OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Safeguarding the Personal Information of all People

A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28

LEADING INTELLIGENCE INTEGRATION

July 2014

Background

The United States is committed to protecting the personal information of all people around the world, regardless of their nationality. Indeed, it is our longstanding practice to conduct signals intelligence (SIGINT) activities only for authorized foreign intelligence and counterintelligence purposes, and to safeguard information obtained through such means from unauthorized access or disclosure. On January 17, 2014, the President issued Presidential Policy Directive (PPD)-28, *Signals Intelligence Activities*, which "articulates principles to guide why, whether, when, and how the United States conducts SIGINT activities for authorized foreign intelligence and counterintelligence purposes." This directive reinforces current practices, establishes new principles that govern how the United States conducts SIGINT collection, and strengthens Executive Branch oversight of SIGINT activities. Moreover, the principles ensure that in conducting SIGINT activities, the United States takes into account not only the nation's security requirements, but also the security and privacy concerns of U.S. allies and partners, the increased globalization of trade and investment, and the commitment to protect privacy rights and civil liberties.

Section 4 of PPD-28 calls on each Intelligence Community element to update or issue new policies and procedures that implement the principles for safeguarding all personal information collected through SIGINT, consistent with technical capabilities and operational needs. In approaching this task, the Intelligence Community recognizes that it must apply policies and procedures in a way that affords safeguards for personal information, minimizes the creation of new barriers to information sharing, and does not impose operationally untenable impediments to collecting and using SIGINT, including impediments to using SIGINT together with other lawfully collected information, to protect national security. Section 4 also requires the Director of National Intelligence, in coordination with the Attorney General, the heads of elements of the Intelligence Community, and the heads of departments and agencies containing elements of the Intelligence Community, to prepare a report evaluating possible additional dissemination and retention safeguards for personal information collected through SIGINT, consistent with technical capabilities and operational needs.

Shortly after the President issued PPD-28, the Office of the Director of National Intelligence (ODNI) established a multidisciplinary interagency working group to discuss a common approach to developing additional safeguards that protect personal information, recognizing that every Intelligence Community element has different mission needs and requirements. The working group members represented Intelligence Community mission and technology functions as well as Intelligence Community legal, policy, and civil liberties and privacy offices. In approaching this task, the group focused on developing key principles to inform all Intelligence Community elements as they implement the requirements of PPD-28 in a manner that protects personal information collected through SIGINT, and determining what additional protections, if appropriate, need to be afforded beyond what PPD-28 requires.

Section I of this status report describes the DNI's evaluation, conducted in coordination with the Attorney General and heads of the Intelligence Community elements, of possible

additional dissemination and retention safeguards for personal information collected through SIGINT consistent with technical capabilities and operational needs. This section includes the key principles that all Intelligence Community elements must follow as they adopt policies and procedures under PPD-28. Section II provides a status report on the progress of the implementation of section 4 of PPD-28.

I. Appropriate Protections for Personal Information Collected through SIGINT

All Intelligence Community elements operate in a manner that protects the civil liberties and privacy rights of U.S. persons wherever located around the world, and of all people in the United States regardless of nationality. The applicable rules are in accordance with several key statutes and executive orders, such as the Privacy Act, the Foreign Intelligence Surveillance Act, and Executive Order 12333, as well as the U.S. Constitution. Beyond abiding by these legal requirements, the Intelligence Community is committed to conducting SIGINT activities in a manner that treats all people with dignity and respect regardless of their nationality or place of residence. PPD-28 reflects these values and calls on each Intelligence Community element to apply principles for safeguarding all personal information collected through SIGINT, consistent with technical capabilities and operational needs. To that end, PPD-28 states that personal information of non-U.S. persons shall be retained and disseminated only if the retention and dissemination "of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333."

In approaching the evaluation of possible additional dissemination and retention safeguards, ODNI focused on developing key principles that all Intelligence Community elements must incorporate to ensure protection for personal information collected through SIGINT.[1] While each Intelligence Community element must have procedures specifically adapted to its unique mission, the generally applicable requirements articulated below satisfy the basic requirements of the PPD and also afford additional protections beyond what the PPD requires.[2]

A. Intelligence Community Elements that Collect SIGINT Should Include the PPD-28 Principles Governing the Collection of SIGINT in Their Procedures.

Section 1 of PPD-28 reinforces four principles for the collection of SIGINT:

---

[1] By its terms, PPD-28 applies only to SIGINT activities conducted to collect communications or information about communications. This is a particular category of intelligence information that, by its nature, often has significant civil liberties and privacy implications. Intelligence Community elements should not take an overly narrow approach to defining what information will be protected under their PPD-28 procedures.

[2] While comparable protections are to be sought, PPD-28 does not require the Intelligence Community to apply the *identical* procedures to both U.S. person and non-U.S. person information. However, in determining what particular protections should exist for all personal information derived from SIGINT regardless of nationality, section 2.3 of Executive Order 12333 serves as an appropriate starting point.

(1) The collection of SIGINT shall be authorized by statute or Executive Order, proclamation, or other Presidential directive, and undertaken in accordance with the Constitution and applicable statutes, Executive Orders, proclamations, and Presidential directives.

(2) Privacy and civil liberties shall be integral considerations in the planning of U.S. SIGINT activities. The United States shall not collect SIGINT for the purposes of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. SIGINT shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purpose.

(3) The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.

(4) SIGINT activities shall be as tailored as feasible. In determining whether to collect SIGINT, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to SIGINT should be prioritized.

These principles are based on the understanding that the collection of SIGINT is necessary to protect national security, to advance foreign policy interests, and to protect U.S. citizens and interests, as well as the citizens of its allies and partners from harm. At the same time, these principles take into account the multiple risks associated with collecting SIGINT including those to privacy, to global commerce, and to U.S. foreign relations. Accordingly, these principles, which reflect our commitment to the rule of law and to privacy and civil liberties, must be reflected in each Intelligence Community element's PPD-28 procedures.

In addition to including these four principles in their procedures, Intelligence Community elements should take steps to ensure their proper implementation. First, to ensure that a new and unique SIGINT collection program or significant changes to existing programs are authorized by law and are not conducted for a prohibited purpose, the procedures should address appropriate approvals and coordination before starting such a new and unique SIGINT collection program or before making significant changes to an existing SIGINT collection program. New and unique programs or significant changes to existing programs would generally include those that result in substantial new collection of personal information as compared to existing programs, regardless of the nationality of the persons involved. Second, to ensure that civil liberties and privacy protections are integral considerations in the planning and execution of SIGINT collection activities, the Intelligence Community element executing a new or unique SIGINT collection program or making significant changes to an existing program

should assess, in consultation with the agency officials responsible for civil liberties and privacy protections, and in a manner consistent with its need to act with speed, agility, and flexibility, whether there are appropriate safeguards in place to protect personal information before an element begins the program. Finally, to ensure SIGINT activities are as tailored as feasible, Intelligence Community policies should require that, whenever practicable, Intelligence Community elements focus collection on specific foreign intelligence targets or topics through the use of discriminants (e.g., specific facilities, selection terms, identifiers, etc.).

B. Intelligence Community Element Procedures Should Include the Limitations on the Use of SIGINT Collected in Bulk.

Section 2 of PPD-28 acknowledges the importance of collecting SIGINT in bulk to help identify new and emerging threats or other vital national security information. At the same time, the United States recognizes that collecting information in bulk may result in the collection of information about persons whose activities are not of interest to the Intelligence Community. PPD-28 therefore places limitations on the use of SIGINT collected in bulk.[3] More specifically, PPD-28 requires that, when the United States collects non-publicly available SIGINT in bulk, it shall use that data only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S. or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named above. PPD-28 also states that in no event may SIGINT be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or achieving any purpose other than those identified above.

Just as Intelligence Community procedures must reflect the principles governing the collection of SIGINT, the procedures must also reflect the limitations on the use of SIGINT collected in bulk. Moreover, Intelligence Community element procedures should include safeguards to satisfy the requirements of this section. In developing procedures to comply with this requirement, the Intelligence Community must be mindful that to make full use of intelligence information, an Intelligence Community element may need to use SIGINT collected in bulk together with other lawfully collected information. In such situations, Intelligence Community elements should take care to comply with the limitations applicable to the use of bulk SIGINT collection.

[3] These limitations are intended to restrict the use of unevaluated, non-publicly available SIGINT information; they are not intended to limit the use of information that has already been evaluated and disseminated in accordance with applicable safeguards.

C. Intelligence Community Element Procedures Should Set Appropriate Standards for Querying SIGINT Data.

The Intelligence Community recognizes that personal information must be protected throughout the lifecycle of that information. Just as PPD-28 requires dissemination and retention limitations for SIGINT, there are additional limitations on the use of unevaluated SIGINT. Accordingly, in the case of unevaluated SIGINT information contained in datasets or repositories, Intelligence Community element policies should reinforce existing analytic practices and standards whereby analysts must seek to structure queries or other search terms and techniques to identify intelligence information relevant to a valid intelligence or law enforcement task; focus queries about persons on the categories of intelligence information responsive to an intelligence or law enforcement requirement; and minimize the review of personal information not pertinent to intelligence or law enforcement requirements.

D. The Mere Fact that SIGINT is About a Foreign Person is Not, Absent Additional Information, Sufficient to Permanently Retain or to Disseminate Such Information.

PPD-28 requires Intelligence Community elements to have SIGINT dissemination and retention procedures for non-U.S. persons that are comparable to the protections afforded to U.S. persons under section 2.3 of Executive Order 12333. Under section 2.3, the Intelligence Community is authorized to retain and disseminate information concerning U.S. persons that falls into any one of several categories. One such category is information that constitutes foreign intelligence. Executive Order 12333 defines this term as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists." This definition ensures that the Intelligence Community is able to retain and disseminate information necessary for the United States to advance its national security and foreign policy interests. Nonetheless, the definition's reference to "information relating to . . . activities of . . . foreign persons," if read literally, could permit an element to permanently retain or to disseminate any information about any activity of any foreign person. Intelligence Community elements should permanently retain or disseminate such personal information only if the personal information relates to an authorized intelligence requirement, is reasonably believed to be evidence of a crime, or meets one of the other standards for retention or dissemination identified in section 2.3 of Executive Order 12333 for U.S. person information, and not *solely* because of the person's non-U.S. person status. SIGINT information about the routine activities of a foreign person alone would not meet this requirement without some indication that the information falls into one of these categories.

E. Intelligence Community Elements Should Consider, as a Default Position, Subjecting Comparable Non-U.S. Person Personal Information to the Same Retention Periods Afforded to U.S. Persons' Information in Intelligence Community Procedures.

PPD-28 provides that an Intelligence Community element may retain personal information of non-U.S. persons contained in SIGINT only if comparable information concerning

U.S. persons could be retained by that element under section 2.3 of Executive Order 12333. To that end, an Intelligence Community element should consider, as a default position, applying the U.S. person retention periods contained in its Attorney General approved guidelines to non-U.S. person personal information to the extent consistent with the protection of national security or law enforcement requirements. SIGINT that has not been affirmatively determined to meet a longer retention standard should not be retained for more than five years, unless the DNI determines that continued retention is in the national security interest of the United States.

F. The DNI Should Grant An Extension of the 5-Year Temporary Retention Period Only After Evaluating a Written Justification from the Intelligence Community Element.

There will be times when the five-year retention period is insufficient. For example, certain terrorist or other networks of foreign intelligence interest may develop over decades, not years. The DNI takes seriously the obligation to evaluate carefully requests to extend the retention period. The DNI may authorize an extension of the retention period when it is in the national security interest of the United States and after having received a written request from the Intelligence Community element that includes a justification from the requesting Intelligence Community element and the views of the appropriate element civil liberties and privacy officer. Moreover, the DNI will generally not extend the temporary retention of information for more than an additional five years at a time.

G. Intelligence Community Elements Should Establish Dissemination Procedures That Protect All Personal Information Collected Through SIGINT.

Intelligence Community elements understand and appreciate the civil liberties and privacy risks associated with the dissemination of personal information of non-U.S. persons. PPD-28 acknowledges these risks by providing that procedures should permit the dissemination of personal information of non-U.S. persons only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333.

This requirement has several components. First, Intelligence Community element procedures should permit the dissemination of personal information of non-U.S. persons only if it is relevant to the underlying authorized purpose of the dissemination. Second, when unevaluated personal information is disseminated, the disseminating Intelligence Community element should inform the recipient that the dissemination may contain personal information so that the recipient can take appropriate steps to protect that information. Finally, procedures the DNI, Attorney General, and Secretary of Defense are developing in accordance with section 2.3 of Executive Order 12333 for the dissemination of unevaluated SIGINT to other Intelligence Community elements should include a requirement that a receiving element have in place approved procedures for protection of all personal information as required under PPD-28.

H. Intelligence Community Elements Shall Ensure There Are Adequate Procedures to Address Privacy and Civil Liberties Complaints.

Each Intelligence Community element shall ensure that it makes available to its workforce information on how agency personnel may securely report violations of law, rule, or regulation; gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to the public health or safety consistent with Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information*, including any SIGINT-related concerns they may have regarding compliance with established standards, civil liberties, and privacy.

Moreover, as required by PPD-28, the procedures must require that when a significant compliance issue occurs involving personal information of any person, regardless of nationality, collected through SIGINT, the issue shall be reported promptly to the head of the IC element. The head of the IC element will notify the DNI who, under PPD-28, is responsible for determining what, if any corrective actions are necessary in a manner consistent with PPD-28. If the issues involve a non-U.S. person, the DNI, in consultation with the Secretary of State and head of the notifying Intelligence Community element, shall determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel.

I. Intelligence Community Elements Shall Require the Completion of Appropriate and Adequate Training as a Condition of Accessing or Handling Unevaluated Personal Information in SIGINT.

To ensure that both the requirements of PPD-28 and implementing procedures are followed, Intelligence Community elements must review and update existing training or develop new mandatory training, to ensure that the workforce fully understands the responsibility to protect personal information, regardless of nationality. Successful completion of this training must be a prerequisite for accessing and using personal information in unevaluated and unminimzed SIGINT.

J. Intelligence Community Elements Shall Develop Robust Oversight and Compliance Programs to Ensure Adherence to PPD-28 and Implementing Procedures.

It is not sufficient for Intelligence Community elements to simply develop policies and procedures to protect personal information. Agencies must periodically review implementation of the procedures for collecting, retaining, and disseminating personal information. Indeed, it is critical that effective oversight mechanisms are in place to ensure compliance with PPD-28 procedures. To that end, Intelligence Community elements should have appropriate measures to facilitate oversight over the implementation and safeguards protecting personal information collected through SIGINT. These measures should include periodic auditing. To facilitate that oversight, Intelligence Community elements could strive to design information systems to

monitor activity in datasets involving unevaluated personal information and facilitate the monitoring, recording, and reviewing of queries or other searches of personal information.

In addition, agency privacy and civil liberty officers, in coordination with the ODNI Civil Liberties and Privacy Office and other appropriate oversight and compliance components of the departments and agencies collecting and using unevaluated SIGINT information under PPD-28, will periodically review the Intelligence Community elements' practices for protecting personal information contained in SIGINT and their compliance with those procedures.

K. Intelligence Community Elements Shall Have Procedures Implementing PPD-28.

As required by PPD-28, every Intelligence Community element must have procedures for handling information collected through SIGINT. This requirement applies to the Intelligence Community as a whole, including elements that do not collect but only receive SIGINT information, such as SIGINT reports. The scope and details of these procedures may vary based on whether and how each Intelligence Community element collects, retains, and disseminates SIGINT information. For example, if an Intelligence Community element collects, retains, and disseminates foreign intelligence derived from SIGINT, its procedures must cover each phase. Another Intelligence Community element, however, may only have access to or only receive evaluated SIGINT information, such as in the form of finished intelligence reporting. Accordingly, it is appropriate for agencies to develop procedures that are tailored to their actual uses of SIGINT. To that end, Intelligence Community elements that collect or receive unevaluated SIGINT may have procedures that are different from the procedures for Intelligence Community elements that merely receive finished intelligence products containing SIGINT or receive other evaluated SIGINT information. Most agencies already have adequate existing procedures for some aspects of PPD-28, particularly for record retention schedules and data security.

L. Intelligence Community Element Procedures to Implement PPD-28 Shall be Publicly Available.

Consistent with the President's direction and in accordance with section 4(b) of PPD-28, Intelligence Community elements shall publicly release their PPD-28 implementation policies and procedures to the maximum extent possible, consistent with classification requirements. If national security requires that aspects of an Intelligence Community element's procedures remain classified, that Intelligence Community element shall notify the DNI.

In addition to publicly releasing these procedures, and to promote public understanding of and public trust in intelligence activities and the safeguards in place to protect personal information, the Intelligence Community will provide, to the maximum extent feasible, descriptions of how personal information is protected, prepared in a manner designed to enhance public understanding, and descriptions, including any issues or challenges, consistent with national security requirements, of the status of implementation efforts.

M. Intelligence Community Elements Should Identify Existing Data Security and Access and Data Quality Procedures that Protect SIGINT.

We believe that existing Intelligence Community and Intelligence Community element policies provide foundational requirements for the protection of the personal information of all persons, regardless of nationality. For example, existing procedures require Intelligence Community elements to include personal information in intelligence products only as consistent with applicable Intelligence Community standards for accuracy and objectivity. In addition to minimization procedures, PPD-28 requires Intelligence Community elements to have procedures governing data security and access. To that end, the Intelligence Community should identify and publicly disclose, to the extent consistent with national security concerns, existing data security, access, and data quality procedures that satisfy the PPD-28 requirements.

N. Intelligence Community Elements Must Have the Flexibility to Deviate from their PPD-28 Implementing Procedures After Receiving Senior Level Approval.

It is important that elements have the ability to deviate from their procedures when national security requires doing so, but only with approval at a senior level within the Intelligence Community element and notice to the DNI and the Attorney General.

II. Status of Intelligence Community's Implementation of Section 4

The ODNI, in consultation with the Attorney General, is working to ensure that all Intelligence Community elements establish policies and procedures that comply with PPD-28. These procedures should be consistent with the principles discussed in Section I above and any additional Intelligence Community policies, standards, procedures, or guidance the Director of National Intelligence may issue. Based on current progress, ODNI assesses that all elements of the Intelligence Community are on track to have policies and procedures in place by January 17, 2015.

The National Security Agency/Central Security Service (NSA/CSS) has been developing a set of supplemental procedures to build the requirements of PPD-28 into the policy framework that governs the U.S. SIGINT System. The set of procedures NSA/CSS is developing will serve to supplement the preexisting procedures applicable to the information and data deemed to be covered by PPD-28. The NSA/CSS procedures are titled "Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of SIGINT Information and Data Containing Personal Information of Non-United States Persons." The implementation of PPD-28 requirements by means of a single, releasable document will foster transparency.

The remaining Intelligence Community elements are still in the process of determining what, if any, impact PPD-28 will have on their existing policies and procedures. It is likely that the changes they will be required to make will be narrower than NSA's, because other Intelligence Community elements are primarily consumers of intelligence information derived

from SIGINT only after it has been evaluated and disseminated by the collecting agency, in accordance with that agency's SIGINT minimization procedures. CIA, for example, has current policies, processes, access controls, or training in place or will create additional measures to ensure protection of personal information obtained via SIGINT activities, with the goal of consistent implementation across CIA. To that end, CIA is drafting an updated policy to encompass the safeguarding of personal information consistent with PPD-28 expectations. CIA will designate a senior Agency officer(s) to oversee compliance with PPD-28, in coordination with other relevant oversight entities, as appropriate.

III. Conclusion

The Intelligence Community is committed to protect the personal information of all people around the world, regardless of their nationality. The Intelligence Community is prepared to establish policies and procedures based on the principles discussed above that provide protections for personal information collected through SIGINT. While each Intelligence Community element will be required to have procedures specifically adapted to its mission, we believe that the underlying requirements articulated above not only satisfy the basic requirements of the PPD but, in many cases, also afford additional appropriate protections beyond what the PPD requires. Based on current progress, ODNI assesses that all elements of the Intelligence Community are on track to have policies and procedures in place by January 17, 2015.