

§ 7408. National Academy of Sciences study on computer and network security in critical infrastructures

(a) Study

Not later than 3 months after November 27, 2002, the Director of the National Institute of Standards and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to conduct a study of the vulnerabilities of the Nation's network infrastructure and make recommendations for appropriate improvements. The National Research Council shall—

(1) review existing studies and associated data on the architectural, hardware, and software vulnerabilities and interdependencies in United States critical infrastructure networks;

(2) identify and assess gaps in technical capability for robust critical infrastructure network security and make recommendations for research priorities and resource requirements; and

(3) review any and all other essential elements of computer and network security, including security of industrial process controls, to be determined in the conduct of the study.

(b) Report

The Director of the National Institute of Standards and Technology shall transmit a report containing the results of the study and recommendations required by subsection (a) to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Science not later than 21 months after November 27, 2002.

(c) Security

The Director of the National Institute of Standards and Technology shall ensure that no information that is classified is included in any publicly released version of the report required by this section.

(d) Authorization of appropriations

There are authorized to be appropriated to the Secretary of Commerce for the National Institute of Standards and Technology for the purposes of carrying out this section, \$700,000.

(Pub. L. 107-305, §12, Nov. 27, 2002, 116 Stat. 2380.)

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Science of House of Representatives changed to Committee on Science and Technology of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Science and Technology of House of Representatives changed to Committee on Science, Space, and Technology of House of Representatives by House Resolution No. 5, One Hundred Twelfth Congress, Jan. 5, 2011.

§ 7409. Coordination of Federal cyber security research and development

The Director of the National Science Foundation and the Director of the National Institute of Standards and Technology shall coordinate the research programs authorized by this chapter or pursuant to amendments made by this

chapter. The Director of the Office of Science and Technology Policy shall work with the Director of the National Science Foundation and the Director of the National Institute of Standards and Technology to ensure that programs authorized by this chapter or pursuant to amendments made by this chapter are taken into account in any government-wide cyber security research effort.

(Pub. L. 107-305, §13, Nov. 27, 2002, 116 Stat. 2380.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, was in the original “this Act”, meaning Pub. L. 107-305, Nov. 27, 2002, 116 Stat. 2367, known as the Cyber Security Research and Development Act, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7401 of this title.

§ 7410. Grant eligibility requirements and compliance with immigration laws

(a) Immigration status

No grant or fellowship may be awarded under this chapter, directly or indirectly, to any individual who is in violation of the terms of his or her status as a nonimmigrant under section 1101(a)(15)(F), (M), or (J) of title 8.

(b) Aliens from certain countries

No grant or fellowship may be awarded under this chapter, directly or indirectly, to any alien from a country that is a state sponsor of international terrorism, as defined under section 1735(b) of title 8, unless the Secretary of State determines, in consultation with the Attorney General and the heads of other appropriate agencies, that such alien does not pose a threat to the safety or national security of the United States.

(c) Non-complying institutions

No grant or fellowship may be awarded under this chapter, directly or indirectly, to any institution of higher education or non-profit institution (or consortia thereof) that has—

(1) materially failed to comply with the recordkeeping and reporting requirements to receive nonimmigrant students or exchange visitor program participants under section 1101(a)(15)(F), (M), or (J) of title 8, or section 1372 of title 8, as required by section 1762 of title 8; or

(2) been suspended or terminated pursuant to section 1762(c) of title 8.

(Pub. L. 107-305, §16, Nov. 27, 2002, 116 Stat. 2381.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, was in the original “this Act”, meaning Pub. L. 107-305, Nov. 27, 2002, 116 Stat. 2367, known as the Cyber Security Research and Development Act, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7401 of this title and Tables.

§ 7411. Report on grant and fellowship programs

Within 24 months after November 27, 2002, the Director, in consultation with the Assistant to

the President for National Security Affairs, shall submit to Congress a report reviewing this chapter to ensure that the programs and fellowships are being awarded under this chapter to individuals and institutions of higher education who are in compliance with the Immigration and Nationality Act (8 U.S.C. 1101 *et seq.*) in order to protect our national security.

(Pub. L. 107-305, §17, Nov. 27, 2002, 116 Stat. 2381.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, was in the original “this Act”, meaning Pub. L. 107-305, Nov. 27, 2002, 116 Stat. 2367, known as the Cyber Security Research and Development Act, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 7401 of this title and Tables.

The Immigration and Nationality Act, referred to in text, is act June 27, 1952, ch. 477, 66 Stat. 163, which is classified principally to chapter 12 (§1101 *et seq.*) of Title 8, Aliens and Nationality. For complete classification of this Act to the Code, see Short Title note set out under section 1101 of Title 8 and Tables.

CHAPTER 100A—CYBERSECURITY ENHANCEMENT

Sec.	
7421.	Definitions.
7422.	No regulatory authority.
7423.	No additional funds authorized.

SUBCHAPTER I—CYBERSECURITY RESEARCH AND DEVELOPMENT

7431.	Federal cybersecurity research and development.
7432.	National cybersecurity challenges.

SUBCHAPTER II—EDUCATION AND WORKFORCE DEVELOPMENT

7441.	Cybersecurity competitions and challenges.
7442.	Federal Cyber Scholarship-for-Service Program.
7443.	National cybersecurity awareness and education program.

SUBCHAPTER III—CYBERSECURITY AWARENESS AND PREPAREDNESS

7451.	Transferred.
-------	--------------

SUBCHAPTER IV—ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

7461.	Definitions.
7462.	International cybersecurity technical standards.
7463.	Cloud computing strategy.
7464.	Identity management research and development.

§ 7421. Definitions

In this chapter:

(1) Cybersecurity mission

The term “cybersecurity mission” means activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as such activities relate to the security and stability of cyberspace.

(2) Information system

The term “information system” has the meaning given that term in section 3502 of title 44.

(Pub. L. 113-274, §2, Dec. 18, 2014, 128 Stat. 2971.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, was in the original “this Act”, meaning Pub. L. 113-274, Dec. 18, 2014, 128 Stat. 2971, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out below and Tables.

Statutory Notes and Related Subsidiaries

SHORT TITLE

Pub. L. 113-274, §1(a), Dec. 18, 2014, 128 Stat. 2971, provided that: “This Act [enacting this chapter and amending sections 272, 278g-3, 7403, and 7406 of this title] may be cited as the ‘Cybersecurity Enhancement Act of 2014.’”

Executive Documents

EX. ORD. NO. 13984. TAKING ADDITIONAL STEPS TO ADDRESS THE NATIONAL EMERGENCY WITH RESPECT TO SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES

Ex. Ord. No. 13984, Jan. 19, 2021, 86 F.R. 6837, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 301 of title 3, United States Code:

I, DONALD J. TRUMP, President of the United States of America, find that additional steps must be taken to deal with the national emergency related to significant malicious cyber-enabled activities declared in Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended [50 U.S.C. 1701 note], to address the use of United States Infrastructure as a Service (IaaS) products by foreign malicious cyber actors. IaaS products provide persons the ability to run software and store data on servers offered for rent or lease without responsibility for the maintenance and operating costs of those servers. Foreign malicious cyber actors aim to harm the United States economy through the theft of intellectual property and sensitive data and to threaten national security by targeting United States critical infrastructure for malicious cyber-enabled activities. Foreign actors use United States IaaS products for a variety of tasks in carrying out malicious cyber-enabled activities, which makes it extremely difficult for United States officials to track and obtain information through legal process before these foreign actors transition to replacement infrastructure and destroy evidence of their prior activities; foreign resellers of United States IaaS products make it easier for foreign actors to access these products and evade detection. This order provides authority to impose record-keeping obligations with respect to foreign transactions. To address these threats, to deter foreign malicious cyber actors’ use of United States IaaS products, and to assist in the investigation of transactions involving foreign malicious cyber actors, the United States must ensure that providers offering United States IaaS products verify the identity of persons obtaining an IaaS account (“Account”) for the provision of these products and maintain records of those transactions. In appropriate circumstances, to further protect against malicious cyber-enabled activities, the United States must also limit certain foreign actors’ access to United States IaaS products. Further, the United States must encour-