''(a) IN GENERAL.—The President shall—

''(1) develop a national policy for the United States relating to cyberspace, cybersecurity, and cyber warfare; and

''(2) submit to the appropriate congressional committees a report on the policy.

''(b) ELEMENTS.—The national policy required under subsection (a) shall include the following elements:

''(1) Delineation of the instruments of national power available to deter or respond to cyber attacks or other malicious cyber activities by a foreign power or actor that targets United States interests.

''(2) Available or planned response options to address the full range of potential cyber attacks on United States interests that could be conducted by potential adversaries of the United States.

''(3) Available or planned denial options that prioritize the defensibility and resiliency against cyber attacks and malicious cyber activities that are carried out against infrastructure critical to the political integrity, economic security, and national security of the United States.

''(4) Available or planned cyber capabilities that may be used to impose costs on any foreign power targeting the United States or United States persons with a cyber attack or malicious cyber activity.

''(5) Development of multi-prong response options, such as—

''(A) boosting the cyber resilience of critical United States strike systems (including cyber, nuclear, and non-nuclear systems) in order to ensure the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attack;

''(B) developing offensive cyber capabilities and specific plans and strategies to put at risk targets most valued by adversaries of the United States and their key decision makers; and

''(C) enhancing attribution capabilities and developing intelligence and offensive cyber capabilities to detect, disrupt, and potentially expose malicious cyber activities.

''(c) LIMITATION ON AVAILABILITY OF FUNDS.—

''(1) IN GENERAL.—Of the funds authorized to be appropriated by this Act [see Tables for classification] or otherwise made available for fiscal year 2018 for procurement, research, development, test and evaluation, and operations and maintenance, for the covered activities of the Defense Information Systems Agency, not more than 60 percent may be obligated or expended until the date on which the President submits to the appropriate congressional committees the report under subsection (a)(2).

''(2) COVERED ACTIVITIES DESCRIBED.—The covered activities referred to in paragraph (1) are the activities of the Defense Information Systems Agency in support of—

''(A) the White House Communication Agency; and

''(B) the White House Situation Support Staff.

''(d) DEFINITIONS.—In this section:

''(1) The term 'foreign power' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

''(2) The term 'appropriate congressional committees' means—

''(A) the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives];

''(B) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives; and

''(C) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate.''

§ 130h. Prohibitions relating to missile defense information and systems

(a) CERTAIN ''HIT-TO-KILL'' TECHNOLOGY AND TELEMETRY DATA.—None of the funds authorized to be appropriated or otherwise made available for any fiscal year for the Department of Defense may be used to provide the Russian Federation with ''hit-to-kill'' technology and telemetry data for missile defense interceptors or target vehicles.

(b) OTHER SENSITIVE MISSILE DEFENSE INFORMATION.—None of the funds authorized to be appropriated or otherwise made available for any fiscal year for the Department of Defense may be used to provide the Russian Federation with—

(1) information relating to velocity at burnout of missile defense interceptors or targets of the United States; or

(2) classified or otherwise controlled missile defense information.

(c) EXCEPTION.—The prohibitions in subsections (a) and (b) shall not apply to the United States providing to the Russian Federation information regarding ballistic missile early warning.

(d) INTEGRATION.—None of the funds authorized to be appropriated or otherwise made available for any fiscal year for the Department of Defense may be obligated or expended to integrate a missile defense system of the Russian Federation or a missile defense system of the People's Republic of China into any missile defense system of the United States.

(e) SUNSET.—The prohibitions in subsections (a), (b), and (d) shall expire on January 1, 2019.

(Added Pub. L. 114–92, div. A, title XVI, § 1671(a)(1), Nov. 25, 2015, 129 Stat. 1129; amended Pub. L. 114–328, div. A, title X, § 1081(a)(1), title XVI, § 1682(a)(1), (b), Dec. 23, 2016, 130 Stat. 2417, 2623, 2624.)

AMENDMENTS

2016—Pub. L. 114–328, § 1682(a)(1)(C), added section catchline and struck out former section catchline which read as follows: ''Prohibitions on providing certain missile defense information to Russian Federation''.

Subsec. (c). Pub. L. 114–328, § 1081(a)(1), substituted ''subsections (a) and (b)'' for ''subsection (a) and (b)''.

Subsec. (d). Pub. L. 114–328, § 1682(a)(1)(B), added subsec. (d). Former subsec. (d) redesignated (e).

Pub. L. 114–328, § 1081(a)(1), substituted ''subsections (a) and (b)'' for ''subsection (a) and (b)''.

Subsec. (e). Pub. L. 114–328, § 1682(a)(1)(A), (b), redesignated subsec. (d) as (e) and amended it generally. Prior to amendment, text read as follows: ''The prohibitions in subsections (a) and (b) shall expire on January 1, 2017.''

§ 130i. Protection of certain facilities and assets from unmanned aircraft

(a) AUTHORITY.—Notwithstanding section 46502 of title 49, or any provision of title 18, the Secretary of Defense may take, and may authorize members of the armed forces and officers and civilian employees of the Department of Defense with assigned duties that include safety, security, or protection of personnel, facilities, or assets, to take, such actions described in subsection (b)(1) that are necessary to mitigate the threat (as defined by the Secretary of Defense, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

(b) ACTIONS DESCRIBED.—(1) The actions described in this paragraph are the following:

(A) Detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(F) Use reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

(2) The Secretary of Defense shall develop the actions described in paragraph (1) in coordination with the Secretary of Transportation.

(c) FORFEITURE.—Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary of Defense is subject to forfeiture to the United States.

(d) REGULATIONS AND GUIDANCE.—(1) The Secretary of Defense and the Secretary of Transportation may prescribe regulations and shall issue guidance in the respective areas of each Secretary to carry out this section.

(2)(A) The Secretary of Defense and the Secretary of Transportation shall coordinate in the development of guidance under paragraph (1).

(B) The Secretary of Defense shall coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance or otherwise implementing this section if such guidance or implementation might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

(e) PRIVACY PROTECTION.—The regulations prescribed or guidance issued under subsection (d) shall ensure that—

(1) the interception or acquisition of, or access to, communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the fourth amendment to the Constitution and applicable provisions of Federal law;

(2) communications to or from an unmanned aircraft system are intercepted, acquired, or accessed only to the extent necessary to support a function of the Department of Defense;

(3) records of such communications are not maintained for more than 180 days unless the Secretary of Defense determines that maintenance of such records—

(A) is necessary to support one or more functions of the Department of Defense; or

(B) is required for a longer period to support a civilian law enforcement agency or by any other applicable law or regulation; and

(4) such communications are not disclosed outside the Department of Defense unless the disclosure—

(A) would fulfill a function of the Department of Defense;

(B) would support a civilian law enforcement agency or the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory action with regard to, an action described in subsection (b)(1); or

(C) is otherwise required by law or regulation.

(f) BUDGET.—The Secretary of Defense shall submit to Congress, as a part of the defense budget materials for each fiscal year after fiscal year 2018, a consolidated funding display that identifies the funding source for the actions described in subsection (b)(1) within the Department of Defense. The funding display shall be in unclassified form, but may contain a classified annex.

(g) SEMIANNUAL BRIEFINGS.—(1) On a semiannual basis during the five-year period beginning March 1, 2018, the Secretary of Defense and the Secretary of Transportation, shall jointly provide a briefing to the appropriate congressional committees on the activities carried out pursuant to this section. Such briefings shall include—

(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the National Airspace System;

(B) a description of instances where actions described in subsection (b)(1) have been taken;

(C) how the Secretaries have informed the public as to the possible use of authorities under this section; and

(D) how the Secretaries have engaged with Federal, State, and local law enforcement agencies to implement and use such authorities.

(2) Each briefing under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified briefing.

(h) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

(1) vest in the Secretary of Defense any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration under title 49; and

(2) vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Secretary of Defense under this title.

(i) PARTIAL TERMINATION.—(1) Except as provided by paragraph (2), the authority to carry out this section with respect to the covered facilities or assets specified in clauses (iv) through (viii) of subsection (j)(3)[1] shall terminate on December 31, 2020.

---

[1] So in original. Probably should be ''subsection (j)(3)(C)''.

(2) The President may extend by 180 days the termination date specified in paragraph (1) if before November 15, 2020, the President certifies to Congress that such extension is in the national security interests of the United States.

(j) DEFINITIONS.—In this section:

(1) The term ''appropriate congressional committees'' means—

(A) the congressional defense committees;

(B) the Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Commerce, Science, and Transportation of the Senate; and

(C) the Permanent Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Transportation and Infrastructure of the House of Representatives.

(2) The term ''budget'', with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31.

(3) The term ''covered facility or asset'' means any facility or asset that—

(A) is identified by the Secretary of Defense, in consultation with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;

(B) is located in the United States (including the territories and possessions of the United States); and

(C) directly relates to the missions of the Department of Defense pertaining to—

(i) nuclear deterrence, including with respect to nuclear command and control, integrated tactical warning and attack assessment, and continuity of government;

(ii) missile defense;

(iii) national security space;

(iv) assistance in protecting the President or the Vice President (or other officer immediately next in order of succession to the office of the President) pursuant to the Presidential Protection Assistance Act of 1976 (18 U.S.C. 3056 note);

(v) air defense of the United States, including air sovereignty, ground-based air defense, and the National Capital Region integrated air defense system;

(vi) combat support agencies (as defined in paragraphs (1) through (4) of section 193(f) of this title);

(vii) special operations activities specified in paragraphs (1) through (9) of section 167(k) of this title;

(viii) production, storage, transportation, or decommissioning of high-yield explosive munitions, by the Department; or

(ix) a Major Range and Test Facility Base (as defined in section 196(i) of this title).

(4) The term ''defense budget materials'', with respect to a fiscal year, means the materials submitted to Congress by the Secretary of Defense in support of the budget for that fiscal year.

(5) The terms ''electronic communication'', ''intercept'', ''oral communication'', and ''wire communication'' have the meanings given those terms in section 2510 of title 18.

(6) The terms ''unmanned aircraft'' and ''unmanned aircraft system'' have the meanings given those terms in section 331 of the FAA Modernization and Reform Act of 2012 (Public Law 112–95; 49 U.S.C. 40101 note).

(Added Pub. L. 114–328, div. A, title XVI, §1697(a), Dec. 23, 2016, 130 Stat. 2639; amended Pub. L. 115–91, div. A, title XVI, §1692, Dec. 12, 2017, 131 Stat. 1788.)

REFERENCES IN TEXT

The Presidential Protection Assistance Act of 1976, referred to in subsec. (j)(3)(C)(iv), is Pub. L. 94–524, Oct. 17, 1976, 90 Stat. 2475, which enacted and amended provisions set out as notes under section 3056 of Title 18, Crimes and Criminal Procedure. For complete classification of this Act to the Code, see Tables.

AMENDMENTS

2017—Pub. L. 115–91 amended section generally. Prior to amendment, section related to protection of certain facilities and assets from unmanned aircraft and consisted of provisions relating to authority of Secretary of Defense, authorized actions, forfeiture, regulations, and definitions.

§ 130j. Notification requirements for sensitive military cyber operations

(a) IN GENERAL.—Except as provided in subsection (d), the Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of any sensitive military cyber operation conducted under this title no later than 48 hours following such operation.

(b) PROCEDURES.—(1) The Secretary of Defense shall establish and submit to the congressional defense committees procedures for complying with the requirements of subsection (a) consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify the congressional defense committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

(2) The congressional defense committees shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to the committees pursuant to this section.

(3) In the event of an unauthorized disclosure of a sensitive military cyber operation covered by this section, the Secretary shall ensure, to the maximum extent practicable, that the congressional defense committees are notified immediately of the sensitive military cyber operation concerned. The notification under this paragraph may be verbal or written, but in the event of a verbal notification a written notification shall be provided by not later than 48 hours after the provision of the verbal notification.

(c) SENSITIVE MILITARY CYBER OPERATION DEFINED.—(1) In this section, the term ''sensitive military cyber operation'' means an action described in paragraph (2) that—

(A) is carried out by the armed forces of the United States; and

(B) is intended to cause cyber effects outside a geographic location—