

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;

(D) how to guarantee the privacy of an individual, including that individual’s identity, information, and lawful transactions when stored in distributed systems or transmitted over networks;

(E) how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet;

(F) how to determine the origin of a message transmitted over the Internet;

(G) how to support privacy in conjunction with improved security;

(H) how to address the problem of insider threats;

(I) how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity;

(J) how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services; and

(K) any additional objectives the heads of the applicable agencies and departments, in coordination with the head of any relevant Federal agency and with input from stakeholders, including appropriate national laboratories, industry, and academia, determine appropriate.

(2) Requirements

(A) Contents of plan

The strategic plan shall—

(i) specify and prioritize near-term, mid-term, and long-term research objectives, including objectives associated with the research identified in section 7403(a)(1) of this title;

(ii) specify how the near-term objectives described in clause (i) complement research and development areas in which the private sector is actively engaged;

(iii) describe how the heads of the applicable agencies and departments will focus on innovative, transformational technologies with the potential to enhance the security, reliability, resilience, and trustworthiness of the digital infrastructure, and to protect consumer privacy;

(iv) describe how the heads of the applicable agencies and departments will foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely benefit of society and the national interest, including through the dissemination of best practices and other outreach activities;

(v) describe how the heads of the applicable agencies and departments will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems; and

(vi) describe how the heads of the applicable agencies and departments will facilitate access by academic researchers to the infrastructure described in clause (v), as well as to relevant data, including event data.