

sible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.

SEC. 3. *ISAO Standards Organization.* (a) The Secretary, in consultation with other Federal entities responsible for conducting cybersecurity and related activities, shall, through an open and competitive process, enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order. The standards shall further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information. The standards will address the baseline capabilities that ISAOs under this order should possess and be able to demonstrate. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical means, and privacy protections, such as minimization, for ISAO operation and ISAO member participation.

(b) To be selected, the SO must demonstrate the ability to engage and work across the broad community of organizations engaged in sharing information related to cybersecurity risks and incidents, including ISAOs, and associations and private companies engaged in information sharing in support of their customers.

(c) The agreement referenced in section 3(a) shall require that the SO engage in an open public review and comment process for the development of the standards referenced above, soliciting the viewpoints of existing entities engaged in sharing information related to cybersecurity risks and incidents, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders.

(d) The Secretary shall support the development of these standards and, in carrying out the requirements set forth in this section, shall consult with the Office of Management and Budget, the National Institute of Standards and Technology in the Department of Commerce, Department of Justice, the Information Security Oversight Office in the National Archives and Records Administration, the Office of the Director of National Intelligence, Sector-Specific Agencies, and other interested Federal entities. All standards shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

SEC. 4. *Critical Infrastructure Protection Program.* (a) Pursuant to sections 213 and 214(h) of the Critical Infrastructure Information Act of 2002, I hereby designate the NCCIC as a critical infrastructure protection program and delegate to it authority to enter into voluntary agreements with ISAOs in order to promote critical infrastructure security with respect to cybersecurity.

(b) Other Federal entities responsible for conducting cybersecurity and related activities to address threats to the public health and safety, national security, and economic security, consistent with the objectives of this order, may participate in activities under these agreements.

(c) The Secretary will determine the eligibility of ISAOs and their members for any necessary facility or personnel security clearances associated with voluntary agreements in accordance with Executive Order 13549 of August 18, 2010 (Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities), and Executive Order 12829 of January 6, 1993 (National Industrial Security Program), as amended, including as amended by this order.

SEC. 5. *Privacy and Civil Liberties Protections.* (a) Agencies shall coordinate their activities under this order

with their senior agency officials for privacy and civil liberties and ensure that appropriate protections for privacy and civil liberties are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) Senior privacy and civil liberties officials for agencies engaged in activities under this order shall conduct assessments of their agency's activities and provide those assessments to the Department of Homeland Security (DHS) Chief Privacy Officer and the DHS Office for Civil Rights and Civil Liberties for consideration and inclusion in the Privacy and Civil Liberties Assessment report required under Executive Order 13636.

SEC. 6. *National Industrial Security Program.* [Amended Ex. Ord. No. 12829, set out as a note under section 3161 of Title 50, War and National Defense.]

SEC. 7. *Definitions.* (a) "Critical infrastructure information" has the meaning given the term in section 212(3) of the Critical Infrastructure Information Act of 2002.

(b) "Critical infrastructure protection program" has the meaning given the term in section 212(4) of the Critical Infrastructure Information Act of 2002.

(c) "Cybersecurity risk" has the meaning given the term in section 226(a)(1) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(d) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(e) "Incident" has the meaning given the term in section 226(a)(2) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(f) "Information Sharing and Analysis Organization" has the meaning given the term in section 212(5) of the Critical Infrastructure Information Act of 2002.

(g) "Sector-Specific Agency" has the meaning given the term in PPD-21, or any successor.

SEC. 8. *General Provisions.* (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law or Executive Order to an 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 and subject to the availability of appropriations. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law including those activities conducted with the private sector relating to criminal and national security threats. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods.

(d) This order 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.

BARACK OBAMA.

[Reference to a Sector Specific Agency (including any permutations or conjugations thereof) deemed to be a reference to the Sector Risk Management Agency of the relevant critical infrastructure sector and have the meaning given such term in section 650 of this title, see section 652a(c)(3) of this title, enacted Jan. 1, 2021.]

### § 121a. Homeland Security Intelligence Program

There is established within the Department of Homeland Security a Homeland Security Intel-

ligence Program. The Homeland Security Intelligence Program constitutes the intelligence activities of the Office of Intelligence and Analysis of the Department that serve predominantly departmental missions.

(Pub. L. 112-277, title V, § 501, Jan. 14, 2013, 126 Stat. 2476.)

#### Editorial Notes

##### CODIFICATION

Section was enacted as part of the Intelligence Authorization Act for Fiscal Year 2013, and not as part of the Homeland Security Act of 2002 which comprises this chapter.

### § 122. Access to information

#### (a) In general

##### (1) Threat and vulnerability information

Except as otherwise directed by the President, the Secretary shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government.

##### (2) Other information

The Secretary shall also have access to other information relating to matters under the responsibility of the Secretary that may be collected, possessed, or prepared by an agency of the Federal Government as the President may further provide.

#### (b) Manner of access

Except as otherwise directed by the President, with respect to information to which the Secretary has access pursuant to this section—

(1) the Secretary may obtain such material upon request, and may enter into cooperative arrangements with other executive agencies to provide such material or provide Department officials with access to it on a regular or routine basis, including requests or arrangements involving broad categories of material, access to electronic databases, or both; and

(2) regardless of whether the Secretary has made any request or entered into any cooperative arrangement pursuant to paragraph (1), all agencies of the Federal Government shall promptly provide to the Secretary—

(A) all reports (including information reports containing intelligence which has not been fully evaluated), assessments, and analytical information relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary;

(B) all information concerning the vulnerability of the infrastructure of the United States, or other vulnerabilities of the United States, to terrorism, whether or not such information has been analyzed;

(C) all other information relating to significant and credible threats of terrorism

against the United States, whether or not such information has been analyzed; and

(D) such other information or material as the President may direct.

#### (c) Treatment under certain laws

The Secretary shall be deemed to be a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all information from law enforcement agencies that is required to be given to the Director of National Intelligence, under any provision of the following:

(1) The USA PATRIOT Act of 2001 (Public Law 107-56).

(2) Section 2517(6) of title 18.

(3) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.

#### (d) Access to intelligence and other information

##### (1) Access by elements of Federal Government

Nothing in this subchapter shall preclude any element of the intelligence community (as that term is defined in section 3003(4) of title 50,<sup>1</sup> or any other element of the Federal Government with responsibility for analyzing terrorist threat information, from receiving any intelligence or other information relating to terrorism.

##### (2) Sharing of information

The Secretary, in consultation with the Director of National Intelligence, shall work to ensure that intelligence or other information relating to terrorism to which the Department has access is appropriately shared with the elements of the Federal Government referred to in paragraph (1), as well as with State and local governments, as appropriate.

(Pub. L. 107-296, title II, § 202, Nov. 25, 2002, 116 Stat. 2149; Pub. L. 115-278, § 2(g)(2)(D), Nov. 16, 2018, 132 Stat. 4177.)

#### Editorial Notes

##### REFERENCES IN TEXT

The USA PATRIOT Act of 2001, referred to in subsec. (c)(1), is Pub. L. 107-56, Oct. 26, 2001, 115 Stat. 272, known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 or the USA PATRIOT Act. For complete classification of this Act to the Code, see Short Title of 2001 Amendment note set out under section 1 of Title 18, Crimes and Criminal Procedure, and Tables.

The Federal Rules of Criminal Procedure, referred to in subsec. (c)(3), are set out in the Appendix to Title 18, Crimes and Criminal Procedure.

This subchapter, referred to in subsec. (d)(1), was in the original “this title”, meaning title II of Pub. L. 107-296, Nov. 25, 2002, 116 Stat. 2145, which enacted this subchapter, amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure, sections 10102 and 10122 of Title 34, Crime Control and Law Enforcement, and section 3003 of Title 50, War and National Defense, and enacted provisions set out as a note under section 101 of this title and listed in a Provisions for Review, Promulgation, or Amendment of Federal Sentencing Guidelines Relating to Specific Offenses table set out under section 994 of Title 28, Judici-

<sup>1</sup> So in original. There probably should be a closing parenthesis after “50”.