NSA Civil Liberties and Privacy Office

Transparency Report:
THE USA FREEDOM Act Business Records FISA Implementation

15 January 2016

I. Introduction: Assessing the Privacy Impact of the USA FREEDOM Act

The National Security Agency's Civil Liberties and Privacy Office (CLPO)[1] conducted a civil liberties and privacy impact assessment examining how the National Security Agency (NSA) is implementing the changes effected by the USA FREEDOM Act to the telephone metadata program that the Agency had conducted pursuant to the "Business Records" provision in Section 215 of the USA PATRIOT Act. The latter section amended the Foreign Intelligence Surveillance Act (FISA) and authorized NSA to collect and analyze certain telephone metadata. The USA FREEDOM Act, which was enacted in June 2015 and became effective on November 29, 2015, made significant changes to NSA's authority in this regard. This report summarizes CLPO's assessment and its underlying analysis of how this new authority is being implemented.

Civil liberties and privacy impact assessments inform NSA's decision making. They identify potential civil liberties and privacy (CLP) impacts, describe and document CLP safeguards applied to a given activity, and support increased transparency within NSA, to external overseers, and, as appropriate, to the public. As part of the implementation of the Principles of Intelligence Transparency for the Intelligence Community (IC), the NSA CLPO is publishing this unclassified report.

Assessments apply the eight Fair Information Practice Principles (FIPPs, Appendix A) and serve as the basis for identifying civil liberties and privacy impacts. The FIPPs are the standard by which the government and many in the private sector assess privacy impacts and develop mitigations. The FIPPs also establish a basis for identifying and mitigating civil liberties impacts by providing a framework to identify features of an activity that may impact an individual without a justifiable purpose, be used against an individual's interest without sufficient limitation, or negatively affect an individual without accountability or a means of redress, among others.

NSA's goal under the USA FREEDOM Act remains the same as that under its predecessor program: to collect, analyze, and disseminate foreign intelligence information about international terrorist threats. The government has strengthened privacy safeguards by, among other things, ending the collection of telephone metadata in bulk and having telecommunications providers, pursuant to court orders, hold and query the data.

NSA's implementation of the USA FREEDOM Act has been and continues to be a complex effort that requires the active participation of multiple offices across NSA with technical, legal, civil liberties and privacy, and compliance expertise. NSA's Civil Liberties and Privacy Office has played and continues to play an integral part in this process, ensuring that civil liberties and privacy risks and impacts are thoroughly assessed (and, as appropriate, mitigated) as the Agency developed and continues to refine the technical architecture needed to support the new authority.

[1] NSA's Civil Liberties and Privacy Office (CLPO) was established in 2014. CLPO is responsible to the Director of the National Security Agency for ensuring that civil liberties and privacy protections are integrated into policies, plans, procedures, technology, programs and activities across the NSA/CSS global cryptologic enterprise.

This report first presents a definition of key terms and then provides an overview of the process for obtaining telephone metadata pursuant to the USA FREEDOM Act. The report concludes by providing a detailed privacy and civil liberties analysis of the metadata procedures against the FIPPs.

In conducting this assessment, NSA identified and implemented policies, procedures, compliance safeguards, and metrics that minimize the civil liberties and privacy impact, while also enabling the Agency to demonstrate its good stewardship of the authority granted under the USA FREEDOM Act.

II. Definition of Key Terms

There are several key terms to understand before describing how NSA has implemented the USA FREEDOM Act:

Call detail records (CDRs)—also known as "metadata" – from telecommunications providers. A CDR is defined in the USA FREEDOM Act as session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile Station Equipment Identity (IMEI) number), a telephone calling card number, or the time or duration of a call. CDRs do not include the contents of any communications, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information.[2] Under the USA FREEDOM Act, CDRs will be held and queried by the providers.

FISC-approved specific selection term. A selection term, such as a telephone number, when it has been determined that there is a reasonable, articulable suspicion (RAS) that the selection term is associated with one or more foreign powers or their agents engaged in international terrorism or activities in preparation therefore. Such a selection term and the evidence that documents its association with foreign powers or their agents engaged in international terrorism or activities in preparation therefore must be reviewed by NSA's Office of General Counsel before submission to the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) for preparation of an application to the Foreign Intelligence Surveillance Court (FISC), or a request to the Attorney General in an emergency. The FISC may approve the specific selection term only if the FISC concludes that the RAS standard mandated by the USA FREEDOM Act has been satisfied.[3]

One-hop results. Selection terms that are in direct contact with a FISC-approved specific selection term are considered "one-hop" results. In other words, if NSA determines and the FISC agrees that there is RAS to believe that a specific telephone number is associated with foreign powers or their agents engaged in international terrorism or activities in preparation therefore, then any telephone numbers in contact with that telephone number would be "one hop" from that specific telephone number.

Two-hop results. Selection terms in direct contact with the one-hop selection terms are considered "two-hop" results. As described above, two-hop results would be the telephone numbers that had been in contact with the one-hop telephone numbers.

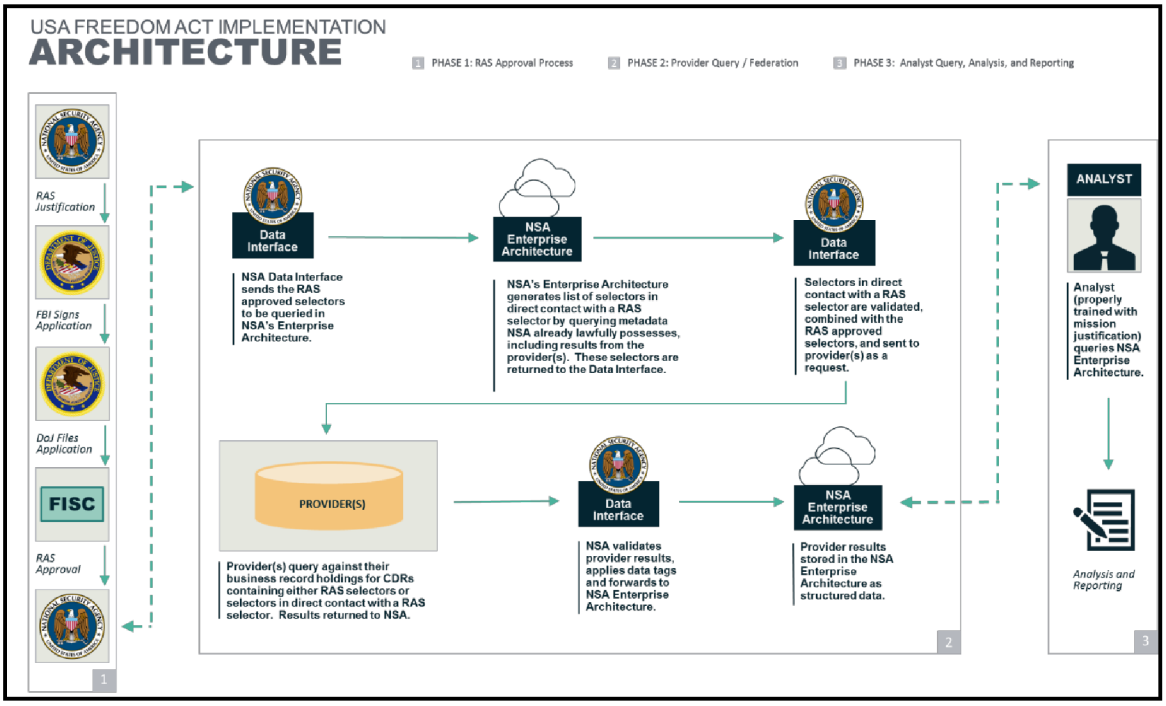
---

[2] *See* The USA FREEDOM Act of 2015, §107: DEFINITIONS.

[3] The RAS standard is the same legal standard used to implement the previous telephone metadata program under Section 215 of the USA PATRIOT Act.

III. Overview of the USA FREEDOM Act Architecture

This section describes the workflow and the core steps of NSA's implementation of the USA FREEDOM Act. This section concludes with a hypothetical example to help illustrate how the process works in practice.



High-Level Architecture for the USA FREEDOM Act Business Records FISA Implementation

1. **Application and Authorization:** FBI will submit an application to the FISC through the DOJ to receive authorization for one or more specific selection terms where (1) there are reasonable grounds to believe that the requested CDRs are relevant to an authorized investigation to protect against international terrorism, and (2) there is RAS to believe that the specific selection term to be used as a basis for the production is associated with a foreign power, or an agent of a foreign power, engaged in international terrorism or activities in preparation therefore. If the FISC agrees that the government has met the statutory requirements, the Court will issue an order approving submission of the specific selection term to the provider(s) that directs the provider(s) to produce the requested CDRs in a form useful to the government. In an emergency, a specific selection term meeting these statutory requirements may be submitted to the Attorney General. The Attorney General must agree that the government has met the statutory requirements and will authorize the submission of the specific selection term to the

provider(s) in the first instance, generally with an application to be filed with the FISC within seven days.[4]

2. **Collection:** The FISC-approved specific selection term, along with any one-hop results generated from metadata NSA already lawfully possesses from previous results returned from the provider(s) and other authorities[5], will be submitted to the authorized provider(s).[6] The provider(s) will return CDRs that are responsive to the request, meaning the results will consist of CDRs that are within one or two hops of a FISC-approved specific selection term. ***This step will be repeated periodically for the duration of the order to capture any new, responsive CDRs – but in no case will the procedures generate third or further hops from a FISC-approved specific selection term.*** The order is valid for no more than 180 days but may be renewed if the FISC determines that the RAS standard continues to be satisfied.

3. **Processing, Analysis, Dissemination, and Retention:** NSA may process, analyze, disseminate, and retain CDR results only in the manner permitted by the USA FREEDOM Act minimization procedures adopted by the Attorney General and approved by the FISC (See Appendix B). Among other things, these procedures require NSA to limit access to the USA FREEDOM Act results to NSA personnel who have received appropriate and adequate training and guidance regarding the procedures and the restrictions that govern the handling and dissemination of information NSA obtains pursuant to the USA FREEDOM Act. Analysts approved for access to the USA FREEDOM Act results will be able to use the results for analysis related to a foreign power, or an agent of a foreign power, engaged in international terrorism or activities in preparation therefore. Dissemination of U.S. person information must be for a counterterrorism purpose or constitute evidence of a crime.[7]

To illustrate the process, assume an NSA intelligence analyst identifies or learns that phone number (202) 555-1234 is being used by a suspected international terrorist. This is the "specific selection term" or "selector" that will be submitted to the FISC (or the Attorney General in an emergency) for approval using the RAS standard. Also assume that, through NSA's examination of metadata produced by the provider(s) or in NSA's possession as a result of the Agency's otherwise lawfully permitted signals

---

[4] *See* The USA FREEDOM Act of 2015, §102 (a)(i)(3). "In the absence of a judicial order approving the production of tangible things under this subsection, the production shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time the Attorney General begins requiring the emergency production of such tangible things, whichever is earliest."

[5] Historical bulk data collected under Section 215 of the USA PATRIOT Act will be retained by NSA until February 29, 2016 solely for technical testing purposes. Separately, NSA remains under a continuing legal obligation to preserve records subject to ongoing civil litigation actions. Historical bulk data collected under Section 215 of the USA PATRIOT Act will never be included when querying internal holdings.

[6] *See* House Committee on the Judiciary. Rept. 114-109 Part 1, p17 (2015).

[7] NSA expects that its analysis of CDRs acquired pursuant to the USA FREEDOM Act will rarely, if ever, result in the dissemination of information solely for a law enforcement purpose.

intelligence activities (*e.g.,* activities conducted pursuant to Section 1.7(c)(1) of Executive Order 12333, as amended), NSA determines that the suspected terrorist has used a 202 area code phone number to call (301) 555-4321. The phone number with the 301 area code is a "first-hop" result. In turn, assume that further analysis or production from the provider(s) reveals (301) 555-4321 was used to call (410) 555-5678. The number with the 410 area code is a "second-hop" result.

Once the one-hop results are retrieved from the NSA's internal holdings, the list of FISC-approved specific selection terms, along with NSA's internal one-hop results, are submitted to the provider(s). The provider(s) respond to the request based on the data within their holdings with CDRs that contain FISC-approved specific selection terms or the one-hop selection term. One-hop returns from providers are placed in NSA's holdings and become part of subsequent query requests, which are executed on a periodic basis. Historical bulk data collected under Section 215 of the USA PATRIOT Act will never be included when querying internal holdings.

Absent information to the contrary, NSA must presume that each user of each of the phone numbers in the above example is a U. S. person, since each phone number has a U.S. area code. NSA's FISC-approved minimization procedures for the USA FREEDOM Act prohibit NSA from disseminating any known or presumed U.S. person information that does not constitute foreign intelligence information related to international terrorism or information necessary to understand foreign intelligence information related to international terrorism or assess its importance or is not evidence of a crime. In addition, the minimization procedures require NSA to destroy promptly any CDRs that are determined not to contain foreign intelligence information. The procedures also set a maximum retention period for CDRs obtained pursuant to the FISC's orders of no more than 5 years after initial delivery to NSA, except that NSA may retain any CDR (or information derived therefrom) that was the basis of a properly approved dissemination of foreign intelligence information.[8]

[8] Note that the minimization procedures also permit NSA to temporarily retain specific CDRs that otherwise would have to be destroyed if DOJ advises NSA in writing that the records are subject to a preservation obligation in pending or anticipated litigation.

IV. Privacy and Civil Liberties Analysis

Fair Information Practice Principle - Transparency

Civil Liberties & Privacy Analysis
The Transparency Principle states that organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII). **CLPO finds that the robust public debate of the USA FREEDOM Act, as well as the Government's release of detailed information about NSA's implementation of the statute, to include release of the minimization procedures in Appendix B of this report, adequately address the Principle of Transparency.**

The USA FREEDOM Act was preceded by extensive public debate following the President's announcement in March 2014 that he intended to seek legislation to fundamentally alter the telephone metadata program that NSA had been conducting pursuant to Section 215 of the USA PATRIOT Act. On 2 June 2015, the USA FREEDOM Act was passed by Congress and signed into law by the President. The government publicly released substantial information about its planned implementation of the USA FREEDOM Act, as well as NSA's plans for data that had been acquired under the old metadata program.[9]

The USA FREEDOM Act also requires the government to publish certain metrics regarding the government's use of the amended Business Records authority. The purpose of the USA FREEDOM Act's mandatory reporting requirements is to provide transparency to the American public. The Office of the Director of National Intelligence (ODNI) plans to report these metrics via ODNI's annual Transparency Report. The key metrics that NSA is obligated to provide are listed below.[10]

- **The number of targets under each order:**[11] Defined as the person using the selector.
    - For example, if a target has a set of four selectors that have been approved, NSA will count one target, not four. Alternatively, if two targets are using one selector that has been approved, NSA will count two targets.

- **The number of unique identifiers used to communicate information collected pursuant to an order:**[12] Defined as each unique record sent back from the provider(s).

[9] *See, e.g.,* Statement of the Office of the Director of National Intelligence, "ODNI Announces Transition to New Telephone Metadata Program," dated 29 November 2015. This press release was accompanied by a "Fact Sheet" that further described NSA's implementation of the new authority.

[10] *See* The USA FREEDOM Act of 2015, §602: ANNUAL REPORTS BY THE GOVERNMENT.

[11] *Ibid.,* §603(b)(5)(A).

[12] *Ibid.,* §603(b)(5)(B).

- If NSA receives the same record separately, whether from multiple providers or one provider, NSA will count each response separately. The Agency recognizes that NSA's metrics, therefore, likely will be over-inclusive.

- **The number of search terms that included information concerning a U.S. person and were used to query any database of CDRs obtained under each order:**[13] Defined as the number of times the USA FREEDOM Act data is queried using a U.S. person query term.

In light of the government's publication of detailed information about the new procedures and the USA FREEDOM Act's mandatory reporting requirements, CLPO finds that the Principle of Transparency is satisfied.

[13] *Ibid.,* §603(b)(5)(C).

Fair Information Practice Principle – Individual Participation

Civil Liberties & Privacy Analysis
The Principle of Individual Participation states that 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. **Although it is unlikely that an individual target will be notified that NSA used the USA FREEDOM Act to acquire telephone metadata about them, CLPO concludes that this is appropriate under the circumstances.**

NSA does not release information that would reveal the identities of the specific individuals whose CDRs are targeted for collection pursuant to the USA FREEDOM Act. Frequently, the very fact that the government suspects that a particular person is engaged in international terrorism or that a particular phone number is being used by such a person must be kept secret in the interests of national security. If a target of an international terrorism investigation becomes aware of the investigation, he or she likely will take steps to thwart investigators. The targets of such investigations also attempt to conceal from the government the identities of their contacts. As a consequence, direct individual participation thwarts the government's legitimate need to identify individuals engaged in international terrorism.

A less intrusive and more effective means of identifying contacts of individuals engaged in international terrorism is to acquire CDRs. CDRs, per the statute, contain only telephone metadata and not, for example, the contents of any personal communication or the caller's name or location of any phone call. CDRs are business records generated by a provider for the provider's own business use. Instead of direct individual participation, the Act requires approval by the FISC (or the Attorney General in emergency situations) before any specific selection term may be used in a query request to the provider(s). In the event of an error, the FISC retains authority to order the government to take corrective action. Other safeguards include rigorous internal and external oversight to ensure full compliance with the law. CLPO concludes that, under the circumstances, the oversight and compliance mechanisms serve as sufficient proxies to satisfy the Principle of Individual Participation.

Fair Information Practice Principle – Purpose Specification

Civil Liberties & Privacy Analysis
The Principle of Purpose Specification provides that 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. **CLPO concludes that NSA's implementation of the USA FREEDOM Act satisfies the Principle of Purpose Specification.**

As noted in the discussion of the Principle of Transparency, the government has publicly released, and continues to release, information about its implementation of the USA FREEDOM Act, as well as NSA's plans for data that had been acquired under the old metadata program. This information, including this report, publicly describes how NSA is implementing the USA FREEDOM Act and also articulates the counterterrorism purpose for the authority. This information is contained in the statute itself, Congressional reports and debate regarding the statute, the FISC-approved minimization procedures, and other publicly released information. Therefore, CLPO finds that the Principle of Purpose Specification has been satisfied.

Fair Information Practice Principle – Data Minimization

Civil Liberties & Privacy Analysis
The Principle of Data Minimization states that organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s). **CLPO concludes that NSA's implementation of the USA FREEDOM Act satisfies the Principle of Data Minimization.**

The new authority explicitly minimizes the amount and type of data accessible to NSA. NSA no longer collects CDRs in bulk under FISA. Under the USA FREEDOM Act, only telephone metadata (not, for example, the contents of any personal communication or the caller's name or location of any phone call) may be acquired. The statute further limits the production of CDRs to those that are FISC-approved and those that are no more than two hops from a FISC-approved specific selection term. Appendix B to this report contains the minimization procedures that were adopted by the Attorney General and approved by the FISC to govern NSA's handling of the telephone metadata that NSA acquires pursuant to the USA FREEDOM Act. These minimization procedures prohibit NSA from reporting any known or presumed U.S. person information that does not constitute foreign intelligence information related to international terrorism or information necessary to understand foreign intelligence information related to international terrorism or assess its importance or is not evidence of a crime.

In addition, the minimization procedures require NSA to destroy promptly any CDRs that are determined not to contain foreign intelligence information. The procedures set a maximum retention period for CDRs obtained pursuant to the FISC's orders of no more than 5 years after initial delivery to NSA, except that NSA may retain any CDR (or information derived therefrom) that was the basis of a properly approved dissemination of foreign intelligence information. In addition, the procedures contain detailed oversight and compliance responsibilities. In short, CLPO finds that the Principle of Data Minimization is satisfied by NSA's USA FREEDOM Act minimization procedures, as well as the limitation in the statute itself that focuses solely on CDRs and limits production of CDRs to those that are no more than two hops from a FISC-approved specific selection term.

Fair Information Practice Principle – Use Limitation

Civil Liberties & Privacy Analysis
The Principle of Use Limitation provides that 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. **CLPO concludes that NSA's implementation of the USA FREEDOM Act satisfies the Principle of Use Limitation.**

The restrictions articulated in the USA FREEDOM Act and the FISC-approved minimization procedures adopted by the Attorney General and described above in the Principle of Data Minimization provide important use limitations. NSA is required to follow the detailed minimization procedures to govern its handling of telephone metadata acquired pursuant to the USA FREEDOM Act. The minimization procedures outline the counterterrorism purpose for collection of the metadata. In addition, NSA cannot acquire CDRs under the procedures unless the Agency starts with a specific selection term related to an open FBI investigation and for which there is RAS to believe the selection term is associated with a foreign power, or an agent of a foreign power, engaged in international terrorism or activities in preparation therefore. Only the FISC, or the Attorney General in an emergency, is authorized under the statute to approve this RAS determination. NSA has also implemented technical controls to help ensure that it only acquires CDRs from the provider(s) that are within no more than two hops from a RAS-approved specific selection term.

In addition, once CDRs have been received and stored by NSA, they will be available for analysis and dissemination related to foreign powers or their agent engaged in international terrorism. Analysts will require appropriate and adequate training, and must have both an international terrorism mission purpose and a need to know in order to be provided access to the CDRs obtained through the USA FREEDOM Act. Analyst queries of records acquired under the USA FREEDOM Act will be intended to determine or identify persons of foreign intelligence interest who may be engaged in international terrorism. All queries will be subject to post-query auditing. The USA FREEDOM Act data will be used to produce intelligence reports, following reporting and minimization procedures. As noted previously, in order for NSA to disseminate U.S. person information based upon the USA FREEDOM Act results, a determination must first be made that the information is foreign intelligence information related to international terrorism, or is necessary to understand foreign intelligence information related to international terrorism or assess its importance. NSA is also permitted to disseminate CDR information concerning U.S. persons or the identity of a U.S. person if the information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes. Therefore, the Principle of Use Limitation is satisfied.

Fair Information Practice Principle – Data Quality and Integrity

Civil Liberties & Privacy Analysis
The Principle of Data Quality and Integrity provides that organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. **CLPO concludes that NSA's implementation of the USA FREEDOM Act satisfies the Principle of Data Quality and Integrity.**

Each CDR is a business record generated by a provider for the provider's own business use. NSA plays no role in ensuring that the provider-generated CDRs accurately reflect the calling events that occurred over the provider's infrastructure, but the provider(s) have their own policies, practices, and incentives for ensuring the accuracy of their records. NSA's requirements for ensuring accurate, relevant, timely, and complete CDRs begin when NSA submits query requests to the provider(s), and the provider(s), in response, produce CDRs to the Agency. NSA's minimization procedures for the telephone metadata acquired pursuant to the USA FREEDOM Act require the Agency to inspect CDRs received from a provider through manual and/or automated means to confirm that the CDRs are responsive to the FISC's production order. The minimization procedures require NSA to destroy promptly any CDRs produced that are determined to be outside the scope of the FISC's applicable order. NSA has worked closely with the provider(s) to ensure that the provider(s) produce records in a useful format and in a timely manner, as required by the USA FREEDOM Act. To this end, NSA and the provider(s) have conducted a significant amount of systems engineering and testing to ensure that CDRs produced under the USA FREEDOM Act are accurate, relevant, timely, and complete. NSA continually processes and manages results returned from the provider(s). Thus, NSA's implementation of the new metadata authority includes three important components:

1) NSA will de-duplicate and re-submit requests to the provider(s) on a periodic basis.

2) NSA will periodically query its internal holdings with FISC-approved specific selection terms to obtain *new* one-hop selectors. These new one-hop results will then be submitted to the provider(s) on a periodic basis.

3) NSA will manage CDR results such that results *do not exceed the two-hop maximum* specified by the USA FREEDOM Act.

In light of these efforts, CLPO finds that the Principle of Data Quality and Integrity is satisfied.

Fair Information Practice Principle – Security

Civil Liberties & Privacy Analysis
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. **CLPO concludes that NSA's implementation of the USA FREEDOM Act satisfies the Principle of Security.**

NSA's minimization procedures for the USA FREEDOM Act require the Agency to process, analyze, and store the CDRs produced by provider(s) within secure networks under NSA's control. The minimization procedures further require that NSA apply unique markings to the CDRs so that NSA can restrict access to authorized personnel who have received appropriate and adequate training on the requirements of NSA's USA FREEDOM Act minimization procedures. NSA has accounted for these security requirements in its implementation of the USA FREEDOM Act telephone metadata procedures. CLPO finds that the Principle of Security is satisfied by NSA's security controls.

Fair Information Practice Principle – Accountablility and Auditing

Civil Liberties & Privacy Analysis
The Principle of Accountablility and Auditing states that 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. **CLPO concludes that NSA's implementation of the USA FREEDOM Act satisfies the Principle of Accountablility and Auditing.**

NSA's minimization procedures for the USA FREEDOM Act contain significant compliance and oversight requirements, including those regarding training, the implementation and monitoring of software controls used to govern access to the CDRs the Agency obtains under the USA FREEDOM Act, and external oversight conducted by DOJ. As part of its implementation of the USA FREEDOM Act metadata procedures, NSA is also applying its longstanding internal intelligence oversight mechanisms to this new authority. Moreover, Congress and the FISC also exercise significant oversight over NSA's implementation of the authority, to include significant reporting requirements.

With respect to training, in particular, all analysts who require access to the USA FREEDOM Act results must successfully complete training tailored to the USA FREEDOM Act statute, FISC-approved applications, and FISC-approved and Attorney General-adopted minimization procedures. This tailored USA FREEDOM Act training consists of modules that cover the USA FREEDOM Act; data handling requirements (including sharing and dissemination) from the FISC-approved minimization procedures applicable to the USA FREEDOM Act orders; incident reporting; purge requirements, and any special requirements imposed by the FISC. Technical personnel will be trained based on their roles and functions. Those personnel who maintain and develop NSA systems that process the USA FREEDOM Act results or process the USA FREEDOM Act data for data fidelity purposes will receive training specific to their work role.

CLPO finds the key components of the USA FREEDOM Act training crucial to educate and inform personnel. In particular, CLPO finds the training of technical personnel particularly important in order to uphold not only the Principles of Accountablility and Auditing, but also, as noted elsewhere in this report, the Principles of Data Minimization, Security, and Use Limitation.

CLPO finds that, taken together, NSA's training, compliance, and oversight mechanisms satisfy the Principle of Accountablility and Auditing.

Appendix A: Fair Information Practice Principles (FIPPs)[14]

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.

- **Accountablility 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.

[14] *See* "The National Strategy for Trusted Identities in Cyberspace", Appendix A (2011).