tion'' and '', China, Iran, North Korea, or other nation state'' after ''Russia''.

DEFINITIONS

For definition of ''congressional intelligence committees'', referred to in subsec. (a)(2)(A), see section 2 of div. N of Pub. L. 115–31, set out as a note under section 3003 of this title.

§ 3370. Supply Chain and Counterintelligence Risk Management Task Force

(a) Appropriate congressional committees defined

In this section, the term ''appropriate congressional committees'' means the following:

(1) The congressional intelligence committees.

(2) The Committee on Armed Services and the Committee on Homeland Security and Governmental Affairs of the Senate.

(3) The Committee on Armed Services, the Committee on Homeland Security, and the Committee on Oversight and Reform of the House of Representatives.

(b) Requirement to establish

The Director of National Intelligence shall establish a Supply Chain and Counterintelligence Risk Management Task Force to standardize information sharing between the intelligence community and the acquisition community of the United States Government with respect to the supply chain and counterintelligence risks.

(c) Members

The Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall be composed of—

(1) a representative of the Defense Security Service of the Department of Defense;

(2) a representative of the General Services Administration;

(3) a representative of the Office of Federal Procurement Policy of the Office of Management and Budget;

(4) a representative of the Department of Homeland Security;

(5) a representative of the Federal Bureau of Investigation;

(6) the Director of the National Counterintelligence and Security Center; and

(7) any other members the Director of National Intelligence determines appropriate.

(d) Security clearances

Each member of the Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall have a security clearance at the top secret level and be able to access sensitive compartmented information.

(e) Annual report

The Supply Chain and Counterintelligence Risk Management Task Force established under subsection (b) shall submit to the appropriate congressional committees an annual report that describes the activities of the Task Force during the previous year, including identification of the supply chain, cybersecurity, and counterintelligence risks shared with the acquisition community of the United States Government by the intelligence community.

(Pub. L. 116–92, div. E, title LXIII, § 6306, Dec. 20, 2019, 133 Stat. 2188.)

DEFINITIONS

For definitions of ''congressional intelligence committees'' and ''intelligence community'', referred to in text, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3370a. Biennial report on foreign investment risks

(a) Intelligence community interagency working group

(1) Requirement to establish

The Director of National Intelligence shall establish an intelligence community interagency working group to prepare the biennial reports required by subsection (b).

(2) Chairperson

The Director of National Intelligence shall serve as the chairperson of such interagency working group.

(3) Membership

Such interagency working group shall be composed of representatives of each element of the intelligence community that the Director of National Intelligence determines appropriate.

(b) Biennial report on foreign investment risks

(1) Report required

Not later than 180 days after December 20, 2019, and not less frequently than once every 2 years thereafter, the Director of National Intelligence shall submit to the appropriate congressional committees a report on foreign investment risks prepared by the interagency working group established under subsection (a).

(2) Elements

Each report required by paragraph (1) shall include identification, analysis, and explanation of the following:

(A) Any current or projected major threats to the national security of the United States with respect to foreign investment.

(B) Any strategy used by a foreign country that such interagency working group has identified to be a country of special concern to use foreign investment to target the acquisition of critical technologies, critical materials, or critical infrastructure.

(C) Any economic espionage efforts directed at the United States by a foreign country, particularly such a country of special concern.

(c) Appropriate congressional committees defined

In this section, the term ''appropriate congressional committees'' means—

(1) the congressional intelligence committees;

(2) the Committee on Homeland Security and Governmental Affairs and the Committee on Foreign Relations of the Senate; and

(3) the Committee on Homeland Security and the Committee on Foreign Affairs of the House of Representatives.

(Pub. L. 116–92, div. E, title LXVII, § 6716, Dec. 20, 2019, 133 Stat. 2227.)

DEFINITIONS

For definitions of ''intelligence community'' and ''congressional intelligence committees'', referred to in text, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3371. Required counterintelligence assessments, briefings, notifications, and reports

(a) Foreign counterintelligence and cybersecurity threats to Federal election campaigns

(1) Reports required

(A) In general

As provided in subparagraph (B), with respect to an election for Federal office, the Director of National Intelligence, in coordination with the Under Secretary of Homeland Security for Intelligence and Analysis and the Director of the Federal Bureau of Investigation, shall make publicly available on an internet website an advisory report on foreign counterintelligence and cybersecurity threats to campaigns of candidates for Federal office. Each such report, consistent with the protection of sources and methods, shall include the following:

(i) A description of foreign counterintelligence and cybersecurity threats to campaigns of candidates for Federal office.

(ii) A summary of best practices that campaigns of candidates for Federal office can employ in seeking to counter such threats.

(iii) An identification of publicly available resources, including United States Government resources, for countering such threats.

(B) Schedule for submittal

(i) In general

Except as provided by clause (ii), with respect to an election for Federal office, a report under this subsection shall be first made available not later than the date that is 1 year before the date of such election, and may be subsequently revised as the Director of National Intelligence determines appropriate.

(ii) 2020 elections

With respect to an election for Federal office that occurs during 2020, the report under this subsection shall be first made available not later than the date that is 60 days after December 20, 2020, and may be subsequently revised as the Director of National Intelligence determines appropriate.

(C) Information to be included

A report under this subsection shall reflect the most current information available to the Director of National Intelligence regarding foreign counterintelligence and cybersecurity threats.

(2) Treatment of campaigns subject to heightened threats

If the Director of the Federal Bureau of Investigation and the Under Secretary of Homeland Security for Intelligence and Analysis jointly determine that a campaign of a candidate for Federal office is subject to a heightened foreign counterintelligence or cybersecurity threat, the Director and the Under Secretary, consistent with the protection of sources and methods, may make available additional information to the appropriate representatives of such campaign.

(b) Omitted

(c) Director of National Intelligence assessment of foreign interference in Federal elections

(1) Assessments required

Not later than 45 days after the end of a Federal election cycle, the Director of National Intelligence, in consultation with the heads of such other executive departments and agencies as the Director considers appropriate, shall—

(A) conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in elections for Federal office occurring during the Federal election cycle; and

(B) transmit the findings of the Director with respect to the assessment conducted under subparagraph (A), along with such supporting information as the Director considers appropriate, to the following:

(i) The President.
(ii) The Secretary of State.
(iii) The Secretary of the Treasury.
(iv) The Secretary of Defense.
(v) The Attorney General.
(vi) The Secretary of Homeland Security.
(vii) Congress.

(2) Elements

An assessment conducted under paragraph (1)(A), with respect to an act described in such paragraph, shall identify, to the maximum extent ascertainable, the following:

(A) The nature of any foreign interference and any methods employed to execute the act.

(B) The persons involved.

(C) The foreign government or governments that authorized, directed, sponsored, or supported the act.

(3) Publication

The Director shall, not later than 60 days after the end of a Federal election cycle, make available to the public, to the greatest extent possible consistent with the protection of sources and methods, the findings transmitted under paragraph (1)(B).

(4) Federal election cycle defined

In this section, the term ''Federal election cycle'' means the period which begins on the day after the date of a regularly scheduled general election for Federal office and which ends on the date of the first regularly scheduled general election for Federal office held after such date.

(5) Effective date

This subsection shall apply with respect to the Federal election cycle that began during