SIDLEY AUSTIN LLP
SIDLEY

October 26, 2015

SAFEGUARDS AND OVERSIGHT OF U.S. SURVEILLANCE UNDER SECTION 702

In *Schrems v. Data Protection Commissioner*, the Court of Justice of the European Union invalidated the US-EU Safe Harbor agreement on the basis that the European Commission had failed to sufficiently assess the protection of personal data of Europeans under the U.S. data protection regime. The Court alluded to U.S. surveillance activities under the PRISM program authorized by Section 702 of the Foreign Intelligence Surveillance Act, and appeared to assume U.S. law permits mass surveillance of Europeans with few limits, little clarity, and no opportunity for redress. However, the Court did not actually review or assess the applicable legal authorities, remedies, or array of checks and balances, safeguards, and independent oversight. If it had done so, it would have found numerous overlapping controls that assure that such surveillance is neither massive nor indiscriminate, but instead targeted to specific individuals and limited purposes, and provides legal remedies for Europeans. Indeed, prior to the scheduled expiration of the 702 program in 2017, U.S. congressional oversight committees will likely be comparing whether privacy safeguards in place for similar foreign programs are as effective as those of Section 702.

Significantly, the independent Privacy and Civil Liberties Oversight Board reviewed surveillance under Section 702 and found: "[T]the Section 702 program is **not based on the indiscriminate collection of information in bulk**. Instead the program consists entirely of **targeting specific [non-U.S.] persons about whom an individualized determination has been made**."[1] Key safeguards and controls include:

- Two cabinet-level officials must jointly **certify to a court** and provide sworn evidence that surveillance in question targets only specific persons for the specific purposes specified by law.
- Section 702 **limits the purposes for which intelligence can be gathered** to foreign intelligence, which includes counter-terrorism, counter-proliferation, and counter-espionage efforts. In PPD-28, President Obama made these limits more specific and extended them to all signals intelligence collection.
- **Court-approved targeting and data minimization procedures** limit the collection, use, dissemination, and retention of obtained information; legally-required data minimization procedures have been formally extended to non-U.S. persons.
- **Europeans have the right to judicial redress** under the Foreign Intelligence Surveillance Act, which allows any aggrieved party, including non-U.S. persons to litigate alleged violations of FISA Section 702.
- Courts, Congress, independent Inspectors General, and privacy and civil liberties officers in each intelligence agency provide **independent oversight of surveillance** activities.
- In PPD 28, President Obama declared, "[O]ur signals intelligence 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."[2]

***

Cameron F. Kerry
Senior Counsel, Sidley Austin LLP
Former General Counsel; Acting Secretary,
U.S. Department of Commerce

Alan Charles Raul
Partner, Sidley Austin LLP
Former Vice Chairman,
Privacy and Civil Liberties Oversight Board

[1] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 702 of the Foreign Intelligence Surveillance Act* 111 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.
[2] Presidential Policy Directive/PPD-28 (Jan. 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

SIDLEY AUSTIN LLP
SIDLEY

October 26, 2015

SAFEGUARDS AND OVERSIGHT OF U.S. SURVEILLANCE UNDER SECTION 702

This paper details the scope and limits of United States surveillance activities conducted under Section 702 of the Foreign Surveillance Intelligence Act. This is the surveillance authority specifically referenced by the Court of Justice of the European Union in *Schrems v. Data Protection Commissioner*. These factors demonstrate that American surveillance under Section 702 is neither massive nor indiscriminate. Rather, the reality is that there are checks and balances and safeguards in place to protect civil liberties and privacy. They further show that Congress, the executive branch, and independent boards provide meaningful oversight.

In brief, data collection under Section 702 has been found by the independent Privacy and Civil Liberties Oversight Board to be targeted to specific individuals, and applicable statutory conditions and presidential directives require that Section 702 surveillance be conducted only for foreign intelligence purposes, subject to meaningful data protection requirements as well as extensive oversight from all branches of government.

Perhaps most significantly, national security surveillance in the U.S. is subject to extensive independent oversight by the Privacy and Civil Liberties Oversight Board. The PCLOB is legally authorized to obtain full access to even the most sensitive classified programs, and is empowered to issue mandatory subpoenas to intelligence agencies and other parties. The authority, access, and stature of the PCLOB may be unmatched in any other jurisdiction. Indeed, prior to the scheduled expiration of the 702 program in 2017, U.S. congressional oversight committees will likely be comparing whether privacy safeguards in place for similar foreign programs are as effective as those of Section 702.

With regard to redress, the Foreign Intelligence Surveillance Act expressly provides that any aggrieved party, including non-U.S. persons, is authorized to litigate alleged violations of FISA Section 702 (only actual "agents of foreign powers" are barred from litigating).

Finally, the President has extended legally-required data "minimization" procedures to foreign citizens outside the U.S., and explicitly acknowledged the need to respect the dignity of all persons, regardless of their nationality or country of residence.

EU Law and Surveillance

- The CJEU *Schrems* decision stated that the "adequacy" of surveillance law depends on the existence of protections that are "essentially equivalent" to protections under EU law.
- Prior European cases evaluating surveillance measures have outlined several factors to consider when evaluating the consistency of such laws with the Charter of Fundamental Rights and other European instruments. The factors are: predicate offenses that are clearly detailed, specific targets, limited timeframes, procedural clarity, data protections, data destruction, oversight, and redress.[3] The CJEU cited these decisions and factors for "the level of protection guaranteed in the EU legal order" against which the U.S. level of protection is supposed to be measured.

[3] *See, e.g., Weber & Saravia v. Germany*, No. 54934/00 (Eur. Ct. H.R. 2006).

- The Article 29 Working Party, though it lacks substantial oversight power over European intelligence agencies, has stressed the need for oversight and transparency, calling on all countries—within and without Europe—to provide legislative and independent oversight of intelligence activities.[4] Likewise, the Working Party has advocated for nations to provide more transparency as to "how [surveillance] programmes work and what the supervisors do and decide," as well as "maximising public awareness."[5]
- The outline below demonstrates that the U.S. surveillance provision at issue in the *Schrems* decision, FISA Section 702, satisfies the above factors and complies with the Working Party's call for transparency.

Section 702 of Foreign Intelligence Surveillance Act

- To collect communications and information passing through electronic communications providers located in the U.S. under this section, the government must obtain:
    1. Joint Cabinet-Level Certification: The Attorney General (AG) and Director of National Intelligence (DNI) must jointly certify to the FISA court (Foreign Intelligence Surveillance Court, or FISC), under oath and with supporting documentation, that:
        - "a significant purpose of the acquisition is to obtain foreign intelligence,"[6] which is limited to "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists"[7];
        - court-approved targeting procedures are in place that ensure that the acquisition of information is limited to "target[ed] persons"[8]; and
        - minimization procedures that must be approved by a court are in place that (1) "are reasonably designed … to minimize the acquisition and retention" of information of non-targeted persons and (2) require that that such information not to be disseminated, except in limited, enumerated instances.[9]
    2. Court Approval: The FISC must determine that the certification contains all of the required elements and that the specified targeting and minimization procedures are sufficient.[10]

[4] *See, e.g.*, Article 29 Data Protection Working Party, 819/14/EN WP 215, *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes*, at 8–11 (Apr. 10, 2014), http://www.cnpd.public.lu/fr/publications/groupe-art29/wp215_en.pdf.
[5] *Id.* at 12.
[6] 50 U.S.C. § 1881a(g).
[7] Presidential Policy Directive/PPD-28 (Jan. 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
[8] 50 U.S.C. § 1881a(d), (g).
[9] 50 U.S.C. §§ 1801(h), 1881a(e), (g). See below for discussion of presidentially-mandated extension of "minimization" procedures to non-U.S. persons.
[10] 50 U.S.C. § 1881a(i).

- Only under limited, emergency situations may the AG and DNI delay seeking court approval for up to seven days, after which court approval must be obtained.[11]

3. Joint Cabinet-Level Authorization: The AG and DNI must then jointly authorize "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[12]

   - This authorization can be served only on electronic communication service providers, which are defined as telecommunications carriers and other communications providers.[13]
   - No other U.S. entities besides electronic communications providers are subject to Section 702 orders.[14]

This Law and These Procedures Provide Significant Protections

- **The Purpose Is Specified.**
  - AG and DNI must jointly certify to the court (and provide sworn evidence) that a significant purpose of collecting communications is "to obtain foreign intelligence information," noting the specific foreign power and reason for the surveillance.[15]
- **Specificity of Targeting.**
  - AG and DNI must jointly certify to the court (and provide sworn evidence) that their analysts have identified particular persons "reasonably believed to be located outside the United States" and that their collection will limited to communications related to those persons connected to specific foreign powers; the surveillance must be conducted using court-approved procedures that are in place to prevent collection of communications of persons in US.[16]
  - The President has directed NSA to "follow protocols designed to protect the privacy of ordinary people" regardless of nationality.[17]
  - As found by the independent Privacy and Civil Liberties Oversight Board (PCLOB): "[T]the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead the program consists entirely of targeting specific [non-U.S.] persons about whom an individualized determination has been made."[18]

[11] 50 U.S.C. § 1881a(g)(1)(B).
[12] 50 U.S.C. § 1881a(a)
[13] *See* 50 U.S.C. § 1801(4).
[14] *See* 50 U.S.C. § 1881a(h)
[15] 50 U.S.C. § 1881a(g)(2)
[16] 50 U.S.C. § 1881a(d), (g).
[17] President Barack Obama, Remarks on Review of Signals Intelligence (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[18] PCLOB, *Report on the Telephone Records Program Conducted under Section 702 of the Foreign Intelligence Surveillance Act* 111 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.

- **Limited Timeframe**
  - Section 702 authorizations are limited to one year.
  - To continue beyond 1 year, the AG and DNI must make *another* joint, Cabinet-level certification and obtain court approval *again*.[19]
- **Clarity of Process**
  - Section 702 describes in detail the certifications necessary to collect communications and the targeting and minimization procedures to be used in doing so.[20] (The statutory provisions comprising Section 702 are attached in full.)
  - Court orders and opinions regarding Section 702 certifications have been made available to the public. [21]
  - AG has submitted guidelines for collection of information, which have been reviewed and approved by the court, and which the DNI has made publicly available.[22]
- **Data Protection Safeguards**
  - Government is bound by court-approved data minimization procedures that limit access to and use of information collected.[23]
  - Information collected is not used for purposes outside those enumerated in the statute and in PPD-28.[24]
  - PPD-28 expressly provides[25]:
    - Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.

[19] 50 U.S.C. § 1881a(a).
[20] 50 U.S.C. § 1881a(d), (e), (g).
[21] ODNI, Declassified Documents Concerning FISA, IC on the Record (Mar. 3, 2015), http://icontherecord.tumblr.com/post/112610953998/release-of-documents-concerning-activities-under.
[22] ODNI, Minimization Procedures (July 24, 2014), http://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf
[23] 50 U.S.C. § 1806(a); 50 U.S.C. § 1881a(g)(2)(A).
[24] Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, September 8, 2013. Available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage.
[25] *See* Presidential Policy Directive/PPD-28, sec. 1(b), (c) &(d)("Principles Governing the Collection of Signals Intelligence").

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

- **Deletion/Destruction**
  - Data collected must be deleted five years after the expiration of a certification absent a determination of relevance or secret meaning.[26]
  - Inadvertently collected information must be destroyed.[27]
- **Oversight**
  - Judicial review:
    - A court must approve certifications jointly submitted by the AG and DNI authorizing collection of foreign intelligence information.[28]
    - A court must approve Intelligence Community's targeting and data minimization procedures.[29]
    - Electronic service providers may challenge AG/DNI directives before the court.[30]
    - Aggrieved persons can file suit as described below.
  - Additional Independent Review:
    - PCLOB and the President's Review Group on Intelligence and Communications Technologies have conducted public reviews of the program with full access to classified information, including the ability to review precisely what actionable intelligence was provided by Section 702.[31]

[26] 2014 NSA 702 Minimization Procedures, Section 3(c)(1).
[27] 50 USC 1806(i) *as limited by* 2014 NSA 702 Minimization Procedures, Section 3(d). (Extended to non-U.S. persons via PPD-28.)
[28] 50 U.S.C. § 1881a(i).
[29] 50 U.S.C. § 1881a(i).
[30] 50 U.S.C. § 1881a(h)(4).
[31] *See, e.g.*, PCLOB, *Report on the Telephone Records Program Conducted under Section 702 of the Foreign Intelligence Surveillance Act* 111 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf; President's Review Group on Intelligence and Communications Technology, Liberty and Security in a Changing World (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

- Both the PCLOB and the President's Review Group reported that the Section 702 surveillance program has led to identification of terrorist operatives and to the prevention of terrorist attacks—not only in the United States but also more than 40 such attacks abroad.[32]
- Inspectors General are authorized to review compliance with the targeting and data minimization procedures.[33]

▪ Reporting requirements:

- DOJ and DNI as well as the NSA, CIA, and FBI must provide annual assessment on compliance with targeting and minimization procedures to the FISC and Congress.[34]
- DOJ provides a semi-annual report on implementation of 702 to the FISC and Congress.[35]

▪ Transparency:

- Government is required to issue transparency reports, detailing the number of certifications, FISA orders, and targets.[36]
- 2014 Transparency Report "estimated number of targets affected" under Section 702 was 92,707.[37]
- Electronic communications providers may publish transparency reports.[38]

o **Redress**

▪ All aggrieved persons (excepting only foreign powers and their agents) are expressly authorized to file suit against the government and its agents for unauthorized electronic surveillance.[39]

---

[32] *See* PCLOB, *Report on Section 702*, at 105–06, https://www.pclob.gov/library/702-Report.pdf; President's Review Group on Intelligence and Communications Technology, *Liberty and Security in a Changing World* , at 119 n.119, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[33] 50 U.S.C. § 1881a(l)(2).
[34] *See, e.g.*, ODNI, *Signals Intelligence Reform 2015 Anniversary Report*, http://icontherecord.tumblr.com/ppd-28/2015/.
[35] 50 U.S.C. § 1881a(l)(1).
[36] *See, e.g.*, ODNI, 2013 Transparency Report (June 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013; NSA Dir. of Civil Liberties and Privacy Office Report (Apr. 16, 2014), http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.
[37] ODNI, *2014 Statistical Transparency Report* (Apr. 22, 2015), http://www.dni.gov/files/icotr/CY14%20Statistical%20Transparency%20Report.pdf.
[38] *See, e.g.*, Letter from James M. Cole, Dep. Att'y Gen., to Colin Stretch et al. (Jan. 27, 2014) (permitting internet companies to report aggregate data regarding national security letters), *available at* http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf.
[39] 50 U.S.C. § 1810; *see also ACLU v. Clapper*, No. 14-42, at 25– (2d Cir. May 7, 2015) (concluding that standing existed to challenge surveillance measures under Section 215 of the PATRIOT Act because surveillance was indiscriminate).

- If the government intends to use information in any law-enforcement proceeding, it must provide notice to the individual, who can then challenge that use.[40]
- Non-US citizens have private right of action to sue government for alleged violations of § 702. [41]
- Significant civil and criminal penalties for violations of statutory authorizations.[42]

Section 702 Surveillance Is Subject to Presidential Policy Directive PPD-28 that Extends Minimization Rules and Other Data Protections to Non-U.S. Persons

- **Presidential Policy Directive 28.** Issued in January 2014 (copy of PPD-28 attached in full).
  - President Obama: "the directive makes clear that the United States only uses signals intelligence for legitimate national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary people."[43]
  - Non-U.S. Persons are specifically protected, as directed by the President:
    - "[O]ur signals intelligence 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.[44]
  - "[T]he United States conducts signals intelligence activities [only] for authorized foreign intelligence and counterintelligence purposes."[45]
  - PPD-28 imposes **"**limits … to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside."[46]
  - In January 2015, the Privacy and Civil Liberties Oversight Board issued the Recommendations Assessment Report, finding that the government had already implemented many aspects of the PPD-28.[47]
  - The Office of DNI also released the Signals Intelligence Reform 2015 Anniversary Report, documenting the extensive reforms made in the executive agencies.[48]

Additional Developments to Note

- **USA Freedom Act:** enacted on June 2, 2015 to end "bulk" collection of metadata under Patriot Act § 215.

---

[40] *See, e.g.*, *Mapp v. Ohio*, 367 U.S. 643, 657 (1961).
[41] *See, e.g.*, 50 U.S.C. § 1810 (excepting only persons that are agents of a foreign power).
[42] 50 U.S.C. §§ 1809 (criminal penalties), 1810 (liquidated damages).
[43] President Barack Obama, Remarks on Our Signal Intelligence Review (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[44] Presidential Policy Directive/PPD-28 (Jan. 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
[45] *Id.*
[46] *Id.*
[47] *See* PCLOB, Recommendation Assessment Report (Jan. 29, 2015), https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf.
[48] ODNI, *Signals Intelligence Reform 2015 Anniversary Report*, http://icontherecord.tumblr.com/ppd-28/2015/.

- **Judicial Redress Act:** has passed House of Representatives and awaits consideration in Senate; will authorize non-U.S. Persons to litigate claims for Privacy Act violations in US Courts.
- **LEADS Act:** Pending in the Senate; would generally prohibit extraterritorial search warrants, and require US to utilize MLAT process except in cases where the target of the search warrant is a US person.

***

Cameron F. Kerry
Senior Counsel, Sidley Austin LLP
Former General Counsel; Acting Secretary,
U.S. Department of Commerce

Alan Charles Raul
Partner, Sidley Austin LLP
Former Vice Chairman,
Privacy and Civil Liberties Oversight Board

(2) Foreign Intelligence Surveillance Court; Court

The terms ''Foreign Intelligence Surveillance Court'' and ''Court'' mean the court established under section 1803(a) of this title.

(3) Foreign Intelligence Surveillance Court of Review; Court of Review

The terms ''Foreign Intelligence Surveillance Court of Review'' and ''Court of Review'' mean the court established under section 1803(b) of this title.

(4) Electronic communication service provider

The term ''electronic communication service provider'' means—

(A) a telecommunications carrier, as that term is defined in section 153 of title 47;

(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18;

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18;

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

(5) Intelligence community

The term ''intelligence community'' has the meaning given the term in section 401a(4) of this title.

(Pub. L. 95–511, title VII, § 701, as added Pub. L. 110–261, title I, § 101(a)(2), July 10, 2008, 122 Stat. 2437.)

REPEAL OF SECTION

Pub. L. 110–261, title IV, § 403(b)(1), July 10, 2008, 122 Stat. 2474, provided that, except as provided in section 404 of Pub. L. 110–261, set out as a note under section 1801 of this title, effective Dec. 31, 2012, this section is repealed.

PRIOR PROVISIONS

A prior section 701 of Pub. L. 95–511 was set out as a note under section 1801 of this title, prior to repeal by Pub. L. 110–261.

EFFECTIVE DATE OF REPEAL

Pub. L. 110–261, title IV, § 403(b)(1), July 10, 2008, 122 Stat. 2474, provided that, except as provided in section 404 of Pub. L. 110–261, set out as a Transition Procedures note under section 1801 of this title, the repeals made by section 403(b)(1) are effective Dec. 31, 2012.

§ 1881a. Procedures for targeting certain persons outside the United States other than United States persons

(a) Authorization

Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) Limitations

An acquisition authorized under subsection (a)—

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(c) Conduct of acquisition

(1) In general

An acquisition authorized under subsection (a) shall be conducted only in accordance with—

(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

(B) upon submission of a certification in accordance with subsection (g), such certification.

(2) Determination

A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.

(3) Timing of determination

The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—

(A) before the submission of a certification in accordance with subsection (g); or

(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

(4) Construction

Nothing in subchapter I shall be construed to require an application for a court order under such subchapter for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

(d) Targeting procedures

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall

adopt targeting procedures that are reasonably designed to—

(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(2) Judicial review

The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(e) Minimization procedures

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 1801(h) of this title or section 1821(4) of this title, as appropriate, for acquisitions authorized under subsection (a).

(2) Judicial review

The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(f) Guidelines for compliance with limitations

(1) Requirement to adopt

The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—

(A) compliance with the limitations in subsection (b); and

(B) that an application for a court order is filed as required by this chapter.

(2) Submission of guidelines

The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—

(A) the congressional intelligence committees;

(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

(C) the Foreign Intelligence Surveillance Court.

(g) Certification

(1) In general

(A) Requirement

Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

(B) Exception

If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.

(2) Requirements

A certification made under this subsection shall—

(A) attest that—

(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to—

(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

(ii) the minimization procedures to be used with respect to such acquisition—

(I) meet the definition of minimization procedures under section 1801(h) or 1821(4) of this title, as appropriate; and

(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;

(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this chapter;

(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;

(v) a significant purpose of the acquisition is to obtain foreign intelligence information;

(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

(vii) the acquisition complies with the limitations in subsection (b);

(B) include the procedures adopted in accordance with subsections (d) and (e);

(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—

(i) appointed by the President, by and with the advice and consent of the Senate; or

(ii) the head of an element of the intelligence community;

(D) include—

(i) an effective date for the authorization that is at least 30 days after the submis-

sion of the written certification to the court; or

(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

(3) Change in effective date

The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

(4) Limitation

A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

(5) Maintenance of certification

The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

(6) Review

A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).

(h) Directives and judicial review of directives

(1) Authority

With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—

(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) Compensation

The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(3) Release from liability

No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(4) Challenging of directives

(A) Authority to challenge

An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) Assignment

The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 1803(e)(1) of this title not later than 24 hours after the filing of such petition.

(C) Standards for review

A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

(D) Procedures for initial review

A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

(E) Procedures for plenary review

If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

(F) Continued effect

Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

(G) Contempt of Court

Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(5) Enforcement of directives

(A) Order to compel

If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) Assignment

The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 1803(e)(1) of this title not later than 24 hours after the filing of such petition.

(C) Procedures for review

A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

(D) Contempt of Court

Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(E) Process

Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

(6) Appeal

(A) Appeal to the Court of Review

The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

(B) Certiorari to the Supreme Court

The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(i) Judicial review of certifications and procedures

(1) In general

(A) Review by the Foreign Intelligence Surveillance Court

The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.

(B) Time period for review

The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

(C) Amendments

The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

(2) Review

The Court shall review the following:

(A) Certification

A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements.

(B) Targeting procedures

The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—

(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(C) Minimization procedures

The minimization procedures adopted in accordance with subsection (e) to assess

whether such procedures meet the definition of minimization procedures under section 1801(h) of this title or section 1821(4) of this title, as appropriate.

(3) Orders

(A) Approval

If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

(B) Correction of deficiencies

If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—

(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or

(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

(C) Requirement for written statement

In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

(4) Appeal

(A) Appeal to the Court of Review

The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

(B) Continuation of acquisition pending rehearing or appeal

Any acquisition affected by an order under paragraph (3)(B) may continue—

(i) during the pendency of any rehearing of the order by the Court en banc; and

(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

(C) Implementation pending appeal

Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

(D) Certiorari to the Supreme Court

The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(5) Schedule

(A) Reauthorization of authorizations in effect

If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

(B) Reauthorization of orders, authorizations, and directives

If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

(j) Judicial proceedings

(1) Expedited judicial proceedings

Judicial proceedings under this section shall be conducted as expeditiously as possible.

(2) Time limits

A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

(k) Maintenance and security of records and proceedings

(1) Standards

The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, or-

ders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(2) Filing and review

All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

(3) Retention of records

The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

(*l*) Assessments and reviews

(1) Semiannual assessment

Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to—

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

(2) Agency assessment

The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General—

(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(D) shall provide each such review to—

(i) the Attorney General;

(ii) the Director of National Intelligence; and

(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(3) Annual review

(A) Requirement to conduct

The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

(B) Use of review

The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

(C) Provision of review

The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—

(i) the Foreign Intelligence Surveillance Court;

(ii) the Attorney General;

(iii) the Director of National Intelligence; and

(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(Pub. L. 95–511, title VII, § 702, as added Pub. L. 110–261, title I, § 101(a)(2), July 10, 2008, 122 Stat. 2438.)

REPEAL OF SECTION

Pub. L. 110–261, title IV, § 403(b)(1), July 10, 2008, 122 Stat. 2474, provided that, except as provided in section 404 of Pub. L. 110–261, set out as a note under section 1801 of this title, effective Dec. 31, 2012, this section is repealed.

REFERENCES IN TEXT

This chapter, referred to in subsecs. (f)(1)(B) and (g)(2)(A)(iii), was in the original ''this Act'', meaning Pub. L. 95–511, Oct. 25, 1978, 92 Stat. 1783, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of this title and Tables.

Senate Resolution 400 of the 94th Congress, referred to in subsec. (*l*), was agreed to May 19, 1976, and was subsequently amended by both Senate resolution and public law. The Resolution, which established the Senate Select Committee on Intelligence, is not classified to the Code.

EFFECTIVE DATE OF REPEAL

Pub. L. 110–261, title IV, § 403(b)(1), July 10, 2008, 122 Stat. 2474, provided that, except as provided in section 404 of Pub. L. 110–261, set out as a Transition Procedures note under section 1801 of this title, the repeals made by section 403(b)(1) are effective Dec. 31, 2012.

§ 1881b. Certain acquisitions inside the United States targeting United States persons outside the United States

(a) Jurisdiction of the Foreign Intelligence Surveillance Court

(1) In general

The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this chapter, and such acquisition is conducted within the United States.

(2) Limitation

If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect. Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other subchapter of this chapter.

(b) Application

(1) In general

Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include—

(A) the identity of the Federal officer making the application;

(B) the identity, if known, or a description of the United States person who is the target of the acquisition;

(C) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—

(i) a person reasonably believed to be located outside the United States; and

(ii) a foreign power, an agent of a foreign power, or an officer or employee of a foreign power;

(D) a statement of proposed minimization procedures that meet the definition of minimization procedures under section 1801(h) or 1821(4) of this title, as appropriate;

(E) a description of the nature of the information sought and the type of communications or activities to be subjected to acquisition;

(F) a certification made by the Attorney General or an official specified in section 1804(a)(6) of this title that—

(i) the certifying official deems the information sought to be foreign intelligence information;

(ii) a significant purpose of the acquisition is to obtain foreign intelligence information;

(iii) such information cannot reasonably be obtained by normal investigative techniques;

(iv) designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(v) includes a statement of the basis for the certification that—

(I) the information sought is the type of foreign intelligence information designated; and

(II) such information cannot reasonably be obtained by normal investigative techniques;

(G) a summary statement of the means by which the acquisition will be conducted and

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release January 17, 2014

January 17, 2014

PRESIDENTIAL POLICY DIRECTIVE/PPD-28

SUBJECT: Signals Intelligence Activities

The United States, like other nations, has gathered intelligence throughout its history to ensure that national security and foreign policy decisionmakers have access to timely, accurate, and insightful information.

The collection of signals intelligence 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, signals intelligence activities and the possibility that such activities may be improperly disclosed to the public pose multiple risks. These include risks to: our relationships with other nations, including the cooperation we receive from other nations on law enforcement, counterterrorism, and other issues; our commercial, economic, and financial interests, including a potential loss of international trust in U.S. firms and the decreased willingness of other nations to participate in international data sharing, privacy, and regulatory regimes; the credibility of our commitment to an open, interoperable, and secure global Internet; and the protection of intelligence sources and methods.

In addition, our signals intelligence 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.

In determining why, whether, when, and how the United States conducts signals intelligence activities, we must weigh all of these considerations in a context in which information and communications technologies are constantly changing. The evolution of technology has created a world where communications important to our national security and the communications all of us make as part of our daily lives are transmitted through the same channels. This presents new and diverse opportunities for, and challenges with respect to, the collection of intelligence – and especially signals intelligence. The United States Intelligence Community (IC) has achieved remarkable success in developing enhanced capabilities to perform its signals intelligence mission in this rapidly changing world, and these enhanced capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment.[1] The

---

[1] For the purposes of this directive, the terms "Intelligence Community" and "elements of the Intelligence Community" shall have the same meaning as they do in Executive Order 12333 of December 4, 1981, as amended (Executive Order 12333).

United States must preserve and continue to develop a robust and technologically advanced signals intelligence capability to protect our security and that of our partners and allies. Our signals intelligence capabilities must also be agile enough to enable us to focus on fleeting opportunities or emerging crises and to address not only the issues of today, but also the issues of tomorrow, which we may not be able to foresee.

Advanced technologies can increase risks, as well as opportunities, however, and we must consider these risks when deploying our signals intelligence capabilities. The IC conducts signals intelligence activities with care and precision to ensure that its collection, retention, use, and dissemination of signals intelligence account for these risks. In light of the evolving technological and geopolitical environment, we must continue to ensure that our signals intelligence policies and practices appropriately take into account our alliances and other partnerships; the leadership role that the United States plays in upholding democratic principles and universal human rights; the increased globalization of trade, investment, and information flows; our commitment to an open, interoperable and secure global Internet; and the legitimate privacy and civil liberties concerns of U.S. citizens and citizens of other nations.

Presidents have long directed the acquisition of foreign intelligence and counterintelligence[2] pursuant to their constitutional authority to conduct U.S. foreign relations and to fulfill their constitutional responsibilities as Commander in Chief and Chief Executive. They have also provided direction on the conduct of intelligence activities in furtherance of these authorities and responsibilities, as well as in execution of laws enacted by the Congress. Consistent with this historical practice, this directive articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes.[3]

Section 1. Principles Governing the Collection of Signals Intelligence.

Signals intelligence collection shall be authorized and conducted consistent with the following principles:

(a) The collection of signals intelligence shall be authorized by statute or Executive Order, proclamation, or other Presidential directive, and undertaken in

[2] For the purposes of this directive, the terms "foreign intelligence" and "counterintelligence" shall have the same meaning as they have in Executive Order 12333. Thus, "foreign intelligence" means "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists," and "counterintelligence" means "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities." Executive Order 12333 further notes that "[i]ntelligence includes foreign intelligence and counterintelligence."

[3] Unless otherwise specified, this directive shall apply to signals intelligence activities conducted in order to collect communications or information about communications, except that it shall not apply to signals intelligence activities undertaken to test or develop signals intelligence capabilities.

accordance with the Constitution and applicable statutes, Executive Orders, proclamations, and Presidential directives.

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

(c) 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[4] to U.S. companies and U.S. business sectors commercially.

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

Sec. 2. Limitations on the Use of Signals Intelligence Collected in Bulk.

Locating new or emerging threats and other vital national security information is difficult, as such information is often hidden within the large and complex system of modern global communications. The United States must consequently collect signals intelligence in bulk[5] in certain circumstances in order to identify these threats. Routine communications and communications of national security interest increasingly transit the same networks, however, and the collection of signals intelligence in bulk may consequently result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value. The United States will therefore impose new limits on its use of signals intelligence collected in bulk. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside.

In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data

[4] Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage.

[5] The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection. References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).

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 in this section. In no event may signals intelligence collected in bulk 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 in this section.

The Assistant to the President and National Security Advisor (APNSA), in consultation with the Director of National Intelligence (DNI), shall coordinate, on at least an annual basis, a review of the permissible uses of signals intelligence collected in bulk through the National Security Council Principals and Deputies Committee system identified in PPD-1 or any successor document. At the end of this review, I will be presented with recommended additions to or removals from the list of the permissible uses of signals intelligence collected in bulk.

The DNI shall maintain a list of the permissible uses of signals intelligence collected in bulk. This list shall be updated as necessary and made publicly available to the maximum extent feasible, consistent with the national security.

Sec. 3. Refining the Process for Collecting Signals Intelligence.

U.S. intelligence collection activities present the potential for national security damage if improperly disclosed. Signals intelligence collection raises special concerns, given the opportunities and risks created by the constantly evolving technological and geopolitical environment; the unique nature of such collection and the inherent concerns raised when signals intelligence can only be collected in bulk; and the risk of damage to our national security interests and our law enforcement, intelligence-sharing, and diplomatic relationships should our capabilities or activities be compromised. It is, therefore, essential that national security policymakers consider carefully the value of signals intelligence activities in light of the risks entailed in conducting these activities.

To enable this judgment, the heads of departments and agencies that participate in the policy processes for establishing signals intelligence priorities and requirements shall, on an annual basis, review any priorities or requirements identified by their departments or agencies and advise the DNI whether each should be maintained, with a copy of the advice provided to the APNSA.

Additionally, the classified Annex to this directive, which supplements the existing policy process for reviewing signals intelligence activities, affirms that determinations about whether and how to conduct signals intelligence activities must

carefully evaluate the benefits to our national interests and the risks posed by those activities.[6]

Sec. 4. Safeguarding Personal Information Collected Through Signals Intelligence.

All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information.[7] U.S. signals intelligence activities must, therefore, 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.[8]

(a) *Policies and Procedures.* The DNI, in consultation with the Attorney General, shall ensure that all elements of the IC establish policies and procedures that apply the following principles for safeguarding personal information collected from signals intelligence activities. To the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality:[9]

i. *Minimization.* The sharing of intelligence that contains personal information is necessary to protect our national security and advance our foreign policy interests, as it enables the United States to coordinate activities across our government. At the same time, however, by setting appropriate limits on such sharing, the United States takes legitimate privacy concerns into account and decreases the risks that personal information will be misused or mishandled. Relatedly, the significance to our national security of intelligence is not always apparent upon an initial review of information: intelligence must be retained for a sufficient period of time for the IC to understand its relevance and use

[6] Section 3 of this directive, and the directive's classified Annex, do not apply to (1) signals intelligence activities undertaken by or for the Federal Bureau of Investigation in support of predicated investigations other than those conducted solely for purposes of acquiring foreign intelligence; or (2) signals intelligence activities undertaken in support of military operations in an area of active hostilities, covert action, or human intelligence operations.

[7] Departments and agencies shall apply the term "personal information" in a manner that is consistent for U.S. persons and non-U.S. persons. Accordingly, for the purposes of this directive, the term "personal information" shall cover the same types of information covered by "information concerning U.S. persons" under section 2.3 of Executive Order 12333.

[8] The collection, retention, and dissemination of information concerning "United States persons" is governed by multiple legal and policy requirements, such as those required by the Foreign Intelligence Surveillance Act and Executive Order 12333. For the purposes of this directive, the term "United States person" shall have the same meaning as it does in Executive Order 12333.

[9] The policies and procedures of affected elements of the IC shall also be consistent with any additional IC policies, standards, procedures, and guidance the DNI, in coordination with the Attorney General, the heads of IC elements, and the heads of any other departments containing such elements, may issue to implement these principles. This directive is not intended to alter the rules applicable to U.S. persons in Executive Order 12333, the Foreign Intelligence Surveillance Act, or other applicable law.

it to meet our national security needs. However, long-term storage of personal information unnecessary to protect our national security is inefficient, unnecessary, and raises legitimate privacy concerns. Accordingly, IC elements shall establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities.

- Dissemination: Personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333.

- Retention: Personal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons. Information for which no such determination has been made shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States.

Additionally, within 180 days of the date of this directive, the DNI, in coordination with the Attorney General, the heads of other elements of the IC, and the heads of departments and agencies containing other elements of the IC, shall prepare a report evaluating possible additional dissemination and retention safeguards for personal information collected through signals intelligence, consistent with technical capabilities and operational needs.

ii. *Data Security and Access*. When our national security and foreign policy needs require us to retain certain intelligence, it is vital that the United States take appropriate steps to ensure that any personal information contained within that intelligence is secure. Accordingly, personal information shall be processed and stored under conditions that provide adequate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, Presidential directives, IC directives, and associated policies. Access to such personal information shall be limited to authorized personnel with a need to know the information to perform their mission, consistent with the personnel security requirements of relevant Executive Orders, IC directives, and associated policies. Such personnel will be provided appropriate and adequate training in the principles set forth in this directive. These persons may access and use the information consistent with applicable laws and Executive Orders and the principles of this directive; personal information for which no determination has been made that it can be permissibly disseminated or retained under section 4(a)(i) of this directive shall be accessed only in order to make such determinations

(or to conduct authorized administrative, security, and oversight functions).

iii. *Data Quality.* IC elements strive to provide national security policymakers with timely, accurate, and insightful intelligence, and inaccurate records and reporting can not only undermine our national security interests, but also can result in the collection or analysis of information relating to persons whose activities are not of foreign intelligence or counterintelligence value. Accordingly, personal information shall be included in intelligence products only as consistent with applicable IC standards for accuracy and objectivity, as set forth in relevant IC directives. Moreover, while IC elements should apply the IC Analytic Standards as a whole, particular care should be taken to apply standards relating to the quality and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

iv. *Oversight.* The IC has long recognized that effective oversight is necessary to ensure that we are protecting our national security in a manner consistent with our interests and values. Accordingly, the policies and procedures of IC elements, and departments and agencies containing IC elements, shall include appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information, to include periodic auditing against the standards required by this section.

The policies and procedures shall also recognize and facilitate the performance of oversight by the Inspectors General of IC elements, and departments and agencies containing IC elements, and other relevant oversight entities, as appropriate and consistent with their responsibilities. When a significant compliance issue occurs involving personal information of any person, regardless of nationality, collected as a result of signals intelligence activities, the issue shall, in addition to any existing reporting requirements, be reported promptly to the DNI, who shall determine what, if any, corrective actions are necessary. If the issue involves a non-United States person, the DNI, in consultation with the Secretary of State and the head of the notifying department or agency, 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.

(b) *Update and Publication.* 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.

(c) *Privacy and Civil Liberties Policy Official.* To help ensure that the legitimate privacy interests all people share related to the handling of their personal information are appropriately considered in light of the principles in this section, the APNSA, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy (OSTP) shall identify one or more senior officials who will be responsible for working with the DNI, the Attorney General, the heads of other elements of the IC, and the heads of departments and agencies containing other elements of the IC, as appropriate, as they develop the policies and procedures called for in this section.

(d) *Coordinator for International Diplomacy.* The Secretary of State shall identify a senior official within the Department of State to coordinate with the responsible departments and agencies the United States Government's diplomatic and foreign policy efforts related to international information technology issues and to serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States.

Sec. 5. Reports.

(a) Within 180 days of the date of this directive, the DNI shall provide a status report that updates me on the progress of the IC's implementation of section 4 of this directive.

(b) The Privacy and Civil Liberties Oversight Board is encouraged to provide me with a report that assesses the implementation of any matters contained within this directive that fall within its mandate.

(c) Within 120 days of the date of this directive, the President's Intelligence Advisory Board shall provide me with a report identifying options for assessing the distinction between metadata and other types of information, and for replacing the "need-to-share" or "need-to-know" models for classified information sharing with a Work-Related Access model.

(d) Within 1 year of the date of this directive, the DNI, in coordination with the heads of relevant elements of the IC and OSTP, shall provide me with a report assessing the feasibility of creating software that would allow the IC more easily to conduct targeted information acquisition rather than bulk collection.

Sec. 6. General Provisions.

(a) Nothing in this directive shall be construed to prevent me from exercising my constitutional authority, including as Commander in Chief, Chief Executive, and in the conduct of foreign affairs, as well as my statutory authority. Consistent with this principle, a recipient of this directive may at any time recommend to me, through the APNSA, a change to the policies and procedures contained in this directive.

(b) Nothing in this directive shall be construed to impair or otherwise affect the authority or responsibility granted by law to a United States Government department or agency, or the head thereof, or the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals. This directive is intended to supplement existing processes or procedures for reviewing foreign intelligence or counterintelligence activities and should not be read to supersede such processes and procedures unless explicitly stated.

(c) This directive shall be implemented consistent with applicable U.S. law and subject to the availability of appropriations.

(d) This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

# # #