

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, as amended, 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.

SUBCHAPTER II—EDUCATION AND WORKFORCE DEVELOPMENT

- 7441. Cybersecurity competitions and challenges.
- 7442. Federal Cyber Scholarship-for-Service Program.

SUBCHAPTER III—CYBERSECURITY AWARENESS AND PREPAREDNESS

- 7451. National cybersecurity awareness and education program.

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.)

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.

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.’”

§ 7422. No regulatory authority

Nothing in this chapter shall be construed to confer any regulatory authority on any Federal, State, tribal, or local department or agency.

(Pub. L. 113–274, § 3, Dec. 18, 2014, 128 Stat. 2972.)

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 under section 7421 of this title and Tables.

§ 7423. No additional funds authorized

No additional funds are authorized to carry out this Act, and the amendments made by this Act. This Act, and the amendments made by this Act, shall be carried out using amounts otherwise authorized or appropriated.

(Pub. L. 113–274, § 4, Dec. 18, 2014, 128 Stat. 2972.)

REFERENCES IN TEXT

This Act, and the amendments made by this Act, referred to in text, is Pub. L. 113–274, Dec. 18, 2014, 128 Stat. 2971, which enacted this chapter and amended sections 272, 278g–3, 7403, and 7406 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 7421 of this title and Tables.

SUBCHAPTER I—CYBERSECURITY RESEARCH AND DEVELOPMENT

§ 7431. Federal cybersecurity research and development

(a) Fundamental cybersecurity research

(1) Federal cybersecurity research and development strategic plan

The heads of the applicable agencies and departments, working through the National Science and Technology Council and the Networking and Information Technology Research and Development Program, shall develop and update every 4 years a Federal cybersecurity research and development strategic plan (referred to in this subsection as the “strategic plan”) based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development for information technology and networking systems. The heads of the applicable agencies and departments shall build upon existing programs and plans to develop the strategic plan to meet objectives in cybersecurity, such as—

(A) how to design and build complex software-intensive systems that are secure and reliable when first deployed;

(B) how to test and verify that software and hardware, whether developed locally or obtained from a third party, is free of significant known security flaws;

(C) how to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality;