Fact Sheet on E.O. 12333 Raw SIGINT Availability Procedures

On January 3, 2017, the Director of National Intelligence, in coordination with the Secretary of Defense, issued the "Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333" (the "Raw SIGINT Availability Procedures"). The procedures were approved by the Attorney General on January 3, 2017.

The procedures are called for by Section 2.3 of Executive Order (E.O.) 12333, as amended in 2008. The last paragraph of Section 2.3 of E.O. 12333 provides that elements of the Intelligence Community (IC) may disseminate information to a recipient IC element to allow that element to determine whether information "is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director [of National Intelligence] in coordination with the Secretary of Defense and approved by the Attorney General."[1]

Purpose and Scope

The purpose of the procedures is to enable IC elements to conduct their national security missions more effectively by providing them with access to unevaluated or unminimized (i.e., "raw") signals intelligence (SIGINT) collected by the NSA, subject to appropriate privacy protections for information about U.S. persons. This access will enable IC elements to bring their own analytic expertise to reviewing that information and to use that information in support of their own missions. The procedures provide an important mechanism for enhancing information sharing, integration, and collaboration in the IC. In addition, the procedures are consistent with recommendations of the 9/11 Commission and other reviews of the Intelligence Community.

The procedures do not alter the rules that apply to the NSA's collection, retention, or dissemination of information, other than to permit the NSA to disseminate raw SIGINT information that it has already lawfully collected under E.O. 12333 to other authorized IC recipients. Further, the procedures do not alter the legal authorities or civil liberties or privacy protections provided by the Foreign Intelligence Surveillance Act (FISA) and by Presidential Policy Directive 28 (PPD-28), Signals Intelligence Activities. PPD-28 requires IC elements to have procedures for safeguarding the personal information of non-U.S. persons collected from signals intelligence activities. IC elements requesting access to raw SIGINT pursuant to the Raw SIGINT Availability Procedures will need to review and, if necessary, update their PPD-28 procedures to ensure that they account for access to, and use of, raw SIGINT.

[1] The first paragraph of Section 2.3 provides that elements of the IC may collect, retain, and disseminate information concerning United States persons in accordance with procedures established by the head of the IC element and approved by the Attorney General, in consultation with the DNI. Those procedures are distinct from the Raw SIGINT Availability Procedures.

Civil Liberties and Privacy Protections in the Procedures

- The procedures include protections to ensure that the civil liberties and privacy of U.S. persons are protected and that all activities undertaken pursuant to the procedures comply with the Constitution and other applicable law and policy. These protections fall into three broad groups:

    - First, the procedures establish requirements for requesting access to raw SIGINT. Access will be limited to circumstances where the information is expected to further a foreign intelligence or counterintelligence mission in a significant way.

    - Second, the procedures establish rules that a recipient IC element must follow when accessing, processing, or retaining raw SIGINT, as well as rules for disseminating information derived from raw SIGINT. The processing, retention, and dissemination rules closely follow those used by the NSA.

    - Third, the procedures establish training, auditing, oversight, and compliance requirements to ensure the proper handling of U.S. person information.

Requests for Access

- An access request must be made by a high-level official at the requesting element. Requests must be in writing and made in consultation with the element's legal counsel and the appropriate senior official responsible for the protection of civil liberties and privacy.

- Requests must explain how the raw SIGINT is expected to further, in a significant way, a particular foreign intelligence or counterintelligence mission or function of the element and why other sources cannot provide the information that the element expects to obtain from the raw SIGINT. Requests must also explain how the element will protect the raw SIGINT and describe how the requesting element's compliance and oversight programs comport with the requirements of the procedures.

- A high-level NSA official must review and, if appropriate, approve the request based on a determination that the request is reasonable in light of all of the circumstances.

- Prior to the NSA making raw SIGINT available to a requesting element, approval of the request must be memorialized in a Memorandum of Agreement governing the availability, retention, and use of the information. This agreement must be approved by high-level officials not only at the requesting element and the NSA, but also at the ODNI (acting in coordination with the Department of Defense (DoD)).

Rules for Processing, Retention, and Dissemination

Domestic Communications

- The NSA's SIGINT mission is focused on the collection of foreign communications; therefore, a recipient IC element should rarely encounter a "domestic communication." A domestic communication is defined by the procedures as a "communication where the sender and all intended recipients are located in the United States and that was acquired under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."

- The procedures provide that recipient IC elements "may not use a query, identifier, or other selection term that is intended to select domestic communications." If, despite this limitation, a domestic communication is inadvertently retrieved, the procedures require the recipient IC element to destroy it promptly upon recognition unless the Attorney General determines that the contents of the communication indicate a threat of death or serious bodily harm to any person.

Restrictions on the Processing of Raw SIGINT

- A recipient element may only access and process raw SIGINT for the authorized foreign intelligence or counterintelligence purposes documented in the applicable Memorandum of Agreement. This restriction serves to prohibit recipient elements from querying raw SIGINT for a law enforcement purpose.

- A recipient element may use a selection term based on the identity of a communicant or the fact that the communications mention a particular person, but the element may only use a selection term associated with a U.S. person or person in the United States if the element's legal and compliance officials confirm that the selection term is associated with a U.S. person who is a current FISA target, or if the selection is approved by the Attorney General, or in certain limited cases, is approved by the Director of the NSA or the head of the recipient element (or a high-level designee).

- A recipient element may conduct communications metadata analysis, to include contact chaining, for approved foreign intelligence or counterintelligence purposes without regard to the location or nationality of the communicants. Recipient elements conducting communications metadata analysis under the procedures must report annually to the Attorney General on their activities.

Restrictions on the Retention of Raw SIGINT

- The procedures limit recipient elements to specific time periods for evaluating raw SIGINT. In no circumstances may a recipient element retain raw SIGINT beyond the time that the NSA may retain it.

- A recipient element may permanently retain communications to, from, or about U.S. persons only if they are: (1) foreign communications and (2) the element has processed the communications so as to eliminate any U.S. person information (defined by the procedures to be "information that is reasonably likely to identify one or more specific U.S. persons") or the element has determined that the dissemination of such communications without elimination of reference to such U.S. persons would be permitted under the dissemination provisions of these procedures.

Restrictions on the Dissemination of Raw SIGINT

- A recipient element may disseminate U.S. person information derived solely from raw SIGINT only if a high-level official identified in the governing Memorandum of Agreement determines that the intended recipient has a need for the U.S. person information in the performance of his or her official duties and one of the following conditions is met:

    - The U.S. person has consented to the dissemination.

    - The U.S. person information is publicly available information.

    - The U.S. person information is necessary to understand the foreign intelligence or counterintelligence information or assess its importance.

    - The information is evidence of a possible commission of a crime and is reported consistent with the IC element's crime reporting obligations. Of note, IC elements may not query or search raw SIGINT for a law enforcement purpose, but they may report evidence of a possible crime that they encounter in the course of conducting authorized foreign intelligence or counterintelligence activities.

    - The dissemination is required by law, treaty, or Executive Branch policies or agreements.

- The procedures further restrict disseminations to foreign governments or government-sponsored international entities. The dissemination must be approved by the Director of the NSA or a designee, who must determine that it is consistent with applicable international agreements, and foreign disclosure policy and directives, including those requiring analysis of potential harm to any individual.

Training, Auditing, Oversight and Compliance

- *Training*. All IC element personnel who have access to raw SIGINT under the procedures must receive training on these procedures. The training will cover the applicable privacy protective measures, such as the rules regarding query terms associated with U.S. persons or with persons in the United States, the requirements for accessing, processing, and retaining raw SIGINT, and the requirements for disseminating

information derived from raw SIGINT. A recipient element must develop its training program in coordination with the NSA and pursuant to standards developed by the ODNI in consultation with the DoD.

- *Auditing*. The procedures have detailed auditing requirements to ensure that IC elements can effectively monitor compliance.

    - Access to raw SIGINT must be monitored, recorded, and audited by supervisory or other appropriate personnel of the recipient element.

    - Recipient elements must monitor and record all queries used by their personnel, and supervisory or other appropriate personnel must audit and review the use of such queries and search terms. The recipient element's compliance program will specify the frequency of these audits, but, at a minimum, they must be comparable to the NSA standards.

    - Recipient elements must review retrievals of information, or samples of retrievals, from raw SIGINT repositories for compliance with the procedures and for relevance to the authorized mission or function for which access has been provided.

- *Oversight and Compliance Programs and Reviews*. Each recipient element must establish an oversight and compliance program tailored to its handling of raw SIGINT under these procedures. The ODNI Civil Liberties Protection Officer will review and approve these programs in consultation with the NSA to ensure that the program is comparable to the NSA's program for similar activities. In addition, the procedures require recipient elements and the ODNI (and, in the case of DoD elements, the DoD) to periodically review the adequacy of oversight and compliance.