H.R. 756, CYBERSECURITY ENHANCEMENT ACT OF 2013

TITLE I – RESEARCH AND DEVELOPMENT

SEC. 101. DEFINITIONS

Defines the terms National Coordination Office and Program in the title.

SEC. 102. FINDINGS

Describes the findings of this title.

SEC. 103. CYBERSECURITY STRATEGIC R&D PLAN

Requires the agencies to develop, update and implement a strategic plan for cybersecurity research and development (R&D). Requires that the strategic plan be based on an assessment of cybersecurity risk, that it specify and prioritize near-term, mid-term and long-term research objectives and that it describe how the near-term objectives complement R&D occurring in the private sector.

Requires the agencies to solicit input from an advisory committee and outside stakeholders in the development of the strategic plan. Additionally, requires the agencies to describe how they will promote innovation, foster technology transfer, and maintain a national infrastructure for the development of secure, reliable, and resilient networking and information technology systems.

Requires the development of an implementation roadmap that specifies the role of each agency and the level of funding needed to meet each of the research objectives outlined in the strategic plan.

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBERSECURITY

Adds research on the social and behavioral aspects of cybersecurity to the list of cybersecurity research areas that the National Science Foundation may support as part of its total cybersecurity research portfolio.

SEC. 105. NSF CYBERSECURITY R&D PROGRAMS

Reauthorizes the cybersecurity research program at the NSF and includes identity management as one of the research areas supported.

Reauthorizes programs at NSF that provide funding for capacity building grants, graduate student fellowships, graduate student traineeships and research centers in cybersecurity.

Repeals NSF cybersecurity faculty development traineeship program.

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM

Authorizes the cybersecurity scholarship for service program at NSF. The program provides grants to institutions of higher education for the award of scholarships to students pursuing undergraduate and graduate degrees in cybersecurity fields and requires an additional year of service over the number of years for which the scholarship was received.

The program also provides capacity building grants to institutions of higher education, supporting such activities as faculty professional development and the development of cybersecurity-related curricula and courses.

SEC. 107. CYBERSCURITY WORKFORCE ASSESSMENT

Requires the President to issue a report assessing the current and future cybersecurity workforce needs of the federal government, including a comparison of the skills sought by Federal agencies and the private sector; an examination of the supply of cybersecurity talent and the capacity of institutions of higher education to produce cybersecruity professionals; and the identification of any barriers to the recruitment and hiring of cybersecurity professionals.

SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE

Establishes a university-industry task force to explore mechanisms and models for carrying out public-private research partnerships in the area of cybersecurity.

SEC. 109. CYBERSECURITY CHECKLIST AND DISSEMINATION

Updates NIST's authority for the National Checklist Program (NCP) which provides detailed guidance on setting the security configuration of operating systems and applications for the federal government, and requires NIST to develop automated security specifications with respect to checklist content.

SEC. 110. NIST CYBERSECURITY R&D

Amends the National Institute of Standards and Technology Act to codify NIST cybersecurity research and development activities; NIST is authorized to conduct research on the development of a unifying and standardized identity, privilege, and access control management framework and to conduct research related to improving the security of information and networked systems, including the security of industrial control systems.

TITLE II — ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

SEC. 201. DEFINITIONS

Defines the terms Director and Institute in the title.

SEC. 202. INTERNATIONAL CYBERSECURITY TECHNICAL STANDARDS

Requires NIST to consult with the private sector and others to develop and implement a plan to ensure a coordinated United States Government representation in international cybersecurity technical standards development. This plan is due to Congress no later than one year after enactment.

SEC. 203. CLOUD COMPUTING STRATEGY

Directs NIST, in collaboration with Federal agencies and other stakeholders, to continue to develop and implement a comprehensive strategy for the use and adoption of cloud computing services by the Federal government. The strategy should consider activities that accelerate standards development, the development of processes to test standards conformance, and the security of data stored in the cloud.

SEC. 204. PROMOTING CYBERSECURITY AWARENESS AND EDUCATION

Requires NIST to maintain a cybersecurity awareness and education program and to deliver a strategic plan to Congress within 1 year describing the implementation of this program. Requires the program to be aimed at disseminating cybersecurity best practices and standards and include how NIST will make these usable by individuals, small business, state and local governments, and educational institutions.

SEC. 205. IDENTITY MANAGEMENT RESEARCH AND DEVELOPMENT

Requires NIST to continue research and development programs to improve identity management systems.

SEC. 206.

States that no additional funds are authorized for the NIST activities in the bill.