Executive Order 14086—Enhancing Safeguards for United States Signals Intelligence Activities

October 7, 2022

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose*. The United States collects signals intelligence so that its national security decisionmakers have access to the timely, accurate, and insightful information necessary to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm. Signals intelligence capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment, and the United States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners. At the same time, the United States recognizes that 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. Therefore, this order establishes safeguards for such signals intelligence activities.

Sec. 2. *Signals Intelligence Activities*.

(a) *Principles*. Signals intelligence activities shall be authorized and conducted consistent with the following principles:

(i) Signals intelligence activities shall be authorized by statute or by Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and with applicable statutes and Executive Orders, proclamations, and other Presidential directives.

(ii) Signals intelligence activities shall be subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that:

(A) signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and

(B) signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(iii) Signals intelligence activities shall be subjected to rigorous oversight in order to ensure that they comport with the principles identified above.

(b) *Objectives*. Signals intelligence collection activities shall be conducted in pursuit of legitimate objectives.

(i) *Legitimate objectives*.

(A) Signals intelligence collection activities shall be conducted only in pursuit of one or more of the following objectives:

(1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners;

(2) understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners;

(3) understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry;

(4) protecting against foreign military capabilities and activities;

(5) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(6) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(7) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(8) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(9) protecting against threats to the personnel of the United States or of its allies or partners;

(10) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (b)(i) of this section;

(11) protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; and

(12) advancing collection or operational capabilities or activities in order to further a legitimate objective identified in subsection (b)(i) of this section.

(B) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national

security of the United States, for which the President determines that signals intelligence collection activities may be used. The Director of National Intelligence (Director) shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(ii) *Prohibited objectives*.

(A) Signals intelligence collection activities shall not be conducted for the purpose of:

(1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;

(2) suppressing or restricting legitimate privacy interests;

(3) suppressing or restricting a right to legal counsel; or

(4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.

(B) It is not a legitimate objective to collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially. The collection of such information is authorized only to protect the national security of the United States or of its allies or partners.

(iii) *Validation of signals intelligence collection priorities*.

(A) Under section 102A of the National Security Act of 1947, as amended (50 U.S.C. 3024), the Director must establish priorities for the Intelligence Community to ensure the timely and effective collection of national intelligence, including national intelligence collected through signals intelligence. The Director does this through the National Intelligence Priorities Framework (NIPF), which the Director maintains and presents to the President, through the Assistant to the President for National Security Affairs, on a regular basis. In order to ensure that signals intelligence collection activities are undertaken to advance legitimate objectives, before presenting the NIPF or any successor framework that identifies intelligence priorities to the President, the Director shall obtain from the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO) an assessment as to whether, with regard to anticipated signals intelligence collection activities, each of the intelligence priorities identified in the NIPF or successor framework:

(1) advances one or more of the legitimate objectives set forth in subsection (b)(i) of this section;

(2) neither was designed nor is anticipated to result in signals intelligence collection in contravention of the prohibited objectives set forth in subsection (b)(ii) of this section; and

(3) was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(B) If the Director disagrees with any aspect of the CLPO's assessment with respect to any of the intelligence priorities identified in the NIPF or successor

framework, the Director shall include the CLPO's assessment and the Director's views when presenting the NIPF to the President.

(c) *Privacy and civil liberties safeguards*. The following safeguards shall fulfill the principles contained in subsections (a)(ii) and (a)(iii) of this section.

(i) *Collection of signals intelligence.*

(A) The United States shall conduct signals intelligence collection activities only following a determination that a specific signals intelligence collection activity, based on a reasonable assessment of all relevant factors, is necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; it could be used, for example, to ensure alternative pathways for validation or for maintaining reliable access to the same information. In determining whether to collect signals intelligence consistent with this principle, the United States—through an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees—shall consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, and shall prioritize such available, feasible, and appropriate alternatives to signals intelligence.

(B) Signals intelligence collection activities shall be as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant factors, not disproportionately impact privacy and civil liberties. Such factors may include, depending on the circumstances, the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals, including unintended third parties; the nature and sensitivity of the data to be collected; and the safeguards afforded to the information collected.

(C) For purposes of subsection (c)(i) of this section, the scope of a specific signals intelligence collection activity may include, for example, a specific line of effort or target, as appropriate.

(ii) *Bulk collection of signals intelligence.*

(A) Targeted collection shall be prioritized. The bulk collection of signals intelligence shall be authorized only based on a determination—by an element of the Intelligence Community or through an interagency committee consisting in whole or in part of the heads of elements of the Intelligence Community, the heads of departments containing such elements, or their designees—that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection. When it is determined to be necessary to engage in bulk collection in order to advance a validated intelligence priority, the element of the Intelligence Community shall apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.

(B) Each element of the Intelligence Community that collects signals intelligence through bulk collection shall use such information only in pursuit of one or more of the following objectives:

(1) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(2) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(3) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(4) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(5) protecting against threats to the personnel of the United States or of its allies or partners; and

(6) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (c)(ii) of this section.

(C) The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that bulk collection may be used. The Director shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

(D) In order to minimize any impact on privacy and civil liberties, a targeted signals intelligence collection activity that temporarily uses data acquired without discriminants (for example, without specific identifiers or selection terms) shall be subject to the safeguards described in this subsection, unless such data is:

(1) used only to support the initial technical phase of the targeted signals intelligence collection activity;

(2) retained for only the short period of time required to complete this phase; and

(3) thereafter deleted.

(iii) *Handling of personal information collected through signals intelligence.*

(A) *Minimization*. Each element of the Intelligence Community that handles personal information collected through signals intelligence shall establish and apply policies and procedures designed to minimize the dissemination and retention of personal information collected through signals intelligence.

(1) *Dissemination*. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(a) shall disseminate non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable types of information that section 2.3 of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended, states may be disseminated in the case of information concerning United States persons;

(b) shall not disseminate personal information collected through signals intelligence solely because of a person's nationality or country of residence;

(c) shall disseminate within the United States Government personal information collected through signals intelligence only if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information;

(d) shall take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned before disseminating personal information collected through signals intelligence to recipients outside the United States Government, including to a foreign government or international organization; and

(e) shall not disseminate personal information collected through signals intelligence for the purpose of circumventing the provisions of this order.

(2) *Retention*. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(a) shall retain non-United States persons' personal information collected through signals intelligence only if the retention of comparable information concerning United States persons would be permitted under applicable law and shall subject such information to the same retention periods that would apply to comparable information concerning United States persons;

(b) shall subject non-United States persons' personal information collected through signals intelligence for which no final retention determination has been made to the same temporary retention periods that would apply to comparable information concerning United States persons; and

(c) shall delete non-United States persons' personal information collected through signals intelligence that may no longer be retained in the same manner that comparable information concerning United States persons would be deleted.

(B) *Data security and access*. Each element of the Intelligence Community that handles personal information collected through signals intelligence:

(1) shall process and store personal information collected through signals intelligence under conditions that provide appropriate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, other Presidential directives, Intelligence Community directives, and associated policies;

(2) shall limit access to such personal information to authorized personnel who have a need to know the information to perform their mission and have

received appropriate training on the requirements of applicable United States law, as described in policies and procedures issued under subsection (c)(iv) of this section; and

(3) shall ensure that personal information collected through signals intelligence for which no final retention determination has been made is accessed only in order to make or support such a determination or to conduct authorized administrative, testing, development, security, or oversight functions.

(C) *Data quality*. Each element of the Intelligence Community that handles personal information collected through signals intelligence shall include such personal information in intelligence products only as consistent with applicable Intelligence Community standards for accuracy and objectivity, with a focus on applying 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.

(D) *Queries of bulk collection*. Each element of the Intelligence Community that conducts queries of unminimized signals intelligence obtained by bulk collection shall do so consistent with the permissible uses of signals intelligence obtained by bulk collection identified in subsection (c)(ii)(B) of this section and according to policies and procedures issued under subsection (c)(iv) of this section, which shall appropriately take into account the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

(E) *Documentation*. In order to facilitate the oversight processes set forth in subsection (d) of this section and the redress mechanism set forth in section 3 of this order, each element of the Intelligence Community that engages in signals intelligence collection activities shall maintain documentation to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected. The content of any such documentation may vary based on the circumstances but shall, to the extent reasonable, provide the factual basis pursuant to which the element of the Intelligence Community, based on a reasonable assessment of all relevant factors, assesses that the signals intelligence collection activity is necessary to advance a validated intelligence priority.

(iv) *Update and publication of policies and procedures*. The head of each element of the Intelligence Community:

(A) shall continue to use the policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014 (Signals Intelligence Activities) (PPD–28), until they are updated pursuant to subsection (c)(iv)(B) of this section;

(B) shall, within 1 year of the date of this order, in consultation with the Attorney General, the CLPO, and the Privacy and Civil Liberties Oversight Board (PCLOB), update those policies and procedures as necessary to implement the privacy and civil liberties safeguards in this order; and

(C) shall, within 1 year of the date of this order, release these policies and procedures publicly to the maximum extent possible, consistent with the protection of intelligence sources and methods, in order to enhance the public's understanding of, and to promote public trust in, the safeguards pursuant to which the United States conducts signals intelligence activities.

(v) Review by the PCLOB.

(A) *Nature of review*. Consistent with applicable law, the PCLOB is encouraged to conduct a review of the updated policies and procedures described in subsection (c)(iv)(B) of this section once they have been issued to ensure that they are consistent with the enhanced safeguards contained in this order.

(B) *Consideration of review*. Within 180 days of completion of any review by the PCLOB described in subsection (c)(v)(A) of this section, the head of each element of the Intelligence Community shall carefully consider and shall implement or otherwise address all recommendations contained in such review, consistent with applicable law.

(d) *Subjecting signals intelligence activities to rigorous oversight*. The actions directed in this subsection are designed to build on the oversight mechanisms that elements of the Intelligence Community already have in place, in order to further ensure that signals intelligence activities are subjected to rigorous oversight.

(i) *Legal, oversight, and compliance officials*. Each element of the Intelligence Community that collects signals intelligence:

(A) shall have in place senior-level legal, oversight, and compliance officials who conduct periodic oversight of signals intelligence activities, including an Inspector General, a Privacy and Civil Liberties Officer, and an officer or officers in a designated compliance role with the authority to conduct oversight of and ensure compliance with applicable United States law;

(B) shall provide such legal, oversight, and compliance officials access to all information pertinent to carrying out their oversight responsibilities under this subsection, consistent with the protection of intelligence sources or methods, including their oversight responsibilities to ensure that any appropriate actions are taken to remediate an incident of non-compliance with applicable United States law; and

(C) shall not take any actions designed to impede or improperly influence such legal, oversight, and compliance officials in carrying out their oversight responsibilities under this subsection.

(ii) *Training*. Each element of the Intelligence Community shall maintain appropriate training requirements to ensure that all employees with access to signals intelligence know and understand the requirements of this order and the policies and procedures for reporting and remediating incidents of non-compliance with applicable United States law.

(iii) *Significant incidents of non-compliance.*

(A) Each element of the Intelligence Community shall ensure that, if a legal, oversight, or compliance official, as described in subsection (d)(i) of this section, or any other employee, identifies a significant incident of non-compliance with applicable United States law, the incident is reported promptly to the head of the element of the Intelligence Community, the head of the executive department or agency (agency) containing the element of the Intelligence Community (to the extent relevant), and the Director.

(B) Upon receipt of such report, the head of the element of the Intelligence Community, the head of the agency containing the element of the Intelligence Community (to the extent relevant), and the Director shall ensure that any

necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance.

(e) *Savings clause*. Provided the signals intelligence collection is conducted consistent with and in the manner prescribed by this section of this order, this order does not limit any signals intelligence collection technique authorized under the National Security Act of 1947, as amended (50 U.S.C. 3001 *et seq*.), the Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. 1801 *et seq*.) (FISA), Executive Order 12333, or other applicable law or Presidential directive.

Sec. 3. *Signals Intelligence Redress Mechanism*.

(a) *Purpose*. This section establishes a redress mechanism to review qualifying complaints transmitted by the appropriate public authority in a qualifying state concerning United States signals intelligence activities for any covered violation of United States law and, if necessary, appropriate remediation.

(b) *Process for submission of qualifying complaints.* Within 60 days of the date of this order, the Director, in consultation with the Attorney General and the heads of elements of the Intelligence Community that collect or handle personal information collected through signals intelligence, shall establish a process for the submission of qualifying complaints transmitted by the appropriate public authority in a qualifying state.

(c) *Initial investigation of qualifying complaints by the CLPO*.

(i) *Establishment*. The Director, in consultation with the Attorney General, shall establish a process that authorizes the CLPO to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints. This process shall govern how the CLPO will review qualifying complaints in a manner that protects classified or otherwise privileged or protected information and shall ensure, at a minimum, that for each qualifying complaint the CLPO shall:

(A) review information necessary to investigate the qualifying complaint;

(B) exercise its statutory and delegated authority to determine whether there was a covered violation by:

(i) taking into account both relevant national security interests and applicable privacy protections;

(ii) giving appropriate deference to any relevant determinations made by national security officials; and

(iii) applying the law impartially;

(C) determine the appropriate remediation for any covered violation;

(D) provide a classified report on information indicating a violation of any authority subject to the oversight of the Foreign Intelligence Surveillance Court (FISC) to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure;

(E) after the review is completed, inform the complainant, through the appropriate public authority in a qualifying state and without confirming or denying that the complainant was subject to United States signals intelligence activities, that:

(1) "the review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation";

(2) the complainant or an element of the Intelligence Community may, as prescribed in the regulations issued by the Attorney General pursuant to section 3(d)(i) of this order, apply for review of the CLPO's determinations by the Data Protection Review Court described in subsection (d) of this section; and

(3) if either the complainant or an element of the Intelligence Community applies for review by the Data Protection Review Court, a special advocate will be selected by the Data Protection Review Court to advocate regarding the complainant's interest in the matter;

(F) maintain appropriate documentation of its review of the qualifying complaint and produce a classified decision explaining the basis for its factual findings, determination with respect to whether a covered violation occurred, and determination of the appropriate remediation in the event there was such a violation, consistent with its statutory and delegated authority;

(G) prepare a classified ex parte record of review, which shall consist of the appropriate documentation of its review of the qualifying complaint and the classified decision described in subsection (c)(i)(F) of this section; and

(H) provide any necessary support to the Data Protection Review Court.

(ii) *Binding effect*. Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by the CLPO to undertake appropriate remediation pursuant to subsection (c)(i)(C) of this section, subject to any contrary determination by the Data Protection Review Court.

(iii) *Assistance*. Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the reviews described in subsection (c)(i) of this section, consistent with the protection of intelligence sources and methods, and shall not take any actions designed to impede or improperly influence the CLPO's reviews. Privacy and civil liberties officials within elements of the Intelligence Community shall also support the CLPO as it performs the reviews described in subsection (c)(i) of this section.

(iv) *Independence*. The Director shall not interfere with a review by the CLPO of a qualifying complaint under subsection (c)(i) of this section; nor shall the Director remove the CLPO for any actions taken pursuant to this order, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity.

(d) *Data Protection Review Court*.

(i) *Establishment*. The Attorney General is authorized to and shall establish a process to review determinations made by the CLPO under subsection (c)(i) of this section. In exercising that authority, the Attorney General shall, within 60 days of the date of this order, promulgate regulations establishing a Data Protection Review Court to exercise the Attorney General's authority to review such determinations. These regulations shall, at a minimum, provide that:

(A) The Attorney General, in consultation with the Secretary of Commerce, the Director, and the PCLOB, shall appoint individuals to serve as judges on the Data Protection Review Court, who shall be legal practitioners with appropriate experience in the fields of data privacy and national security law, giving weight to individuals with prior judicial experience, and who shall not be, at the time of their initial appointment, employees of the United States Government. During their term

of appointment on the Data Protection Review Court, such judges shall not have any official duties or employment within the United States Government other than their official duties and employment as judges on the Data Protection Review Court.

(B) Upon receipt of an application for review filed by the complainant or an element of the Intelligence Community of a determination made by the CLPO under subsection (c) of this section, a three-judge panel of the Data Protection Review Court shall be convened to review the application. Service on the Data Protection Review Court panel shall require that the judge hold the requisite security clearances to access classified national security information.

(C) Upon being convened, the Data Protection Review Court panel shall select a special advocate through procedures prescribed in the Attorney General's regulations. The special advocate shall assist the panel in its consideration of the application for review, including by advocating regarding the complainant's interest in the matter and ensuring that the Data Protection Review Court panel is well informed of the issues and the law with respect to the matter. Service as a special advocate shall require that the special advocate hold the requisite security clearances to access classified national security information and to adhere to restrictions prescribed in the Attorney General's regulations on communications with the complainant to ensure the protection of classified or otherwise privileged or protected information.

(D) The Data Protection Review Court panel shall impartially review the determinations made by the CLPO with respect to whether a covered violation occurred and the appropriate remediation in the event there was such a violation. The review shall be based at a minimum on the classified ex parte record of review described in subsection (c)(i)(F) of this section and information or submissions provided by the complainant, the special advocate, or an element of the Intelligence Community. In reviewing determinations made by the CLPO, the Data Protection Review Court panel shall be guided by relevant decisions of the United States Supreme Court in the same way as are courts established under Article III of the United States Constitution, including those decisions regarding appropriate deference to relevant determinations of national security officials.

(E) In the event that the Data Protection Review Court panel disagrees with any of the CLPO's determinations with respect to whether a covered violation occurred or the appropriate remediation in the event there was such a violation, the panel shall issue its own determinations.

(F) The Data Protection Review Court panel shall provide a classified report on information indicating a violation of any authority subject to the oversight of the FISC to the Assistant Attorney General for National Security, who shall report violations to the FISC in accordance with its rules of procedure.

(G) After the review is completed, the CLPO shall be informed of the Data Protection Review Court panel's determinations through procedures prescribed by the Attorney General's regulations.

(H) After a review is completed in response to a complainant's application for review, the Data Protection Review Court, through procedures prescribed by the Attorney General's regulations, shall inform the complainant, through the appropriate public authority in a qualifying state and without confirming or

denying that the complainant was subject to United States signals intelligence activities, that "the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation."

(ii) *Binding effect*. Each element of the Intelligence Community, and each agency containing an element of the Intelligence Community, shall comply with any determination by a Data Protection Review Court panel to undertake appropriate remediation.

(iii) *Assistance*. Each element of the Intelligence Community shall provide the CLPO with access to information necessary to conduct the review described in subsection (d)(i) of this section, consistent with the protection of intelligence sources and methods, that a Data Protection Review Court panel requests from the CLPO and shall not take any actions for the purpose of impeding or improperly influencing a panel's review.

(iv) *Independence*. The Attorney General shall not interfere with a review by a Data Protection Review Court panel of a determination the CLPO made regarding a qualifying complaint under subsection (c)(i) of this section; nor shall the Attorney General remove any judges appointed as provided in subsection (d)(i)(A) of this section, or remove any judge from service on a Data Protection Review Court panel, except for instances of misconduct, malfeasance, breach of security, neglect of duty, or incapacity, after taking due account of the standards in the Rules for Judicial-Conduct and Judicial-Disability Proceedings promulgated by the Judicial Conference of the United States pursuant to the Judicial Conduct and Disability Act (28 U.S.C. 351 *et seq*.).

(v) *Record of determinations*. For each qualifying complaint transmitted by the appropriate public authority in a qualifying state, the Secretary of Commerce shall:

(A) maintain a record of the complainant who submitted such complaint;

(B) not later than 5 years after the date of this order and no less than every 5 years thereafter, contact the relevant element or elements of the Intelligence Community regarding whether information pertaining to the review of such complaint by the CLPO has been declassified and whether information pertaining to the review of any application for review submitted to the Data Protection Review Court has been declassified, including whether an element of the Intelligence Community filed an application for review with the Data Protection Review Court; and

(C) if informed that such information has been declassified, notify the complainant, through the appropriate public authority in a qualifying state, that information pertaining to the review of their complaint by the CLPO or to the review of any application for review submitted to the Data Protection Review Court may be available under applicable law.

(e) *Annual review by PCLOB of redress process*.

(i) *Nature of review.* Consistent with applicable law, the PCLOB is encouraged to conduct an annual review of the processing of qualifying complaints by the redress mechanism established by section 3 of this order, including whether the CLPO and the Data Protection Review Court processed qualifying complaints in a timely manner; whether the CLPO and the Data Protection Review Court are obtaining full access to necessary information; whether the CLPO and the Data Protection Review Court are operating consistent with this order; whether the safeguards established by section 2 of

this order are properly considered in the processes of the CLPO and the Data Protection Review Court; and whether the elements of the Intelligence Community have fully complied with determinations made by the CLPO and the Data Protection Review Court.

(ii) *Assistance*. The Attorney General, the CLPO, and the elements of the Intelligence Community shall provide the PCLOB with access to information necessary to conduct the review described in subsection (e)(i) of this section, consistent with the protection of intelligence sources and methods.

(iii) *Report and certification*. Within 30 days of completing any review described in subsection (e)(i) of this section, the PCLOB is encouraged to:

(A) provide the President, the Attorney General, the Director, the heads of elements of the Intelligence Community, the CLPO, and the congressional intelligence committees with a classified report detailing the results of its review;

(B) release to the public an unclassified version of the report; and

(C) make an annual public certification as to whether the redress mechanism established pursuant to section 3 of this order is processing complaints consistent with this order.

(iv) *Consideration of review*. Within 180 days of receipt of any report by the PCLOB described in subsection (e)(iii)(A) of this section, the Attorney General, the Director, the heads of elements of the Intelligence Community, and the CLPO shall carefully consider and shall implement or otherwise address all recommendations contained in such report, consistent with applicable law.

(f) *Designation of qualifying state*.

(i) To implement the redress mechanism established by section 3 of this order, the Attorney General is authorized to designate a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

(A) the laws of the country, the regional economic integration organization, or the regional economic integration organization's member countries require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or a member country of the regional economic integration organization;

(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries of the regional economic integration organization permit, or are anticipated to permit, the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; and

(C) such designation would advance the national interests of the United States.

(ii) The Attorney General may revoke or amend such a designation, effective immediately or on a date specified by the Attorney General, if the Attorney General determines, in consultation with the Secretary of State, the Secretary of Commerce, and the Director, that:

(A) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not provide appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the country or to a member country of the regional economic integration organization;

(B) the country, the regional economic integration organization, or the regional economic integration organization's member countries do not permit the transfer of personal information for commercial purposes between the territory of that country or those member countries and the territory of the United States; or

(C) such designation is not in the national interests of the United States.

Sec. 4. *Definitions*. For purposes of this order:

(a) "Appropriate remediation" means lawful measures designed to fully redress an identified covered violation regarding a specific complainant and limited to measures designed to address that specific complainant's complaint, taking into account the ways that a violation of the kind identified have customarily been addressed. Such measures may include, depending on the specific covered violation at issue, curing through administrative measures violations found to have been procedural or technical errors relating to otherwise lawful access to or handling of data, terminating acquisition of data where collection is not lawfully authorized, deleting data that had been acquired without lawful authorization, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to those appropriately trained, or recalling intelligence reports containing data acquired without lawful authorization or that were otherwise disseminated in a manner inconsistent with United States law. Appropriate remediation shall be narrowly tailored to redress the covered violation and to minimize adverse impacts on the operations of the Intelligence Community and the national security of the United States.

(b) "Bulk collection" means the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms).

(c) "Counterintelligence" shall have the same meaning as it has in Executive Order 12333.

(d) "Covered violation" means a violation that:

(i) arises from signals intelligence activities conducted after the date of this order regarding data transferred to the United States from a qualifying state after the effective date of the Attorney General's designation for such state, as provided in section 3(f)(i) of this order;

(ii) adversely affects the complainant's individual privacy and civil liberties interests; and

(iii) violates one or more of the following:

(A) the United States Constitution;

(B) the applicable sections of FISA or any applicable FISC-approved procedures;

(C) Executive Order 12333 or any applicable agency procedures pursuant to Executive Order 12333;

(D) this order or any applicable agency policies and procedures issued or updated pursuant to this order (or the policies and procedures identified in section

2(c)(iv)(A) of this order before they are updated pursuant to section 2(c)(iv)(B) of this order);

(E) any successor statute, order, policies, or procedures to those identified in section 4(d)(iii)(B)-(D) of this order; or

(F) any other statute, order, policies, or procedures adopted after the date of this order that provides privacy and civil liberties safeguards with respect to United States signals intelligence activities within the scope of this order, as identified in a list published and updated by the Attorney General, in consultation with the Director of National Intelligence.

(e) "Foreign intelligence" shall have the same meaning as it has in Executive Order 12333.

(f) "Intelligence" shall have the same meaning as it has in Executive Order 12333.

(g) "Intelligence Community" and "elements of the Intelligence Community" shall have the same meaning as they have in Executive Order 12333.

(h) "National security" shall have the same meaning as it has in Executive Order 13526 of December 29, 2009 (Classified National Security Information).

(i) "Non-United States person" means a person who is not a United States person.

(j) "Personnel of the United States or of its allies or partners" means any current or former member of the Armed Forces of the United States, any current or former official of the United States Government, and any other person currently or formerly employed by or working on behalf of the United States Government, as well as any current or former member of the military, current or former official, or other person currently or formerly employed by or working on behalf of an ally or partner.

(k) "Qualifying complaint" means a complaint, submitted in writing, that:

(i) alleges a covered violation has occurred that pertains to personal information of or about the complainant, a natural person, reasonably believed to have been transferred to the United States from a qualifying state after the effective date of the Attorney General's designation for such state, as provided in section 3(f)(i) of this order;

(ii) includes the following basic information to enable a review: information that forms the basis for alleging that a covered violation has occurred, which need not demonstrate that the complainant's data has in fact been subject to United States signals intelligence activities; the nature of the relief sought; the specific means by which personal information of or about the complainant was believed to have been transmitted to the United States; the identities of the United States Government entities believed to be involved in the alleged violation (if known); and any other measures the complainant pursued to obtain the relief requested and the response received through those other measures;

(iii) is not frivolous, vexatious, or made in bad faith;

(iv) is brought on behalf of the complainant, acting on that person's own behalf, and not as a representative of a governmental, nongovernmental, or intergovernmental organization; and

(v) is transmitted by the appropriate public authority in a qualifying state, after it has verified the identity of the complainant and that the complaint satisfies the conditions of section 5(k)(i)–(iv) of this order.

(l) "Significant incident of non-compliance" shall mean a systemic or intentional failure to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned.

(m) "United States person" shall have the same meaning as it has in Executive Order 12333.

(n) "Validated intelligence priority" shall mean, for most United States signals intelligence collection activities, a priority validated under the process described in section 2(b)(iii) of this order; or, in narrow circumstances (for example, when such process cannot be carried out because of a need to address a new or evolving intelligence requirement), shall mean a priority set by the President or the head of an element of the Intelligence Community in accordance with the criteria described in section 2(b)(iii)(A)(1)–(3) of this order to the extent feasible.

(o) "Weapons of mass destruction" shall have the same meaning as it has in Executive Order 13526.

Sec. 5. *General Provisions*. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law, including orders of and procedures approved by the FISC, and subject to the availability of appropriations.

(c) Nothing in this order precludes the application of more privacy-protective safeguards for United States signals intelligence activities that would apply in the absence of this order. In the case of any conflict between this order and other applicable law, the more privacy-protective safeguards shall govern the conduct of signals intelligence activities, to the maximum extent allowed by law.

(d) Nothing in this order prohibits elements of the Intelligence Community from disseminating information relating to a crime for law enforcement purposes; disseminating warnings of threats of killing, serious bodily injury, or kidnapping; disseminating cyber threat, incident, or intrusion response information; notifying victims or warning potential victims of crime; or complying with dissemination obligations required by statute, treaty, or court order, including orders of and procedures approved by the FISC or other court orders.

(e) The collection, retention, and dissemination of information concerning United States persons is governed by multiple legal and policy requirements, such as those required by FISA and Executive Order 12333. This order is not intended to alter the rules applicable to United States persons adopted pursuant to FISA, Executive Order 12333, or other applicable law.

(f) This order shall apply to signals intelligence activities consistent with the scope of PPD–28's application to such activities prior to PPD–28's partial revocation by the national security memorandum issued concurrently with this order. To implement this subsection, the head of each agency containing an element of the Intelligence Community, in consultation with the Attorney General and the Director, is hereby delegated the authority to issue guidance, which may be classified, as appropriate, as to the scope of application of this order with respect to the element or elements of the Intelligence Community within their agency. The CLPO and the Data Protection Review Court, in carrying out the functions assigned to it under this order, shall treat such guidance as authoritative and binding.

(g) Nothing in this order confers authority to declassify or disclose classified national security information except as authorized pursuant to Executive Order 13526 or any successor order. Consistent with the requirements of Executive Order 13526, the CLPO, the Data Protection Review Court, and the special advocates shall not have authority to declassify classified national security information, nor shall they disclose any classified or otherwise privileged or protected information except to authorized and appropriately cleared individuals who have a need to know the information.

(h) This order creates an entitlement to submit qualifying complaints to the CLPO and to obtain review of the CLPO's decisions by the Data Protection Review Court in accordance with the redress mechanism established in section 3 of this order. This order is not intended to, and does not, create any other entitlement, 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. This order is not intended to, and does not, modify the availability or scope of any judicial review of the decisions rendered through the redress mechanism, which is governed by existing law.

JOSEPH R. BIDEN, JR.

The White House,
October 7, 2022.

[Filed with the Office of the Federal Register, 8:45 a.m., October 13, 2022]

NOTE: This Executive order was published in the *Federal Register* on October 14.

Categories: Executive Orders : Signals intelligence activities, U.S., enhancing safeguards.

Subjects: Defense and national security : Electronic surveillance program.

DCPD Number: DCPD202200894.