

section, see section 5003 of div. E of Pub. L. 116-92, set out as a note under section 3003 of this title.

§ 3371b. Information sharing with State election officials

(a) State defined

In this section, the term “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(b) Security clearances

(1) In general

Not later than 30 days after December 20, 2019, the Director of National Intelligence shall support the Under Secretary of Homeland Security for Intelligence and Analysis, and any other official of the Department of Homeland Security designated by the Secretary of Homeland Security, in sponsoring a security clearance up to the top secret level for each eligible chief election official of a State or the District of Columbia, and additional eligible designees of such election official as appropriate, at the time that such election official assumes such position.

(2) Interim clearances

Consistent with applicable policies and directives, the Director of National Intelligence may issue interim clearances, for a period to be determined by the Director, to a chief election official as described in paragraph (1) and up to one designee of such official under such paragraph.

(c) Information sharing

(1) In general

The Director of National Intelligence shall assist the Under Secretary of Homeland Security for Intelligence and Analysis and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department (as specified in section 113(a)(1)(H) of title 6) with sharing any appropriate classified information related to threats to election systems and to the integrity of the election process with chief election officials and such designees who have received a security clearance under subsection (b).

(2) Coordination

The Under Secretary of Homeland Security for Intelligence and Analysis shall coordinate with the Director of National Intelligence and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department (as specified in section 113(a)(1)(H) of title 6) to facilitate the sharing of information to the affected Secretaries of State or States.

(Pub. L. 116-92, div. E, title LXV, § 6506, Dec. 20, 2019, 133 Stat. 2206.)

§ 3371c. Notification of significant foreign cyber intrusions and active measures campaigns directed at elections for Federal offices

(a) Definitions

In this section:

(1) Active measures campaign

The term “active measures campaign” means a foreign semi-covert or covert intelligence operation.

(2) Candidate, election, and political party

The terms “candidate”, “election”, and “political party” have the meanings given those terms in section 30101 of title 52.

(3) Congressional leadership

The term “congressional leadership” includes the following:

(A) The majority leader of the Senate.

(B) The minority leader of the Senate.

(C) The Speaker of the House of Representatives.

(D) The minority leader of the House of Representatives.

(4) Cyber intrusion

The term “cyber intrusion” means an electronic occurrence that actually or imminently jeopardizes, without lawful authority, electronic election infrastructure, or the integrity, confidentiality, or availability of information within such infrastructure.

(5) Electronic election infrastructure

The term “electronic election infrastructure” means an electronic information system of any of the following that is related to an election for Federal office:

(A) The Federal Government.

(B) A State or local government.

(C) A political party.

(D) The election campaign of a candidate.

(6) Federal office

The term “Federal office” has the meaning given that term in section 30101 of title 52.

(7) High confidence

The term “high confidence”, with respect to a determination, means that the determination is based on high-quality information from multiple sources.

(8) Moderate confidence

The term “moderate confidence”, with respect to a determination, means that a determination is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.

(9) Other appropriate congressional committees

The term “other appropriate congressional committees” means—

(A) the Committee on Armed Services, the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

(b) Determinations of significant foreign cyber intrusions and active measures campaigns

The Director of National Intelligence, the Director of the Federal Bureau of Investigation,

and the Secretary of Homeland Security shall jointly carry out subsection (c) if such Directors and the Secretary jointly determine—

(1) that on or after December 20, 2019, a significant foreign cyber intrusion or active measures campaign intended to influence an upcoming election for any Federal office has occurred or is occurring; and

(2) with moderate or high confidence, that such intrusion or campaign can be attributed to a foreign state or to a foreign nonstate person, group, or other entity.

(c) Briefing

(1) In general

Not later than 14 days after making a determination under subsection (b), the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the Secretary of Homeland Security shall jointly provide a briefing to the congressional leadership, the congressional intelligence committees and, consistent with the protection of sources and methods, the other appropriate congressional committees. The briefing shall be classified and address, at a minimum, the following:

(A) A description of the significant foreign cyber intrusion or active measures campaign, as the case may be, covered by the determination.

(B) An identification of the foreign state or foreign nonstate person, group, or other entity, to which such intrusion or campaign has been attributed.

(C) The desirability and feasibility of the public release of information about the cyber intrusion or active measures campaign.

(D) Any other information such Directors and the Secretary jointly determine appropriate.

(2) Electronic election infrastructure briefings

With respect to a significant foreign cyber intrusion covered by a determination under subsection (b), the Secretary of Homeland Security, in consultation with the Director of National Intelligence and the Director of the Federal Bureau of Investigation, shall offer to the owner or operator of any electronic election infrastructure directly affected by such intrusion, a briefing on such intrusion, including steps that may be taken to mitigate such intrusion. Such briefing may be classified and made available only to individuals with appropriate security clearances.

(3) Protection of sources and methods

This subsection shall be carried out in a manner that is consistent with the protection of sources and methods.

(Pub. L. 116–92, div. E, title LXV, § 6507, Dec. 20, 2019, 133 Stat. 2207.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definition of “congressional intelligence committees” as used in this section, see section 5003 of div. E of Pub. L. 116–92, set out as a note under section 3003 of this title.

§ 3371d. Designation of counterintelligence officer to lead election security matters

(a) In general

The Director of National Intelligence shall designate a national counterintelligence officer within the National Counterintelligence and Security Center to lead, manage, and coordinate counterintelligence matters relating to election security.

(b) Additional responsibilities

The person designated under subsection (a) shall also lead, manage, and coordinate counterintelligence matters relating to risks posed by interference from foreign powers (as defined in section 1801 of this title) to the following:

(1) The Federal Government election security supply chain.

(2) Election voting systems and software.

(3) Voter registration databases.

(4) Critical infrastructure related to elections.

(5) Such other Government goods and services as the Director of National Intelligence considers appropriate.

(Pub. L. 116–92, div. E, title LXV, § 6508, Dec. 20, 2019, 133 Stat. 2208.)

§ 3372. Monitoring mineral investments under Belt and Road Initiative of People’s Republic of China

(a) Report required

Not later than 1 year after December 27, 2020, the Director of National Intelligence (referred to in this section as the “Director”), in consultation with the Secretary of the Interior, the Secretary of Energy, the Secretary of Commerce, the Secretary of State, the Secretary of Defense, and the United States Trade Representative, shall submit to the appropriate congressional committees a report on investments in minerals under the Belt and Road Initiative of the People’s Republic of China that includes an assessment of—

(1) notable past mineral investments;

(2) whether and how such investments have increased the extent of control of minerals by the People’s Republic of China;

(3) any efforts by the People’s Republic of China to counter or interfere with the goals of the Energy Resource Governance Initiative of the Department of State; and

(4) the strategy of the People’s Republic of China with respect to mineral investments.

(b) Monitoring mechanism

In conjunction with each report required by subsection (a), the Director shall submit to the appropriate congressional committees a list of any minerals with respect to which—

(1) the People’s Republic of China, directly or through the Belt and Road Initiative—

(A) is increasing its concentration of extraction and processing;

(B) is acquiring significant mining and processing facilities;

(C) is maintaining or increasing export restrictions; or

(D) has achieved substantial control of the supply of minerals used within an industry or related minerals;