OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Status of Implementation of PPD-28:

Response to the PCLOB's Report

- October 2018 -

LEADING INTELLIGENCE INTEGRATION

[PAGE INTENTIONALLY LEFT BLANK]

Status of Implementation of PPD-28

About this Report

This report was prepared by the Office of Civil Liberties, Privacy, and Transparency (CLPT) of the Office of the Director of National Intelligence (ODNI). It was prepared in consultation with other ODNI components with relevant responsibilities, and with counterparts in relevant elements of the Intelligence Community (IC). This report outlines the status of the IC's implementation of Presidential Policy Directive-28, Signals Intelligence (PPD-28), and responds to the report on PPD-28 by the Privacy and Civil Liberties Oversight Board (PCLOB).

Summary

PPD-28 remains in full force and effect. As a formal presidential directive, it has the force of law within the Executive Branch, and compliance is mandatory. As described further below, the IC has systematically implemented the requirements of PPD-28 to ensure that U.S. signals intelligence (SIGINT) activities continue to include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides. IC elements have prepared and published the policies called for by PPD-28, and have been following those policies in conducting their activities.

Section 5 of PPD-28 encourages the PCLOB to provide the President with a report that assesses implementation of any matters contained within PPD-28 that fall within the PCLOB's mandate.[1] The PCLOB issued its report to the President and provided it to Congress in January 2017. [2] The PCLOB PPD028 report was subject to a Freedom of Information Act request, which prompted an interagency review to ensure information was redacted as appropriate. The redacted document is available on the PCLOB's public website, www.pclob.gov.

This report describes how the IC has implemented the four recommendations made by the PCLOB regarding PPD-28.

PPD-28

PPD-28 reinforces longstanding intelligence practices that protect privacy and civil liberties, while requiring agencies to systematically document and implement new processes and procedures. As stated in PPD-28, the United States, like other nations, has gathered intelligence

[1] According to the PCLOB's website, https://www.pclob.gov/:

> Comprised of four part-time members and a full-time chairman, the Board is vested with two fundamental authorities; (1) To review and analyze actions the executive branch takes to protect the nation from terrorism, ensuring the need for such actions is balanced with the need to protect privacy and civil liberties and (2) To ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the nation against terrorism.

[2] Privacy and Civil Liberties Oversight Board, Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities (PCLOB PPD-28 Report).

throughout its history to ensure that national security and foreign policy decision makers have access to timely, accurate, and insightful information. The collection of SIGINT is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm. At the same time, the IC's SIGINT activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

Section 1 of PPD-28 sets forth certain general principles for the conduct of SIGINT activities. In sum, SIGINT shall be authorized by and undertaken only in accordance with the law; privacy and civil liberties shall be integral considerations in the planning of SIGINT activities; SIGINT shall be collected exclusively where there is a foreign or counterintelligence purpose, and not for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; the collection of foreign private commercial information or trade secrets is authorized only to protect national security, and not to afford a competitive advantage to U.S. companies and U.S. business sectors commercially; and SIGINT activities shall be as tailored as feasible.

Section 2 provides that when the United States collects non-publicly available SIGINT in bulk, it shall use that data only for six specific purposes. Section 3 states that it is essential that national security policymakers consider carefully the value of SIGINT activities in light of the risks entailed in conducting these activities, and requires senior leadership involvement in the processes for establishing SIGINT priorities and requirements, and reviewing sensitive targets.

Section 4 of PPD-28 calls on each IC element to update existing or issue new policies and procedures to implement principles for safeguarding all personal information collected through SIGINT, regardless of nationality and consistent with technical capabilities and operational needs.

Implementation

Shortly after the President issued PPD-28, the ODNI established a multidisciplinary interagency working group to discuss a common approach to developing additional safeguards that protect personal information, recognizing that every IC element has different mission needs and requirements. The working group members represented IC mission and technology functions as well as IC legal, policy, and civil liberties and privacy offices. In approaching this task, the group focused on developing key principles to inform all IC 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. This implementation work resulted in the preparation and issuance of a 180-day interim progress report, published in October of 2014.

In January 2015, the IC elements completed their work in reviewing and updating policies and procedures pursuant to Section 4 of PPD-28. The ODNI published links to IC policies and procedures for PPD-28 in this table. These policies and procedures were developed and finalized in a coordinated manner across the IC. As required by PPD-28, these policies and procedures

were developed under the direction of, and in coordination with, the DNI, and in consultation with the Attorney General.

When the ODNI published links to IC elements' PPD-28 policies and procedures, ODNI highlighted certain key areas:[3]

- Limits on retention: IC elements must delete non-U.S. person information collected through SIGINT five years after collection unless the information has been determined to be relevant to, among other things, an authorized foreign intelligence requirement, or if the DNI determines, after considering the views of the ODNI Civil Liberties Protection Officer and agency privacy and civil liberties officials, that continued retention is in the interest of national security.

- Dissemination Restrictions: IC elements have always disseminated intelligence information because it is relevant to foreign intelligence requirements. PPD-28 now explicitly requires that information about a person may not be disseminated solely because he or she is a non-U.S. person. All agency policies contain this restriction, and the ODNI has issued a revised directive (*i.e.*, Intelligence Community Directive (ICD) 203, Analytic Standards) to all IC elements to reflect this requirement.

- Oversight, Training & Compliance Requirements: IC elements have always had strong training, oversight, and compliance programs to ensure we were protecting the privacy and civil liberties of U.S. persons. In response to PPD-28, IC elements have added new training, oversight, and compliance requirements. They have developed and deployed mandatory training programs to ensure that intelligence officers know and understand their responsibility to protect the personal information of all people, regardless of nationality.

In addition, the ODNI has issued two Intelligence Community Standards (ICS's) governing implementation of PPD-28. These standards were issued under the auspices of Intelligence Community Directive (ICD) 107, Civil Liberties, Privacy, and Transparency.[4] In February, 2015, the ODNI published ICS Standard 107-01, Continued Retention of SIGINT Under PPD-28. PPD-28 requires IC elements to delete non-U.S. person information collected through SIGINT five years after collection unless the information has been determined to be relevant to, among other things, an authorized foreign intelligence requirement, or if the DNI determines, after considering the views of the ODNI Civil Liberties Protection Officer and agency privacy and civil liberties officials, that continued retention is in the interest of national security. ICS 107-01 established the process to seek a continued retention determination by the DNI.

[3] This section is excerpted from the ODNI's January 2015 statement.

[4] ICD 107 was originally issued in 2012 and covered civil liberties and privacy. It was updated and re-issued in 2018 by DNI Daniel Coats to include transparency within its ambit.

In July 2016, the ODNI published ICS 107-02, Reporting Significant Compliance Issues Involving Personal Information under PPD-28 to the DNI. ICS 107-02 was originally issued in February 2016 and was publicly released in keeping with the Principles of Intelligence Transparency for the Intelligence Community. PPD-28 requires that IC elements promptly report to the DNI significant compliance issues involving personal information of any person, regardless of nationality, collected as a result of SIGINT activities. The DNI will then determine what, if any, corrective actions are necessary. ICS 107-02 establishes the process for reporting such issues to the DNI.

The IC reported its progress in implementing PPD-28 and related reforms through three annual reports, posted on IC on the Record. These reports described developments related to the IC's efforts to implement privacy protections and enhance intelligence transparency.

Current Status

In 2017, the Trump Administration conducted an interagency review of PPD-28 and determined that it should remain in place. Accordingly, PPD-28 remains in full force and effect as a formal presidential directive, which means it continues to have the force of law within the Executive Branch. Compliance remains mandatory. IC elements continue to implement PPD-28's requirements.

PCLOB PPD-28 Report

Section 5 of PPD-28 encourages the PCLOB to provide the President with a report that assesses implementation of any matters contained within PPD-28 that fall within the PCLOB's mandate. The PCLOB issued its report to the President and provided it to Congress in January 2017. The IC then conducted an interagency review to ensure information was appropriately redacted consistent with applicable law.

As noted in the PCLOB PPD-28 Report, the body of the report describes certain aspects of the IC's implementation of PPD-28 and includes four recommendations. This part of the report was adopted by all four extant members of the PCLOB. The report also includes two separate statements, one by Board Members Rachel Brand and Elisebeth Collins, and one by Board Members James Dempsey and Patricia Wald.

PCLOB Recommendations and IC Response.

The PCLOB PPD-28 Report made four recommendations.

Recommendation 1: The Board recommends that the National Security Council ("NSC") and ODNI issue criteria for determining which activities or types of data will be subject to PPD-28's requirements.

Response: As noted when the ODNI's first posted links to the IC elements' PPD-28 procedures in the first SIGINT reform report, "[a]lthough similar in many respects, agency procedures are

not identical. The differences reflect that not all agencies conduct SIGINT collection and that agencies have different mission requirements."

As stated on pages 3 of the PCLOB PPD-28 Report, "[t]he ways in which the IC elements have implemented the directive to date have varied based on their missions and authorities, access to signals intelligence information, and information systems." As previously discussed, the IC carefully reviewed and considered how to implement PPD-28 through an extensive interagency coordination process led by the ODNI and including all IC elements, in close consultation with the Department of Justice. This process took into account the need for policies and procedures to differ based on the mission and activities of the IC elements involved. For example, the policies of agencies that *collect* raw SIGINT necessarily differ from agencies that have no collection authorities, but that instead *consume* disseminated SIGINT reports from collectors.

For the collecting agencies, this process included careful review of the programs and activities that IC elements contemplated being subject to PPD-28 policies. As a general matter, the identity of the programs and activities to which PPD-28 applies remains classified to protect national security. That said, a specific public statement on scope was authorized as part of the so-called Privacy Shield Framework. This statement was included in the letter from the ODNI General Counsel dated February 22, 2016, which is now part of the Privacy Shield Framework. The letter was extensively reviewed and coordinated by relevant IC elements and other government agencies. As stated in the letter, "[c]ollection under Section 702 [of the Foreign Intelligence Surveillance Act (FISA)] is considered SIGINT subject to the requirements of PPD-28." The Privacy Shield Framework, including this letter from the ODNI General Counsel, has been reaffirmed by the Trump Administration. Thus, it is the current official position of the United States Government (including the IC) that PPD-28 applies to collection under Section 702 of FISA.

The ODNI continues to work closely with IC elements to ensure that they are appropriately implementing PPD-28, including its application to agency programs and activities. The IC has extensive interagency coordination and review mechanisms in place to ensure that IC activities are appropriately aligned and compliant with applicable legal and policy requirements, and is using those mechanisms to ensure proper coordination takes place regarding PPD-28. In addition, civil liberties and privacy officials of IC elements regularly engage with one another as part of the IC Civil Liberties and Privacy Council to address issues of common concern, including implementation of PPD-28. The ODNI believes that these measures collectively ensure that PPD-28's protections are being applied to programs and activities with appropriately careful consideration of the purpose and intent of PPD-28, in light of the evolving technological and geopolitical environment in which IC elements operate.

Recommendation 2: IC elements should consider both the mission and privacy implications of applying PPD-28 to multi-sourced systems.

Response: This recommendation is primarily directed at CIA's application of PPD-28 to certain "multi-sourced systems" at CIA (i.e., a system that contains information collected through more than one intelligence discipline). As stated in the report:

> In order to ensure that all information subject to PPD-28 receives PPD-28 protections, the CIA has, at times, opted to apply PPD-28 protections to all information within multi-sourced systems even if the CIA assesses that PPD-28 does not apply to all data within the systems…. The Board appreciates CIA's efforts to comply with the directive and recognizes that it may be both more protective of civil liberties and more economical from a technical, training and resource perspective to be over-inclusive in applying PPD-28 provisions… As the CIA continues to review its holdings for signals intelligence, the Board expects that the CIA will seek out solutions that comply with PPD-28's requirements.

The CIA has accepted the PCLOB's recommendation and has reviewed the application of PPD-28 to its multi-sourced systems, considering both the mission and privacy implications of applying PPD-28 to such systems, and has briefed the PCLOB on the results of this review.

Recommendation 3: The Board recommends that the NSC and ODNI ensure that any IC elements obtaining first-time access to unevaluated signals intelligence update their PPD-28 use, retention and dissemination practices, procedures, and trainings before receiving any unevaluated data.

Response: Consistent with the PCLOB's recommendation, the ODNI will exercise its review and approval authorities to ensure that an IC element has reviewed and updated its PPD-28 implementing policies, as appropriate, as part of the process for seeking approval to obtain access to unevaluated SIGINT, pursuant to 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 text below provides background on the Raw SIGINT Availability Procedures.

On January 3, 2017, the Director of National Intelligence, in coordination with the Secretary of Defense, issued the Raw SIGINT Availability Procedures. The procedures were approved by the Attorney General on January 3, 2017. Section 2.3 of E.O. 12333 provides that elements of the 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." The Raw SIGINT Availability Procedures implement this provision.

The procedures permit IC elements to have access, under appropriate conditions, to the unevaluated or unminimized (i.e., "raw") SIGINT information that the NSA collects pursuant to E.O. 12333, thus enabling elements to bring their own analytic expertise to reviewing that information and to use that information in support of their own missions. The procedures therefore provide an important mechanism for enhancing information sharing, integration, and collaboration in the IC.

The procedures:

- Only allow IC elements to access raw SIGINT in circumstances where the information will further a foreign intelligence or counterintelligence mission in a significant way.
- Do not permit raw SIGINT to be accessed for law enforcement purposes.
- Do not apply to information collected under the Foreign Intelligence Surveillance Act, including Section 702.
- Establish rules that a recipient IC element must follow when accessing, processing, or retaining raw SIGINT, or disseminating information derived from SIGINT. These rules closely follow those used by the NSA.
- Set up extensive training, auditing, oversight, and compliance requirements that are comparable to the NSA's for similar activities.
- Require periodic reauthorization of access and high-level reviews of activities conducted under the procedures.

Regarding PPD-28, the Raw SIGINT Availability Procedures make clear that an IC element requesting access to raw SIGINT must comply with PPD-28 and its implementing policies.

The ODNI has publicly released the Raw SIGINT Availability Procedures with limited redactions to protect classified sources and methods.

Following Attorney General approval in January 2017 of the Raw SIGINT Availability Procedures, ODNI led a working group with the relevant interagency offices to develop, coordinate, and execute implementing guidance for the procedures. As required by the procedures, ODNI CLPT developed and coordinated oversight and compliance guidance for a requesting IC element's handling of raw SIGINT. Pursuant to the procedures, IC elements may not access raw SIGINT until they have met certain requirements, including the establishment of a compliance program comparable to that of NSA, with the same types of privacy protective rules.

The IC process through which the ODNI CLPT will review a requesting IC element's oversight and compliance program remains underway and has not yet been completed with respect to any IC element. Accordingly, ODNI CLPT has not yet approved any oversight and compliance program, and NSA has not yet granted any IC element access to raw SIGINT under the Raw SIGINT Availability Procedures.

Recommendation 4: The Board recommends that to the extent consistent with the protection of classified information, IC elements promptly update their public PPD-28 procedures to reflect any pertinent future changes in practices and policy, including those changes due to issuance of new procedures under Section 2.3 of E.O. 12333.

Response: Consistent with this recommendation, the ODNI will exercise its review and approval authorities to ensure that IC elements promptly update their public PPD-28 procedures to reflect any pertinent changes in practices and policies, including those changes due to issuance of new

procedures under Section 2.3 of E.O. 12333.[5] Determinations on what can be made public will be made consistent with ICD 107, Civil Liberties, Privacy, and Transparency, and with the Principles of Intelligence Transparency for the IC.[6]

[5] Note that Section 4(b) of PPD-28 provides:

> Within 1 year of the date of this directive, IC elements shall update or issue new policies and procedures as necessary to implement section 4 of this directive, in coordination with the DNI. To enhance public understanding of, and promote public trust in, the safeguards in place to protect personal information, these updated or newly issued policies and procedures shall be publicly released to the maximum extent possible, consistent with classification requirements.

[6] Note that, subsequent to the issuance of the PCLOB's PPD-28 Report, the National Counterterrorism Center began receiving unevaluated 702-acquired information as authorized by the Foreign Intelligence Surveillance Court. NCTC's 702 minimization procedures do not authorize NCTC to directly engage in targeting or acquisition, but rather authorize NCTC to receive certain 702-acquired information. Consistent with this PCLOB recommendation, ODNI is in the process of updating its publicly posted policy to reflect NCTC's access to certain unminimized 702 information.