terintelligence (as defined in section 3003 of this title) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Consistent with the responsibility of the Director of Central Intelligence to protect intelligence sources and methods, and the responsibility of the Attorney General to protect sensitive law enforcement information, it shall be lawful for information revealing a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

(2) Definition

In this section, the term ''foreign intelligence information'' means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

(Pub. L. 107–56, title II, § 203(d), Oct. 26, 2001, 115 Stat. 281; Pub. L. 107–296, title VIII, § 897(a), Nov. 25, 2002, 116 Stat. 2257.)

Editorial Notes

CODIFICATION

Section was formerly classified to section 403–5d of this title prior to editorial reclassification and renumbering as this section.

AMENDMENTS

2002—Par. (1). Pub. L. 107–296 inserted at end ''Consistent with the responsibility of the Director of Central Intelligence to protect intelligence sources and methods, and the responsibility of the Attorney General to protect sensitive law enforcement information, it shall be lawful for information revealing a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.''

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of this title.

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

§ 3366. Authorities of heads of other departments and agencies

Notwithstanding any other provision of law, the head of any department or agency of the United States is authorized to receive and utilize funds made available to the department or agency by the Director of National Intelligence pursuant to section 3024(d)(2) of this title, as amended by subsection (a), and receive and utilize any system referred to in such section that is made available to such department or agency.

(Pub. L. 111–259, title IV, § 402(b), Oct. 7, 2010, 124 Stat. 2709.)

Editorial Notes

REFERENCES IN TEXT

Subsection (a), referred to in text, is subsec. (a) of section 402 of Pub. L. 111–259, title IV, Oct. 7, 2010, 124 Stat. 2708, which amended section 403–1 of this title

prior to editorial reclassification and renumbering as section 3024 of this title.

CODIFICATION

Section was formerly classified as a note under section 403–1 of this title prior to editorial reclassification as this section.

§ 3367. Requirement for efficient use by intelligence community of open-source intelligence

The Director of National Intelligence shall ensure that the intelligence community makes efficient and effective use of open-source information and analysis.

(Pub. L. 108–458, title I, § 1052(b), Dec. 17, 2004, 118 Stat. 3683.)

Editorial Notes

CODIFICATION

Section was formerly classified as a note under section 403–1 of this title prior to editorial reclassification as this section.

§ 3368. Assistance for governmental entities and private entities in recognizing online violent extremist content

(a) Assistance to recognize online violent extremist content

Not later than 180 days after May 5, 2017, and consistent with the protection of intelligence sources and methods, the Director of National Intelligence shall publish on a publicly available Internet website a list of all logos, symbols, insignia, and other markings commonly associated with, or adopted by, an organization designated by the Secretary of State as a foreign terrorist organization under section 1189(a) of title 8.

(b) Updates

The Director shall update the list published under subsection (a) every 180 days or more frequently as needed.

(Pub. L. 115–31, div. N, title IV, § 403, May 5, 2017, 131 Stat. 820.)

§ 3369. Cooperative actions to detect and counter foreign influence operations

(a) Findings

Congress makes the following findings:

(1) The Russian Federation, through military intelligence units, also known as the ''GRU'', and Kremlin-linked troll organizations often referred to as the ''Internet Research Agency'', deploy information warfare operations against the United States, its allies and partners, with the goal of advancing the strategic interests of the Russian Federation.

(2) One line of effort deployed as part of these information warfare operations is the weaponization of social media platforms with the goals of intensifying societal tensions, undermining trust in governmental institutions within the United States, its allies and partners in the West, and generally sowing division, fear, and confusion.

(3) These information warfare operations are a threat to the national security of the United States and that of the allies and partners of the United States. As former Director of National Intelligence Dan Coats stated, ''These actions are persistent, they are pervasive and they are meant to undermine America's democracy.''.

(4) These information warfare operations continue to evolve and increase in sophistication.

(5) Other foreign adversaries and hostile non-state actors are increasingly adopting similar tactics of deploying information warfare operations against the West, such as recent state-backed operations from China around the Hong Kong protests identified by social media companies.

(6) Technological advances, including artificial intelligence, will only make it more difficult in the future to detect fraudulent accounts, deceptive material posted on social media, and malign behavior on social media platforms.

(7) Because these information warfare operations are deployed within and across private social media platforms, the companies that own these platforms have a responsibility to detect and facilitate the removal or neutralization of foreign adversary networks operating clandestinely on their platforms.

(8) The social media companies are inherently technologically sophisticated and adept at rapidly analyzing large amounts of data and developing software-based solutions to diverse and ever-changing challenges on their platforms, which makes them well-equipped to address the threat occurring on their platforms.

(9) Independent analyses confirmed Kremlin-linked threat networks, based on data provided by several social media companies to the Select Committee on Intelligence of the Senate, thereby demonstrating that it is possible to discern both broad patterns of cross-platform information warfare operations and specific fraudulent behavior on social media platforms.

(10) General Paul Nakasone, Director of the National Security Agency, emphasized the importance of these independent analyses to the planning and conducting of military cyber operations to frustrate Kremlin-linked information warfare operations against the 2018 midterm elections. General Nakasone stated that the reports ''were very, very helpful in terms of being able to understand exactly what our adversary was trying to do to build dissent within our nation.''.

(11) Institutionalizing ongoing robust, independent, and vigorous analysis of data related to foreign threat networks within and across social media platforms will help counter ongoing information warfare operations against the United States, its allies, and its partners.

(12) Archiving and disclosing to the public the results of these analyses by the social media companies and trusted third-party experts in a transparent manner will serve to demonstrate that the social media companies are detecting and removing foreign malign activities from their platforms while protecting the privacy of the people of the United States and will build public understanding of the