U.S. Non-Military Cybersecurity Research & Development and Related Policies

U.S. House of Representatives passed Cybersecurity Enhancement Act of 2013 (H.R. 756); and the U.S. Senate Commerce, Science, & Transportation Committee passed Cybersecurity Act of 2013 (S. 1353)

There are a plethora of legislative proposals currently being considered in Congress regarding cybersecurity, and certainly more can be expected. These proposals range a broad spectrum of issues dealing with privacy and information sharing to cybercrime offenses and punishment. However, this document primarily deals with non-military cybersecurity research and development, National Institute of Standards and Technology (NIST) activities, federal cybersecurity workforce issues, and promotion of cybersecurity awareness and education efforts, among other things.

Cybersecurity Federal Research and Development Strategic Plan

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 103 would direct, not later than 12 months after the date of enactment of H.R. 756, the Department of Agriculture, the Department of Commerce, the Department of Defense, the Department of Education, the Department of Energy, the Department of Health and Human Services, the Department of the Interior, the Environmental Protection Agency, the National Aeronautics and Space Administration, and the National Science Foundation, working through the National Science and Technology Council and with the assistance of the National Coordination Office, would be required to provide "Congress a 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." In addition, after the initial strategic plan is transmitted to Congress, every 3 years thereafter, the above mentioned agencies would be required to "prepare and transmit to Congress an update of such plan." The strategic plan would be required to include:
    - First, specification and prioritization of "near-term, mid-term and long-term research objectives, including objectives associated with the research areas" that include: authentication, cryptography, and other secure data communications technology; computers forensics and intrusion detection; reliability of computer and network applications, middleware, operating systems, control systems, and communications infrastructure; privacy and confidentiality; network security architecture, including tools for security administration and analysis; emerging threats; vulnerability assessments and techniques for quantifying risk; remote access and wireless security; and enhancement of law enforcement ability to detect, investigate, and prosecute cyber-

crimes, including those that involve privacy of intellectual property; "and how the near-term objectives complement research and development areas in which the private sector is actively engaged."
    - Second, describe how the Networking and Information Technology Research and Development (NITRD) program "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."
    - Third, describe how the Networking and Information Technology Research and Development program "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."
    - Fourth, describe how the Networking and Information Technology Research and Development program "will establish and maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems."
    - Fifth, describe how the Networking and Information Technology Research and Development program "will facilitate access by academic researchers to the infrastructure" described above, "as well as to relevant data, including event data."
    - Sixth, describe how the Networking and Information Technology Research and Development program will engage minorities "to foster a more diverse workforce in this area."
    - Seventh, describe how the Networking and Information Technology Research and Development program "will help to recruit and prepare veterans for the Federal cybersecurity workforce."
- Section 103 would also direct the Department of Agriculture, the Department of Commerce, the Department of Defense, the Department of Education, the Department of Energy, the Department of Health and Human Services, the Department of the Interior, the Environmental Protection Agency, the National Aeronautics and Space Administration, and the National Science Foundation to "develop and annually update an implementation roadmap for the strategic plan." The roadmap would be required to include:
    - First, specification of "the role of each Federal agency in carrying out or sponsoring research and development to meet the research objectives of the strategic plan, including a description of how progress toward the research objectives will be evaluated."
    - Second, specification of "the funding allocated to each major research objective of the strategic plan and the source of funding by agency for the current fiscal year."
    - Third, an estimation of "the funding required for each major research objective of the strategic plan for the following 3 fiscal years."
- In addition, Section 103 would direct the above mentioned agencies, in developing and updating their strategic plans, to solicit recommendations and advice from: NITRD's advisory committees established in the High-Performance Computing Act of 1991; and "a wide range of stakeholders, including industry, academia, including representatives of minority serving institutions and community colleges, National Laboratories, and other relevant organizations and institutions."
- Finally, the above outlined agencies involved in developing and updating their strategic plans would be required to "establish, in coordination with the Office of Management and Budget, a mechanism to track ongoing and completed Federal cybersecurity research and development projects and associated funding."

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 201 would require the Director of the Office of Science and Technology Policy (OSTP), in coordination with the head of any relevant Federal agency, to "build upon programs and plans in effect", as of the date of enactment of S. 1353, "to develop a Federal cybersecurity research and development plan to meet objectives in cybersecurity," which would include:
    - First, "how to design and build complex software-intensive systems that are secure and reliable when first deployed."
    - Second, "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."
    - Third, "how to test and verify that software and hardware obtained from a third party correctly implements stated functionality, and only that functionality."
    - Fourth, "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."
    - Fifth, "how to build new protocols to enable the Internet to have robust security as one of the key capabilities of the Internet."
    - Sixth, "how to determine the origin of a message transmitted over the Internet."
    - Seventh, "how to support privacy in conjunction with improved security."
    - Eighth, "how to address the growing problem of insider threats."
    - Ninth, "how improved consumer education and digital literacy initiatives can address human factors that contribute to cybersecurity."
    - Tenth, "how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services."
    - Eleventh, "any additional objectives the Director of the Office of Science and Technology Policy, in coordination with the head of any relevant Federal agency and with input from stakeholders, including industry and academia, determines appropriate."
- Section 201 would also require the Federal cybersecurity research and development plan to "identify and prioritize near-term, mid-term, and long-term research in computer and information science and engineering to meet the" eleven objectives outlined above, including research in the areas of: authentication, cryptography, and other secure data communications technology; computers forensics and intrusion detection; reliability of computer and network applications, middleware, operating systems, control systems, and communications infrastructure; privacy and confidentiality; network security architecture, including tools for security administration and analysis; emerging threats; vulnerability assessments and techniques for quantifying risk; remote access and wireless security; and enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve privacy of intellectual property.
- Further, "in developing, implementing, and updating the Federal cybersecurity research and development plan, the Director of the Office of Science and Technology Policy" would be required to "work in close cooperation with industry, academia, and other interested stakeholders to ensure, to the extent possible, that Federal cybersecurity research and development is not duplicative of private sector efforts." The Federal cybersecurity research and development plan would be required to "be updated triennially."
- Section 201 would direct the Director of OSTP to "coordinate, to the extent practicable, Federal research and development activities" outlined in Section 201 "with other ongoing research and development security-related initiatives, including research being conducted by: the National Science Foundation; the National Institute of Standards and Technology; the Department of Homeland Security; other Federal agencies; other Federal and private research laboratories,

research entities, and universities; institutions of higher education; relevant nonprofit organizations; and international partners of the United States."

- Finally, the Director of the Office of Science and Technology Policy would be required to submit the plan, not later than 1 year after the date of enactment of S. 1353, and each updated plan to Congress.

Federal Cyber Scholarship for Service Program

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 106 would direct the Director of the National Science Foundation to "continue a Scholarship for Service program" and to "recruit and train the next generation of Federal cybsersecurity professionals and to increase the capacity of the higher education system to produce an information technology workforce with the skills necessary to enhance the security of the" United States' "communications and information infrastructure." The Scholarship for Service program would be required to:
    - First, "provide, through qualified institutions of higher education, including community colleges, scholarships that provide tuition, fees, and a competitive stipend for up to 2 years to students pursuing a bachelor's or master's degree and up to 3 years to students pursuing a doctoral degree in a cybersecurity field."
    - Second, "provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce."
    - Third, "increase the capacity of institutions of higher education throughout all regions of the United States to produce highly qualified cybersecurity professionals, through the award of competitive, merit-reviewed grants that support such activities as: (a) faculty professional development including technical, hands-on experiences in the private sector or government, workshops, seminars, conferences, and other professional development opportunities that will result in improved instructional capabilities; (b) institutional partnerships, including minority serving institutions and community colleges; (c) development and evaluation of cybersecurity-related courses and curricula; and (d) public-private partnerships that will integrate research experiences and hands-on learning into cybersecurity degree programs."
- In addition, "if an individual receives a scholarship under" section 106, "as a condition of receiving such scholarship, the individual upon completion of their degree must serve as a cybersecurity professional within the Federal workforce for" at least "1 year more than the number of years for which the scholarship was received". However, "if a scholarship recipient is not offered employment by a Federal agency or a federally funded research and development center, the service requirement can be satisfied at the Director's discretion by: (a) serving as a cybersecurity professional in a State, local, or tribal government agency; or (b) teaching cybersecurity courses at an institution of higher education."

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 302 would direct the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management and Secretary of Homeland Security, to "continue a Federal Cyber Scholarship for Service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments." The Scholarship for Service program would be required to:
    - First, "provide scholarships to students who are enrolled in programs of study at institutions of higher education leading to degrees or specialized program certifications in the cybersecurity field."

- Second, "provide the scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the Federal information technology workforce."
- Third, "provide a procedure by which the National Science Foundation or a Federal agency, consistent with regulations of the Office of Personnel Management, may request and fund security clearances for scholarship recipients, including providing for clearances during internships or other temporary appointments and after receipt of their degrees."

- In addition, "each scholarship recipient, as a condition of receiving a scholarship under the program," would be required to "enter into an agreement under which the recipient agrees to work in the cybersecurity mission of a Federal, State, local, or tribal agency for a period equal to the length of the scholarship following receipt of the student's degree."

Strategic Plan for Promoting Cybersecurity Awareness and Education

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 204 would direct the Director of NIST, in collaboration with relevant Federal agencies, industry, educational institutions, National Laboratories, the National Coordination Office of the Networking and Information Technology Research and Development program, and other organizations, to "continue to coordinate a cybersecurity awareness and education program to increase knowledge, skills, and awareness of cybersecurity risks, consequences, and best practices through":
  - First, "the widespread dissemination of cybersecurity technical standards and best practices identified by NIST."
  - Second, "efforts to make cybersecurity best practices usable by individuals, small to medium-sized business, State, local, and tribal governments, and education institutions."
  - Third, "improving the state of cybersecurity education at all educational levels."
  - Fourth, "efforts to attract, recruit, and retain qualified professionals to the Federal cybersecurity workforce."
  - Fifth, "improving the skills, training, and professional development of the Federal cybersecurity workforces."
- In addition, the Director of NIST, in coordination with relevant Federal agencies and other stakeholders, would be required to "develop and implement a strategic plan to guide Federal programs and activities in support of a comprehensive cybersecurity awareness and education program as" outlined above. Further, not later than 1 year after the date of enactment of H.R. 756 and every 5 years thereafter, the Director would be required to "transmit the strategic plan" to Congress.

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 401 would direct the Director of NIST, in consultation with appropriate Federal agencies, to "continue to coordinate a national cybersecurity awareness and preparedness campaign" that would:
  - First, "increase the public awareness of cybersecurity, cyber safety, and cyber ethics, including the use of the Internet, social media, entertainment, and other media to reach the public."
  - Second, "increase the understanding of State and local governments and private sector entities of: (a) the benefits of ensuring effective risk management of the information infrastructure versus the costs of failure to do so; and (b) the methods to mitigate and remediate vulnerabilities."

- Third, "support for formal cybersecurity education programs at all education levels to prepare skilled cybersecurity and computer science workers for the private sector and Federal, State, and local government."
- Fourth, create "initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal government and develop strategies for recruitment, training, and retention."

- Further, the Section 401 campaign would be required to "leverage existing programs designed to inform the public of safety and security of products or services, including self-certifications and independently verified assessments regarding the quantification and valuation of information security risk."
- In addition, the Director of NIST, in cooperation with relevant Federal agencies and other stakeholders, would be required to "build upon programs and plans in effect" as of the date of enactment of S. 1353 "to develop and implement a strategic plan to guide Federal programs and activities in support of the national cybersecurity awareness and preparedness campaign." Further, not later than 1 year after the date of enactment of S. 1353, and every 5 years thereafter, the Director of NIST would be required to "transmit the strategic plan" to Congress.

Cybersecurity Workforce Assessment

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 107 would require the President, not later than 180 days after the date of enactment of H.R. 756 to "transmit to the Congress a report addressing the cybersecurity workforce needs of the Federal Government." The report would be required to include:
  - First, "an examination of the current state of and the projected needs of the Federal cybersecurity workforce, including a comparison of the different agencies and departments, and an analysis of the capacity of such agencies and departments to meet those needs."
  - Second, "an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector, and a description of how successful programs are engaging the talents of females" and other minorities.
  - Third, "an examination of the effectiveness of the National Centers of Academic Excellence in Information Assurance Education, the Centers of Academic Excellence in Research, and the Federal Cyber Scholarship for Service programs in promoting higher education and research in cybersecurity and information assurance and in producing a growing number of professionals with the necessary cybersecurity and information assurance expertise, including individuals from States or regions in which the unemployment rate exceeds the national average."
  - Fourth, "an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibilities."
  - Fifth, "recommendations for Federal policies to ensure an adequate, well-trained Federal cybersecurity workforce."

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 303 would require the Director of the National Science Foundation and the Secretary of Homeland Security to "enter into appropriate arrangements with the National Academy of

Sciences to conduct a comprehensive study of government, academic, and private-sector education, accreditation, training, and certification programs for the development of professionals in information infrastructure and cybersecurity." The agreement would be require "the National Academy of Sciences to consult with sector coordinating councils and relevant governmental agencies, regulatory entities, and nongovernmental organizations in the course of the study." The study would be required to include:
    - First, "an evaluation of the body of knowledge and various skills that specific categories of professionals in information infrastructure and cybersecurity should possess in order to secure information systems."
    - Second, "an assessment of whether existing government, academic, and private-sector education, accreditation, training, and certification programs provide the body of knowledge and various skills" required to secure information systems.
    - Third, "an evaluation of: (a) the state of cybersecurity education at institutions of higher education in the United States; (b) the extent of professional development opportunities for faculty in cybersecurity principles and practices; (c) the extent of the partnerships and collaborative cybersecurity curriculum development activities that leverage industry and government needs, resources, and tools; (d) the proposed metrics to assess progress toward improving cybersecurity education; and (e) the descriptions of the content of cybersecurity courses in undergraduate computer science curriculum."
    - Fourth, "an analysis of any barriers to the Federal Government recruiting and hiring cybersecurity talent, including barriers relating to compensation, the hiring process, job classification, and hiring flexibility."
    - Fifth, "an analysis of the sources and availability of cybersecurity talent, a comparison of the skills and expertise sought by the Federal Government the private sector, an examination of the current and future capacity of United States institutions of higher education, including community colleges, to provide current and future cybersecurity professionals, through education and training activities, with those skills sought by the Federal Government, State and local entities, and the private sector."
- In addition, Section 303 would require the National Academy of Sciences to submit to the President and Congress a report on the results of the study, not later than 1 year after the date of enactment of S. 1353. The report would be required to include:
    - First, "findings regarding the state of information infrastructure and cybersecurity education, accreditation, training, and certification programs, including specific areas of deficiency and demonstrable progress."
    - Second, "recommendations for further research and the improvement of information infrastructure and cybersecurity education, accreditation, training, and certification programs."

Public-Private Collaboration on Cybersecurity

<u>House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):</u>

- No similar language.

<u>SCSTC passed Cybersecurity Act of 2013 (S. 1353):</u>

- Section 101 would expand the authorized "implementation activities" of NIST to include a section related to cybersecurity standards, which would direct NIST to, "on an ongoing basis, facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure." Further, Section 101 would direct the Director of NIST, "in carrying out" this new section, to:

    - First, "coordinate closely and continuously with relevant private sector personnel and entities, critical infrastructure owners and operators, sector coordinating councils, information sharing and analysis centers, and other relevant industry organizations, and incorporate industry expertise."
    - Second, "consult with the heads of agencies with national security responsibilities, sector-specific agencies, State and local governments, the governments of other nations, and international organizations."
    - Third, "identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage risks."
    - Fourth, "include methodologies: to identify and mitigate impacts of the cybersecurity measures or controls on business confidentiality; and to protect individual privacy and civil liberties."
    - Fifth, "incorporate voluntary consensus standards and industry best practices."
    - Sixth, "align with voluntary international standards to the fullest extent possible."
    - Seventh, "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes."
    - Eighth, "include such other similar and consistent elements as the Director considers necessary."
- In addition, Section 101 would prohibit NIST from: "the use of specific solutions; "the use of specific information or communications technology products or services"; and "that information or communications technology products or services be designed, developed, or manufactured in a particular manner."
- Further, Section 101 would prohibit "information shared with or provided to NIST for the purposes" of facilitating and supporting the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure, the use of information "by any Federal, State, tribal, or local department or agency to regulate the activity of any entity."

International Cybersecurity Technical Standards

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 202 would direct the Director of National Institute of Standards and Technology (NIST), in coordination with appropriate Federal authorities, to:
    - First, "ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security."
    - Second, not later than 1 year after the date of enactment of H.R. 756, "develop and transmit to the Congress a plan for ensuring such Federal agency coordination."
    - Third, in coordinating with Federal agencies, the Director would be required to "ensure consultation with appropriate private sector stakeholders," as well.

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Mentioned above, Section 101 would require the Director of NIST, when facilitating and supporting the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure, to "consult with the heads of agencies with national security responsibilities, sector-specific agencies, State and local governments, the governments of other nations, and international organizations."

NIST Cybersecurity Research and Development

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 110 would expand the National Institute of Standards and Technology Act to include a section that would require NIST, as part of its research activities, "to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security" to:
    - First, "conduct a research program to develop a unifying and standardized identity, privilege, and access control management framework for the execution of a wide variety of resource protection policies and that is amenable to implementation within a wide variety of existing and emerging computer environments."
    - Second, "carry out research associated with improving the security of information systems and networks."
    - Third, "carry out research associated with improving the testing, measurement, usability, and assurance of information systems and networks."
    - Fourth, "carry out research associated with improving security of industrial control systems."
    - Fifth, "carry out research associated with improving the security and integrity of the information technology supply chain."

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- No similar language.

Cybersecurity University-Industry Task Force

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 108 would direct the Director of the Office of Science and Technology Policy, not later than 180 days after the date of enactment of H.R. 756, to "convene a task force to explore mechanisms for carrying out collaborative research, development, education, and training activities for cybersecurity through a consortium or other appropriate entity with participants from institutions of higher education and industry." The task force's functions would be to:
    - First, "develop options for a collaborative model and an organizational structure for such entity under which the joint research and development activities could be planned, managed, and conducted effectively, including mechanisms for the allocation of resources among the participants in such entity for support of such activity."
    - Second, "identify and prioritize at least three cybersecurity grand challenges, focused on nationally significant problems requiring collaborative and interdisciplinary solutions."
    - Third, "propose a process for developing a research and development agenda for such entity to address the grand challenges" that are identified.
    - Fourth, "define the roles and responsibilities for the participants from institutions of higher education and industry in such entity."
    - Fifth, "propose guidelines for assigning intellectual property rights and for the transfer of research and development results to the private sector."
    - Sixth, "make recommendations for how such entity could be funded from Federal, State, and nongovernmental sources."
- Further, in establishing the task force, the Director of OSTP would be required to "appoint an equal number of individuals from institutions of higher education, including minority-serving institutions and community colleges, and from industry with knowledge and expertise in cybersecurity." The Director of OSTP would be required to transmit the report "describing the findings and recommendations of the task force" to Congress, not later than 12 months after

the date of enactment of H.R. 756. Upon transmittal of the report, the task force would be terminated.

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- No similar language.

Cybersecurity Automation and Checklists for Government Systems

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 109 would require the Director of NIST to "develop, and revise as necessary, security automation standards, associated reference materials, and checklists providing settings and option selections that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government in order to enable standardized and interoperable technologies, architectures, and frameworks for continuous monitoring of information security within the Federal Government." The Director of NIST would be required to "establish priorities for the development of standards, reference materials, and checklists" on the basis of:
    - First, "the security risks associated with the use of the system."
    - Second, "the number of agencies that use a particular system or security tool."
    - Third, "the usefulness of the standards, reference materials, or checklists to Federal agencies that are users or potential users of the system."
    - Fourth, "the effectiveness of the associated standard, reference material, or checklist in creating or enabling continuous monitoring of information security."
    - Fifth, "such other factors as the Director of the National Institute of Standards and Technology determines to be appropriate."
- However, the Director of NIST would be allowed to exclude from the application of this activity "any information technology hardware or software system or security tool for which such Director determines that the development of a standard, reference material, or checklist is inappropriate because of the infrequency of use of the system, the obsolescence of the system, or the inutility or impracticability of developing a standard, reference material, or checklist for the system."
- In addition, the Director of NIST would be required to "ensure that Federal agencies are informed of the availability of any standard, reference material, checklists, or other item developed" under Section 109.
- Finally, the development of standards, reference materials, and checklist under Section 109 for an information technology hardware or software system or tool would not:
    - First, "require any Federal agency to select the specific settings or options recommended by the standard, reference material, or checklist for the system."
    - Second, "establish conditions or prerequisites for Federal agency procurement or deployment of any such system."
    - Third, "imply an endorsement of any such system by the Director of the National Institute of Standards and Technology."
    - Fourth, "preclude any Federal agency from procuring or deploying other information technology hardware or software systems for which no such standard, reference material, or checklist has been developed or identified" under Section 109.

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- No similar language.

Research on the Science of Cybersecurity

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 111 would direct the Director of NSF and the Director of NIST to, "through existing programs and activities, support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics."

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 201 would direct the heads of the Department of Agriculture, the Department of Commerce, the Department of Defense, the Department of Education, the Department of Energy, the Department of Health and Human Services, the Department of the Interior, the Environmental Protection Agency, the National Aeronautics and Space Administration, and the National Science Foundation to, through existing programs and activities, "support research that will lead to the development of a scientific foundation for the field of cybersecurity, including research that increases understanding of the underlying principles of securing complex networked systems, enables repeatable experimentation, and creates quantifiable security metrics."

Cloud Computing Strategy

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 203 would direct the Director of NIST, in collaboration with the Federal CIO Council, and in consultation with other relevant Federal agencies and stakeholders from the private sector, to "continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government." In carrying out the above mentioned strategy, the Director of NIST would be required to consider activities that:
    - First, "accelerate the development, in collaboration with the private sector, of standards that address interoperability and portability of cloud computing services."
    - Second, "advance the development of conformance testing performed by the private sector in support of cloud computing standardization."
    - Third, "support, in consultation with the private sector, the development of appropriate security frameworks and reference materials, and the identification of best practices, for use by Federal agencies to address security and privacy requirements to enable the use and adoption of cloud computer services, including activities: (a) to ensure the physical security of cloud computing data centers and the data stored in such centers; (b) to ensure access to the data stored in cloud computing data centers; (c) to develop security standards as required under section 20 of the National Institute of Standards and Technology Act; and (d) to support the development of the automation of continuous monitoring systems."

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 201 would require the Director of OSTP, in coordination with the head of any relevant Federal agency, to develop a Federal cybersecurity research and development plan to meet several objectives, including "how to protect information processed, transmitted, or stored using cloud computing or transmitted through wireless services."

Identity Management Research and Development

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 205 would direct the Director of NIST to "continue a program to support the development of technical standards, metrology, testbeds, and conformance criteria, taking into account appropriate user concerns, to":
  - First, "improve interoperability among identity management technologies."
  - Second, "strengthen authentication methods of identity management systems."
  - Third, "improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols."
  - Fourth, "improve the usability of identity management systems."

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- No similar language

National Science Foundation Cybersecurity R&D Programs

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- No similar language

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 201 would direct the Director of the NSF to support research that:
  - First, "develops, evaluates, disseminates, and integrates new cybersecurity practices and concepts into the core curriculum of computer science programs and of other programs where graduates of such programs have a substantial probability of developing software after graduation, including new practices and concepts relating to secure coding education and improvement programs."
  - Second, "develops new models for professional development of faculty in cybersecurity education, including secure coding development."

Cybersecurity Modeling and Test Beds

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- Section 205 would direct the Director of NIST to "continue a program to support the development of technical standards, metrology, test beds, and conformance criteria."

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 201 would direct the Director of NSF, in coordination with the Director of OSTP, not later than 1 year after the date of enactment of S. 1353, to "conduct a review of cybersecurity test beds in existence on the date of enactment" of S. 1353, "to inform the grants" outlined below. The review would be required to include "an assessment of whether a sufficient number of cybersecurity test beds are available to meet the research needs under the Federal cybersecurity research and development plan."
- Further, "if the Director of the National Science Foundation, after the review" outlined above, "determines that the research needs under the Federal cybersecurity research and development plan require the establishment of additional cybersecurity test beds, the Director of the National Science Foundation, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, may award grants to institutions of higher education or research and development non-profit institutions to establish cybersecurity test beds." The additional cybersecurity test beds would be required to "be sufficiently large in order to model the scale and complexity of real-time cyber attacks and defenses on real world networks and environments." In addition, the Director of NSF, in coordination with the Secretary of Commerce and the Secretary of Homeland Security, would be required to "evaluate the effectiveness of any

grants awarded" to establish new cybersecurity test beds "in meeting the objectives of the Federal cybersecurity research and development plan," not later than 2 years after the test beds capability review.

NSF Computer and Network Security Research Grant Areas

House passed Cybersecurity Enhancement Act of 2013 (H.R. 756):

- No similar language.

SCSTC passed Cybersecurity Act of 2013 (S. 1353):

- Section 201 would amend the Cyber Security Research and Development Act to add additional areas of research that the Director of NSF can award grants "for basic research on innovative approaches to the structure of computer and network hardware and software that are aimed at enhancing computer security." Those additional areas include:
    - First, "secure fundamental protocols that are integral to inter-network communications and data exchange."
    - Second, "secure software engineering and software assurance, including: (a) programming languages and systems that include fundamental security features; (b) portable or reusable code that remains secure when deployed in various environments; (c) verification and validation technologies to ensure that requirements and specifications have been implemented; and (d) models for comparison and metrics to assure that required standards have been met."
    - Third, "holistic system security that: (a) addresses the building of secure systems from trusted and untrusted components; (b) proactively reduces vulnerabilities; (c) addresses insider threats; and (d) supports privacy in conjunction with improved security."
    - Fourth, "monitoring and detection."
    - Fifth, "mitigation and rapid recovery methods."
    - Sixth, "security of wireless networks and mobile devices."
    - Seventh, "security of cloud infrastructure and services."

About the Space Foundation

The foremost advocate for all sectors of the space industry and an expert in all aspects of space, the Space Foundation is a global, nonprofit leader in space awareness activities, educational programs that bring space into the classroom and major industry events, including the *National Space Symposium*, all in support of its mission "to advance space-related endeavors to inspire, enable and propel humanity." The Space Foundation publishes *The Space Report: The Authoritative Guide to Global Space Activity* and provides three indexes that track daily U.S. stock market performance of the space industry. Through its Space Certification™ and Space Technology Hall of Fame® programs, the Space Foundation recognizes space-based technologies and innovations that have been adapted to improve life on Earth. The Space Foundation was founded in 1983 and is based in Colorado Springs, Colo. Its world headquarters features a public Visitors Center with two main areas - the El Pomar Space Gallery and the Northrop Grumman Science Center featuring Science On a Sphere®. The Space Foundation also conducts research and analysis and government affairs activities from its Washington, D.C., office and has a field office in Houston, Texas. For more information, visit www.SpaceFoundation.org. Follow us on Facebook, LinkedIn and Twitter, and read about the latest space news and Space Foundation activities in *Space Watch*.