''(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.