are: (1) NSA could inadvertently collect data that is not related to the target; and (2) NSA could erroneously mark the data as being collected under one authority when it was actually collected under another authority. These potential errors could impact some methods used to control access to SIGINT mission data. In order to mitigate these risks, NSA has the following **civil liberties and privacy safeguards** in place which continue to be improved as NSA modernizes its systems: (1) NSA maintains an approval process before major new collection begins; (2) NSA has a documented process and automated tools for identifying situations when it receives data it should not have received and then deletes the data; (3) NSA marks the data to understand the source and authority of the data so that access restrictions can be applied; and (4) NSA is transitioning from older repositories to more modern systems, including the Intelligence Community cloud infrastructure, with the goal of improving access controls. The existing civil liberties and privacy protections fall into the three FIPPs categories: Data Minimization, Purpose Specification and Accountability and Auditing.

ANALYZE: Analysis is the means by which SIGINT mission data is used by NSA analysts to create foreign intelligence reports. Three activities must occur before an analyst gains access to SIGINT mission data: (1) Supervisors must approve an analyst to work on a particular mission. (2) supervisors must assign additional personnel to review queries that analysts have performed in NSA SIGINT repositories; and, (3) the analyst must complete required training. Formal and on-the-job training reinforce documented constraints and proper procedures for accessing and querying SIGINT mission data. NSA has a centralized system that documents this information and assists in technically enforcing access control.

In addition, the methods used to identify the source and authority for the data as applied during collection and processing may also be used by other systems to control access to the data. Once access to data has been granted, analysts are permitted to make specific types of queries and use approved analytic tools. Queries require justification, are logged and can be reviewed by each analyst's assigned post-query reviewer, and by compliance personnel who perform additional checks. Query results and analytical tools only present specific data the user is authorized to access.

Supervisors oversee all steps in the analysis process, including foreign language analysis, target knowledge documentation and the composition of foreign intelligence reports. The primary purpose of this oversight is quality control, but it also helps verify that analytic actions are performed in accordance with the rules. As reports are written, another series of checks is performed to ensure only reports that are responsive to customer requirements in the National Intelligence Priorities Framework are produced, that data has been appropriately evaluated, and that any U.S. Person information has been appropriately handled in accordance with procedures.



CLPO Analysis: In conducting analysis of SIGINT mission data, the following civil liberties and privacy risks exist: (1) the analyst could inappropriately access data for non-foreign intelligence purposes; (2) the written justification for the query may possibly be insufficient; (3) U.S. Person information may possibly be returned in a query; and (4) information from different data sets could be inappropriately brought together. To address these risks, NSA has instituted the following **civil liberties and privacy safeguards** : (1) NSA requires an analyst to document why certain queries are being performed thus providing a degree of transparency to the post-query reviewers; (2) NSA has developed job aids to help analysts determine when sensitive queries are permitted or prohibited; (3) NSA has extensive training and policies based on procedures that are approved by the Attorney General related to U.S. Person protections; and (4) queries that analysts have performed in NSA repositories are documented. These existing civil liberties and privacy protections fall into the following FIPPs: Transparency (to overseers), Purpose Specification, Data Minimization, and Accountability and Auditing.

RETAIN: E.O. 12333 and implementing policies and procedures govern how long NSA may keep SIGINT mission data.⁹ In general, targeted SIGINT mission data collected under E.O. 12333 that is unenciphered is retained for up to five years unless there is a determination that continued retention is in the national security interest of the United States.

NSA is legally obligated to retain some data for longer periods. For example, SIGINT records determined to be relevant to current litigation must be preserved and can only be used for litigation purposes. Holders of such records coordinate with the NSA Office of General Counsel and the appropriate management authority to ensure these records are preserved until they are no longer needed.

Data is required to be deleted from NSA systems if it is found to have been acquired without authorization. The process to accomplish such a removal of data has several manual and technical safeguards to help ensure accuracy and completeness.

CLPO Analysis: The civil liberties and privacy risks related to retention are that NSA (1) may possibly retain data that it is no longer authorized to retain; (2) may possibly fail to completely remove data the Agency was not authorized to acquire; and (3) may potentially lose data because of “spillage,” improper intentional disclosure, or malicious exfiltration. In order to mitigate these risks, NSA has the following **civil liberties and privacy safeguards**: (1) a clear policy stating the time period that SIGINT mission data may be retained in accordance with the appropriate legal authority; (2) ongoing improvements in how it marks its data to identify the source, authority and purpose of the collection; ; (3) ongoing improvements to mechanisms to identify, prioritize and inventory retained data; (4) technical mechanisms (or manual mechanisms in older systems) to remove the data in accordance with the retention limitations of the legal

⁹ PPD-28 sets new requirements for the retention of SIGINT data.



authority under which it was collected; and (5) improved data loss prevention measures. NSA is required to remove data it finds that was acquired without authorization and has a documented process for managing compliance issues and reports them as required by law and policy. These existing civil liberties and privacy protections fall into the following two FIPPs: Data Minimization, and Security.

DISSEMINATE: NSA has several ways to disseminate foreign intelligence information. Reports are provided for foreign intelligence purposes, as documented in the National Intelligence Priorities Framework and are distributed based on customer mission profiles to personnel with appropriate security clearances. When SIGINT reports contain extremely sensitive information, an additional pre-publication review occurs that further limits the release of information.

To ensure reports answer valid foreign intelligence requirements, every SIGINT report must include a citation that links it to at least one valid requirement. NSA takes several steps to verify compliance with reporting requirements. These include reviews by senior personnel and supervisors, and some technical checks in software used to edit most reports. One such technical check provides reasonable assurance that reports proposed for dissemination are based only on authorized SIGINT mission data.

While these review efforts are aimed at compliance and quality control, they also help ensure that civil liberties and privacy is protected in two ways. (1) In general, U.S. Person identity information is included in SIGINT reports only if (a) it is necessary to understand the foreign intelligence information or assess its importance, and (b) a determination has been made by the SIGINT approval authority that the recipient has a need for the identity for the performance of official duties. For example, if the SIGINT data describes an individual with U.S. citizenship mentioned by name, the report may not reveal the name of the person. Rather, the phrase “named U.S. Person” will be substituted. NSA follows a strict process for revealing the true identities of U.S. Persons within a report only to properly cleared personnel requiring access to the information to perform his or her official duties.¹⁰ (2) SIGINT reports are based on valid foreign intelligence requirements and no extraneous personal data is included in the reports. NSA policy states that personnel should not include information in reports just because it is available, and they must also complete checklists that assist in reducing the likelihood that personal information is inappropriately included in a report. This specific privacy protection applies to U.S. and non-U.S. Persons alike.

¹⁰ Following applicable guidelines, if SIGINT data contains evidence of a crime, U.S. Person identities may be shared with appropriate law enforcement entities, such as the FBI.



CLPO Analysis: The risks associated with dissemination are that (1) NSA could inappropriately share information that does not have a foreign intelligence purpose, or is based on data that is required to be removed; or (2) NSA may possibly disseminate more information than is relevant to foreign intelligence. In order to mitigate these risks, NSA has the following **civil liberties and privacy safeguards** for disseminating foreign intelligence reports: (1) NSA uses software that perform limited technical checks for most reports as they are prepared and edited; (2) NSA senior reporters perform quality control and legal and policy compliance reviews of reports, providing feedback and directing necessary corrections before a report can be disseminated; (3) procedures are used to protect the identity of U.S. Persons and not reveal them unless (a) it is required to understand or assess its importance of the foreign intelligence information; and (b) a designated official authorizes when and how identities may be revealed in keeping with approved procedures; and (4) source verification occurs to ensure reporting is based only on authorized data. The existing civil liberties and privacy protections fall into the following FIPPs: Use Limitations, Data Minimization, and Accountability and Auditing.

IV. CONCLUSION

In January 2014, NSA established a CLPO, in part to help provide expert advice to the Director of NSA, increase internal oversight of NSA's civil liberties and privacy related activities and develop measures to further strengthen NSA's privacy protections. Part of the aim of this office is to facilitate communications between NSA and the public and others about its mission operations and civil liberties and privacy protections. Recent public and congressional interest, independent oversight bodies, and executive branch policy development has brought many of these issues to the fore. We look forward to continue to engage with the public about these important issues. In this report, CLPO documented NSA's multiple activities that provide civil liberties and privacy protections for six of the eight FIPPs that are underpinned by its management activities, documented compliance program, and investments in people, training, tools and technology. Because NSA has a national security mission, the principles of *Transparency* and *Individual Participation* are not implemented in the same manner they are in organizations with a more public facing mission. The CLPO will continue to engage with academic community members and civil liberties and privacy advocates to identify potential additional activities that NSA can undertake to strengthen the protections related to these two principles.

Similarly, the CLPO will continue to develop and mature mechanisms to conduct civil liberties and privacy assessments and report to overseers and citizens. NSA is interested in public feedback on this report and solicits your ideas for additional areas for exploration. Please contact us via e-mail at CivilLibertiesPrivacy@nsa.gov.



(U) The Fair Information Practice Principles (FIPPs)¹¹

The Fair Information Practice Principles (FIPPs) are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy. The FIPPs are:

- **Transparency:** Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **Individual Participation:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s).
- **Use Limitation:** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity:** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security:** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Universal application of FIPPs provides the basis for confidence and trust in online transactions.

¹¹ From "The National Strategy for Trusted Identities in Cyberspace."