NSA Civil Liberties and Privacy Office

Review of U.S. Person Privacy Protections in the Production and Dissemination of Serialized Intelligence Reports Derived from Signals Intelligence Acquired Pursuant to Title I and Section 702 of the Foreign Intelligence Surveillance Act

Rebecca J. Richards
Civil Liberties and Privacy Office

11 October 2017

I. Executive Summary

This report examines the procedures and practices used by the National Security Agency (NSA) to protect U.S. person information when producing and disseminating serialized intelligence reports derived from signals intelligence (SIGINT) acquired pursuant to Title I and Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA).[1] NSA's Civil Liberties and Privacy Office (CLPO) prepared this report at the request of the Director of National Intelligence (DNI) and in coordination with the DNI's Civil Liberties, Privacy, and Transparency Officer. The Director of CLPO is the primary policy advisor to the Director of NSA and senior leadership on all matters of civil liberties and privacy and is charged with ensuring that privacy protections are integrated into NSA activities. This report reflects a commitment to provide the public and stakeholders with greater transparency into NSA's activities and U.S. person privacy and civil liberties safeguards in the process of disseminating intelligence reports.

As directed by applicable law and policy, NSA collects, processes, analyzes, produces, and disseminates SIGINT information and data for foreign intelligence and counterintelligence purposes, to include support to military operations and force protection. NSA conducts this foreign intelligence mission in response to intelligence requirements from the President, the National Security Council, federal departments and agencies, and their staffs through the National Intelligence Priorities Framework (NIPF). NSA fulfills these national-level requirements through the collection, processing, and analysis of SIGINT derived from electronic signals and systems used by foreign intelligence targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.

In preparing this report, CLPO reviewed (1) applicable privacy protections, as outlined in Attorney General and FISC-approved minimization procedures that govern the dissemination of U.S. person information acquired pursuant to Title I and Section 702 of FISA in serialized intelligence reports; (2) NSA procedures, practices, training, and oversight and compliance activities associated with the dissemination of serialized intelligence reports involving FISA-acquired U.S. person information; and (3) NSA serialized intelligence reports issued over a one-month period that contained FISA-acquired U.S. person information. CLPO considered the Fair Information Practice Principles as a guidepost for understanding whether NSA's practices and procedures governing the dissemination of FISA-acquired information adequately protect U.S. persons' privacy and civil liberties.

[1] This report is limited to an examination of the procedures and practices used to protect FISA-acquired U.S. person information disseminated in *serialized intelligence reports*. This report does not examine other means of dissemination. For purposes of this report, the term "dissemination" should be interpreted as a reference to serialized intelligence reporting, unless otherwise indicated.

As detailed in this report, CLPO's review of NSA's procedures and practices with respect to the dissemination of FISA-acquired information concerning U.S. persons found:

- NSA minimization procedures limit the dissemination of U.S. person information. In general, these procedures limit the dissemination of U.S. person information to those instances where the recipient has a "need to know" and the identity of the U.S. person is necessary to understand the foreign intelligence information or assess its importance. NSA has developed policies and procedures based on the minimization procedures to provide further guidance to NSA personnel in the execution of their duties.
- NSA requires that draft disseminations of U.S. person information be reviewed by a senior analyst prior to release. This ensures that decision making regarding dissemination does not rest with a single individual.
- NSA tailors dissemination by, for example, limiting the number of authorized recipients of intelligence reports, and/or masking U.S. person information contained in the report, or a mixture of both, depending on the nature of the intelligence reports.
- NSA has a process for reviewing on a routine basis dissemination policies for the proactive release of U.S. person information to ensure the policies are effective and appropriate.
- NSA has a well-developed process by which it records and approves the dissemination of masked and unmasked U.S. person information to authorized recipients, allowing the Agency to be transparent and accountable to its overseers.
- Consistent with prior oversight reviews, CLPO discovered no intentional violations of NSA's procedures governing the handling and dissemination of U.S. person information.
- NSA provides extensive and effective training—both classroom and on the job training—for all personnel involved in the process of disseminating SIGINT.
- Compliance and oversight activities are carried out internally by NSA's Compliance Group, Office of the General Counsel (OGC), Office of Inspector General, and CLPO, as well as externally by ODNI, Department of Justice (DOJ), Department of Defense (DOD), Congress, and the FISC.

NSA's SIGINT reports include appropriate handling guidance and caveats, including specific information about FISA-acquired information, to ensure that recipients fully understand restrictions that apply to the use of the information and further dissemination. As is the case for intelligence information disseminated by other elements of the Intelligence Community, CLPO notes that it is the responsibility of the recipients of NSA's SIGINT reporting to ensure compliance with any and all applicable handling caveats and other guidance, to include security classification controls and use restrictions.

II. Scope of Review

Protecting U.S. person privacy is foundational to NSA's mission and begins long before a decision is made to mask or unmask U.S. person information in a particular report. In preparing this report, CLPO reviewed applicable privacy protections governing the dissemination of U.S. person information acquired pursuant to Title I and Section 702 of FISA. CLPO brought together a cross-functional team with representatives from the Directorates of Operations,

Engagement and Policy, and Capabilities. The team also included representatives from NSA's Compliance Group and the OGC. This allowed CLPO to conduct a comprehensive review, drawing on expertise from across the NSA enterprise.

As part of the review, CLPO examined NSA serialized reports containing U.S. person information acquired pursuant to Title I or Section 702 of FISA issued over a one-month period from June 1, 2017 to June 30, 2017. CLPO reviewed reporting that contained both masked and unmasked U.S. person information, associated unmasking requests, and any corresponding customer justifications for such requests, along with NSA's internal process for responding to and documenting those requests.

For purposes of this review, CLPO limited its inquiry to the procedures and practices used to protect FISA-acquired U.S. person information disseminated in *serialized intelligence reports*, and did not examine other means of dissemination. Thus, the term "dissemination," as used in this report, should be interpreted as a reference to serialized intelligence reporting, unless otherwise indicated.

III. Background: Intelligence Collection, Use, and Dissemination at NSA

Privacy protections for U.S. persons[2] are incorporated throughout the SIGINT Cycle from the decision to collect through use, retention, and dissemination. NSA's SIGINT mission is to make the nation safer by providing policy makers and military commanders with timely foreign intelligence information. NSA collects SIGINT for foreign intelligence and counterintelligence purposes, to include support to military operations and force protection, based on requirements from the President, the National Security Council, federal departments and agencies, and their staffs through the NIPF. The NIPF is a high level set of priorities that are further translated into intelligence needs. The U.S. Intelligence Community reviews intelligence needs and determines which intelligence discipline is best suited to answer the particular need. In some cases it may be SIGINT and in others it may be open source, human intelligence, or another type of intelligence. Once the intelligence need is levied on the SIGINT system, NSA reviews the intelligence need and determines how best to acquire foreign intelligence and under what authority.

NSA's SIGINT mission is strictly regulated and conducted in conformity with applicable law and policy. This includes NSA's acquisition of communications under circumstances in which a U.S. person may possess a reasonable expectation of privacy under the Fourth Amendment to the U.S. Constitution. In particular, FISA regulates certain types of intelligence collection activities, including those that occur with compelled assistance from electronic communication service providers.

[2] The definition of U.S. person under FISA means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power as defined in subsection (a)(1), (2), or (3) [of Section 1801 of Title 50].

In general, before NSA may conduct electronic surveillance pursuant to Title I of FISA, the Foreign Intelligence Surveillance Court (FISC) must issue an order after making a probable cause finding, based upon a factual statement in the government's application, that (1) the target is a foreign power or an agent of a foreign power, as defined by FISA and (2) each of the facilities or places at which the electronic surveillance is directed is being used by or is about to be used by a foreign power or agent of a foreign power. In addition to meeting the probable cause standard, the government's application must meet other requirements laid out in FISA.[3] This is a targeted collection of foreign intelligence.

Section 702 permits the government to acquire foreign intelligence information through the targeting of non-U.S. persons located outside the United States. Section 702 acquisitions must be intended to acquire foreign intelligence information related to a certification executed by the Attorney General (AG) and the DNI. Any such certification must be reviewed and approved annually by the FISC. The government's acquisition of communications under its Section 702 authority thus takes place pursuant to judicial review and with the knowledge of the service providers, who are legally compelled to provide assistance. Similar to electronic surveillance conducted pursuant to Title I of FISA, acquisitions under Section 702 involve targeted collection of foreign intelligence.

Minimization Procedures

Minimization procedures regulate NSA's processing of information acquired pursuant to Title I and Section 702 of FISA. As defined in 50 U.S.C. §1801(h), minimization procedures are adopted by the AG and approved by the FISC and must be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

NSA has standard minimization procedures (SMPs) that govern the processing of information acquired pursuant to Title I and Section 702 of FISA. As required by FISA, each set of SMPs has been adopted by the AG and approved by the FISC. These procedures are designed to protect the privacy of U.S. persons. These SMPs are publicly available in redacted form in the appendix to this report.

NSA has developed policies and procedures based on the minimization procedures to provide further guidance to NSA personnel in the execution of their duties. An example of this is Annex A of United States Signals Intelligence Directive (USSID) SP0018, "Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Person."

If NSA wants to share (i.e., disseminate) information collected lawfully pursuant to FISA, the agency must do so in a manner consistent with its minimization procedures. Generally speaking,

[3] 50 U.S.C. §§ 1804(a) and 1823(a)

dissemination refers to the sharing of minimized information that has been evaluated for foreign intelligence value. Dissemination of the identity of a United States person is permitted when at least one of the following criteria is met:

> (1) The U. S. person has consented to dissemination or the information of or concerning the United States person is available publicly.
> (2) The identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch.
> (3) The communication or information indicates that the United States person may be: (A) an agent of a foreign power; (B) a foreign power as defined in Section 101(a)(4) or (6) of FISA; (C) residing outside the United States and holding an official position in the government or military forces of a foreign power; (D) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or (E) acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material.
> (4) The communication or information indicates that the United States person may be the target of intelligence activities of a foreign power.
> (5) The communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information, but only after the agency that originated the information certifies that it is properly classified.
> (6) The communication or information indicates that the United States person may be engaging in international terrorist activities.
> (7) The acquisition of the United States person's communication was authorized by a court order issued pursuant to FISA Section 105 and the communication may relate to the foreign intelligence purpose of the surveillance.
> (8) The communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with FISA Section 106(b) and crimes reporting procedures approved by the Secretary of Defense and the AG.[4]

Even if one of these circumstances exists, the SMPs restrict dissemination to those individuals or customers with a "need to know." "Need to know" criteria are derived from NSA's Title I and 702 SMPs statement that, the dissemination of intelligence based on communications of or concerning a United States person may be made to a recipient requiring the identity of such person for the performance of official duties.

[4]Annex A of USSID SP0018 Section 6b. (Standard Minimization Procedures for Collection Acquired Pursuant to Title I of FISA). These same eight criteria, with minor modifications, are also used with respect to collection acquired pursuant to Section 702. *See* NSA Section 702 Minimization Procedures Section 6(b).

Dissemination Practices and SIGINT Production under FISA

NSA generates intelligence reports only when the information meets one or more specific intelligence requirements, regardless of whether the proposed report contains U.S. person information. NSA disseminates SIGINT to provide U.S. policymakers, military customers, and other authorized users of intelligence with timely, reliable foreign intelligence information. While dissemination derived from Title I or Section 702 of FISA can occur either in writing or verbally, the practice of NSA is to document such disseminations for auditing and oversight purposes. Each report must contain foreign intelligence or counterintelligence information that responds to stated customer requirements. A single serialized report may contain information obtained pursuant to more than one legal authority, but the dissemination rules associated with U.S. persons remain consistent across authorities.[5]

The subject matter of an intelligence report containing FISA-acquired U.S. person information drives the distribution (i.e., list of authorized recipients), the decisions about the extent to which U.S. person information pertaining to the subject matter may or should be shared, and the dissemination controls, handling instructions and caveats that will be applied to the report. Each report reminds the recipient that the information is for intelligence purposes only and may include additional directions related to who else within an agency or organization is or is not allowed to see or use the information.

As the sensitivity of the subject matter increases, NSA implements procedures to restrict distribution by organization, title, or name. Internal NSA policies outline the criteria and procedures to achieve this approach to SIGINT production. An NSA serialized report that is based on information acquired under FISA authorities includes caveats and handing instructions that explicitly tell authorized recipients what they can and cannot do with the information contained in the report. For Section 702, NSA tracks the total number of disseminated serialized reports derived from this authority that contain U.S. person identities. This metric is included in the ODNI's Annual Statistical Transparency Report.

"Masking" is a procedure contemplated by the applicable minimization procedures that provides additional privacy protection for FISA-acquired U.S. person information disseminated in intelligence reports. A reference to a U.S. person is "masked" when the specific identifying information about that person is not included. NSA policy allows, in certain circumstances, for U.S. person information to be unmasked and to be disclosed by name, title, and/or context. In general, when U.S. person information is referenced it is masked, often because only a subset of the authorized recipients have a "need to know" to perform their official duties. If the U.S. identity is masked to protect the privacy of the individual or entity, it will be referenced using a generic term, such as "a named U.S. company" or "a named U.S. person." NSA provides its analysts with comprehensive guidance on how to properly reference masked U.S. identities in SIGINT. This guidance emphasizes the need to avoid contextual identification, which occurs if

[5] The process and procedures described in this report relate specifically to Title I and Section 702 of FISA. Similar procedures exist for other authorities, but were not explicitly reviewed for this report.

the identity of a U.S. person is masked, but enough other pertinent details are included that the authorized recipient can identify the U.S. person from the context.

NSA also responds to customer initiated, post-publication "identity release" requests to approve the unmasking and dissemination of U.S. person identity information that was originally masked in a serialized report. Recipients can request that NSA provide the identity of a masked U.S. person referenced in a serialized SIGINT report if the recipient has a legitimate need to know the identity and has the appropriate security clearances, and if the dissemination would be consistent with NSA's minimization procedures (e.g., the identity is necessary to understand foreign intelligence or counter intelligence information or assess its importance.) Requesters must include a justification for access to U.S. person information.

Pursuant to NSA's internal policies, and subsequent delegations made by the Director NSA (DIRNSA), there are no more than 20 individuals serving in 12 positions across the Agency who possess the authority to approve unmasking requests. The circumstances under which each of these individuals may approve an unmasking request varies based on the U.S. person identity in question and the facts surrounding the request. NSA has developed technology to allow it to document each approved release of U.S. person information to ensure that the Agency maintains appropriate records and provides accountability to both internal and external oversight bodies.

In addition to post publication release, NSA analysts may proactively request approval for dissemination of the U.S. person identity by name, title, or context in a serialized report. For example, if a U.S. person is engaging in international terrorist activities, NSA may proactively name the individual in a disseminated intelligence report. Proactive release of unmasked U.S. person information is a strictly controlled activity, and decision authority at NSA is limited to a small number of individuals who undergo comprehensive training. Subject matter experts on the protection of U.S. persons coordinate on the requests as required. A decision to approve dissemination does not constitute targeting authority and does not permit any collection of a U.S. person's communications.

The dissemination of intelligence information that refers to members of the U.S. Congress or their staffs is restricted under what are known as the "Gates Procedures." The current version of the Gates Procedures, dated 19 January 2017, is contained in Annex A to Intelligence Community Directive No.112.[6]

IV. Training

NSA analysts undergo both formal training and rigorous on-the-job training before being granted authority to disseminate SIGINT. NSA's National Cryptologic School (NCS) oversees a reporting curriculum that trains students to produce timely, accurate, SIGINT reports in a variety of dissemination formats in response to customer requirements and in accordance with NSA

[6] These are publicly available at www.icontherecord.gov.

policies. To have the authority to release a product, additional mandatory training is required. The reporting curriculum:

- ensures mastery of the approved mechanisms for SIGINT dissemination; and
- provides extensive guidance on reporting issues related to the dissemination of U.S. identities in accordance with minimization procedures and applicable laws and policies.

The NCS also has a robust compliance curriculum, and all NSA personnel are required to be familiar with and agree to uphold the laws, policies, procedures, and regulations that govern NSA mission activities and implement privacy protections for U.S. persons. Before gaining access to any unevaluated, unminimized ("raw") NSA SIGINT, an analyst must complete training tailored to the legal and policy guidelines that govern the handling and use of the data, based on the authority under which it was collected. These mandatory annual requirements include scenario-based training, required reading, and a final competency test. The analyst must pass the test in order to be granted or to maintain access to raw SIGINT. Furthermore, if a compliance incident involves a mistake or misunderstanding of relevant policies, corrective action is taken. For example, the analyst may be re-trained or the analyst's access to raw SIGINT may be revoked.

V. SIGINT Oversight and Compliance

NSA has rigorous oversight and compliance programs, both internally and externally, to ensure that SIGINT activities comply with the laws, regulations, minimization procedures, and policies governing those activities in a manner that protects the privacy interests of U.S. persons. All SIGINT disseminations must satisfy the standards for effective oversight: accountability, defensibility, repeatability, and retrievability.

Internal Oversight:

NSA has an enterprise-wide compliance program, led by NSA's Director of Compliance, a position required by law. As part of this structure, NSA has compliance elements throughout its various organizations. Intelligence Oversight Officers provide day-to-day oversight and compliance guidance for SIGINT activities, advising local management on problems, risks, and mitigation procedures. On an enterprise-wide level, NSA has established an Authorities Integration Group to ensure that mission authorities are managed effectively and with precision. The OGC, Office of the Inspector General (OIG), and CLPO also play critical roles in ensuring that NSA operates in accordance with the rules that govern SIGINT activities, as established in various statutes, executive orders, directives, and policies. For example, in 2014, CLPO issued a public report that examines the existing civil liberties and privacy protections built into the process by which NSA obtains, uses, shares, and retains communications of foreign intelligence value pursuant to Section 702 of the FISA.

Additionally, each individual NSA analyst has a responsibility to ensure that his or her individual professional activities are similarly compliant. Specifically, this responsibility includes recognizing and reporting any situations in which he or she may have violated applicable laws or procedures. NSA reports potential compliance incidents promptly to its external overseers and, when appropriate, provides supplemental reports when investigations have been completed. Reportable activity includes, for example, the mishandling of U.S. person information, access to raw SIGINT data without proper authority, and the improper dissemination/handling of SIGINT. When issues of non-compliance arise regarding the way in which NSA carries out FISC-approved collection, NSA takes corrective action and, in parallel, in accordance with the FISC rules of procedure and applicable law, reports such incidents to DOJ and as appropriate, ODNI for further reporting to the FISC and Congress, as appropriate.

External Oversight:

NSA is highly regulated and subject to a spectrum of oversight from all branches of government as a matter of law, policy, and practice. For example, DOJ and ODNI representatives regularly conduct external oversight reviews of NSA's dissemination of information acquired pursuant to Section 702 of FISA. These reviews involve an examination of NSA's compliance with the dissemination provisions of its standard minimization procedures, including NSA's decisions to release U.S. person identities. DOJ and ODNI perform a granular review of disseminated reporting that includes U.S. person information. NSA receives feedback from the DOJ and ODNI team and incorporates this information into formal and informal training for analysts.

The FISC's Rules of Procedure require the government to inform the Court in cases where the government realizes that it has made any material misstatements or omissions to the Court. The government must also report to the FISC noncompliance with FISC orders or FISC-approved minimization procedures.

NSA provides transparency regarding its Section 702-related activities to external oversight bodies (Congress, DOJ, ODNI, DoD, the President's Intelligence Oversight Board and the FISC) through regular briefings, court filings, and incident reporting, and ODNI's Annual Statistical Transparency Report. Agencies that collect information under Section 702 report annually to the House and Senate intelligence and judiciary committees, as well as to the FISC, AG, and DNI, about the number of times U.S. person identities were disseminated, and the number of U.S. person identities subsequently unmasked. The FISA Amendments Act of 2008 also requires that the AG report semi-annually to the congressional intelligence and judiciary committees on numerous aspects of the 702 program, including incidents of non-compliance with applicable procedures, directives, and guidance.

In addition, the Privacy and Civil Liberties Oversight Board (PCLOB) conducted an extensive review of privacy concerns regarding the Section 702 program and issued a public report on its findings in 2014. The PCLOB made a number of recommendations to the government intended to enhance privacy safeguards associated with the program. All of those recommendations have been or are being implemented in full.

VI. CLPO Review of Disseminated Reports

As part of the CLPO review of one month of Title I and Section 702 FISA-related reports that had U.S. person information included, conducted to inform this report, CLPO found that:

- The disseminated reports were all in response to one or more specific identifiable foreign intelligence needs.
- U.S. person information in disseminated reports was proactively released because it met one of the eight criteria for dissemination.
- NSA masked U.S. person information appropriately in disseminated reports.
- Recipients requested masked USP identities to be unmasked in less than half of the intelligence reports.
- The various mechanisms for disseminating U.S. person identity information to include both proactive release and unmasking appeared reasonable.
- The criteria for dissemination in the proactive release were reasonable, particularly given the routine review of the approvals.
- The process for routine review of policies related to both proactive and post publication releases is important for ensuring both customer needs and U.S. person privacy are being addressed.
- There were no indications of intentional violation of NSA's procedures governing the handling and dissemination of U.S. person information.
- On occasion the basis for the unmasking approval was not compiled in a single repository, but upon further discussions with subject matter experts there was sufficient information to understand why a request was approved for unmasking.

VII. Summary of Findings

NSA provides intelligence support in accordance with the NIPF that responds to both strategic and tactical requirements that are based on customer needs and the identification of information gaps. NSA serves a broad range of customers—from military commanders on the ground to executive-level policymakers—by tailoring the way it disseminates SIGINT products, so that many different types of intelligence consumers can benefit from uniquely valuable insights while fully protecting U.S. person privacy. This tailoring may occur through limiting the number of individuals and/or agencies that receive a particular product and/or by masking U.S. person identities and only providing those U.S. identities upon request.

The Fair Information Practice Principles[7] are a broadly recognized set of principles that can be used for assessing privacy risks and identifying mitigation strategies. While not all of principles are directly applicable in the national security context, CLPO used the relevant principles as a guidepost for understanding whether NSA's practices and procedures adequately protect U.S.

[7] The FIPPS are a broadly recognized set of principles for assessing privacy impacts. For example, they have been incorporated into Executive Order 13636, Improving Critical Infrastructure Cybersecurity and the National Strategy for Trusted Identities in Cyberspace. These principles are rooted in the U.S. Department of Health, Education and Welfare's seminal 1973 report, "Records, Computers, and the rights of Citizens." The FIPPs have been implemented in the Privacy Act of 1974, with certain exemptions, including ones that apply to certain national security and law enforcement activities.

person's privacy and civil liberties. CLPO considered the following principles: Transparency, Use Limitation, Data Minimization, Security, Quality and Integrity, Accountability and Auditing. Purpose specification, which relates to the purposes for which information were initially collected, and Individual Participation, which relates to involving the individual in the initial collection, were not considered directly relevant.

The Transparency principle states that organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII), or information about people. CLPO determined that there is appropriate transparency regarding the privacy protections surrounding the dissemination of U.S. person information, as the minimization procedures for Title I and Section 702 have been released almost entirely unredacted. In addition, CLPO has provided a 2014 report on Section 702, as has the PCLOB. In the interest of additional transparency, CLPO issued this report at the unclassified level.

The principle of Data Minimization states that organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose. The steps taken from the outset of the SIGINT production process to determine what U.S. person information can and should be disseminated directly demonstrate how this principle is met, as do NSA's procedures and documentation requirements for the proactive and post-publication release of U.S. identities in disseminated SIGINT.

The principle of Use Limitation provides that organizations should use PII solely for the purposes specified in the notice. In other words, the sharing of PII should be for a purpose compatible with the purpose for which it was collected. NSA's SIGINT production process directly reflects this principle. Analysts consider what information is directly relevant to the NIPF priorities and provide only information that is necessary and relevant to understand the foreign intelligence. The use of special handling and FISA notifications on every disseminated report offers an additional form of notice to users outside NSA that additional considerations must be taken before further using or disseminating the information.

The principle of Data Quality and Integrity provides that organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely and complete. As SIGINT is prepared for dissemination, analysts review pertinent information, which is reviewed through a quality control process to ensure a final product that is accurate, relevant, timely and complete. SIGINT products also include information about the validity and reliability of sources, allowing customers to better assess the nature of the reporting.

The principle of Security states that 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. NSA has technical systems

in place for the issuance of disseminated reports allowing it to know who has received a report and who has requested unmasking of an identity in a report.

The principle of Accountability and Auditing states that organization should be accountable for complying with these principles, providing training to all employees and contractors who use personally identifiable information, auditing the actual use of personally identifiable information to demonstrate compliance with these principles and all applicable privacy protections. NSA has an extensive internal compliance and external oversight function for FISA including a tracking system for disseminations related to U.S. person information.

VIII. Conclusion

CLPO finds that NSA has developed a sophisticated approach to protecting U.S. person privacy in the dissemination of SIGINT collected pursuant to Title I or Section 702 of FISA. The process of masking and unmasking is successfully allowing NSA to disseminate necessary and relevant foreign intelligence to a broad set of customers without negatively impacting U.S. person privacy. The criteria for dissemination in the proactive release were reasonable, particularly given the routine review. The reviews should be continued to ensure the policies remain accurate and effective.

Consistent with other findings, this review found no incidents of intentional non-compliance and found that the NSA's practices and procedures adequately protect U.S. person's privacy and civil liberties.

NSA's SIGINT reports include appropriate handling guidance and caveats to ensure that recipients fully understand restrictions that apply to the use of the information and further dissemination. As is the case for intelligence information disseminated by other elements of the Intelligence Community, CLPO notes that it is the responsibility of the recipients of NSA's SIGINT reporting to ensure compliance with any and all applicable handling caveats and other guidance, to include security classification controls and use restrictions.

Appendix I
Redacted United States Signals Intelligence Directive (USSID) SP0018, "Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Person" and its annexes, which includes the Redacted Title I of FISA Standard Minimization Procedures in Annex A

https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf

Appendix II

Redacted Section 702 FISA Standard Minimization Procedures

https://www.dni.gov/files/documents/icotr/5117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf