Calendar No. 490

113TH CONGRESS *2d Session*	SENATE	REPORT 113–270

CYBERSECURITY ACT OF 2013

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 1353

NOVEMBER 12, 2014.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

49–010 WASHINGTON : 2014

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
MARK PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
MARK BEGICH, Alaska
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
ED MARKEY, Massachusetts
CORY BOOKER, New Jersey
JOHN WALSH, Montana

JOHN THUNE, South Dakota
ROGER F. WICKER, Mississippi
ROY BLUNT, Missouri
MARCO RUBIO, Florida
KELLY AYOTTE, New Hampshire
DEAN HELLER, Nevada
DAN COATS, Indiana
TIM SCOTT, South Carolina
TED CRUZ, Texas
DEB FISCHER, Nebraska
RON JOHNSON, Wisconsin

ELLEN DONESKI, *Staff Director*
JOHN WILLIAMS, *General Counsel*
DAVID SCHWIETERT, *Republican Staff Director*
NICK ROSSI, *Republican Deputy Staff Director*
REBECCA SEIDEL, *Republican General Counsel*

Calendar No. 490

113TH CONGRESS *2d Session* | SENATE | REPORT 113–270

CYBERSECURITY ACT OF 2013

NOVEMBER 12, 2014.—Ordered to be printed

Mr. ROCKEFELLER, from the Committee on Commerce, Science, and Transportation, submitted the following

R E P O R T

[To accompany S. 135]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 1353) to provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The purpose of S. 1353 is to help secure the Nation from cyber threats by clarifying the statutory authority of the National Institute of Standards and Technology (NIST) to facilitate and support the development of a set of voluntary, industry-led standards and best practices to reduce cyber risks to critical infrastructure. The bill would also ensure that the Federal Government supports cutting-edge research, increases public awareness, and improves our workforce to better address cyber threats.

BACKGROUND AND NEEDS

I. THE NATURE AND SCOPE OF THE CYBER THREAT

Over the past two decades, the growth of the Internet and our country's increasing use of interconnected networks have produced unprecedented economic growth and innovation. However, our ever-increasing reliance upon the Internet has also allowed new threats to develop. As individuals, businesses, and governments

shift more of their activities and store more of their information online, they become vulnerable to attackers intent on conducting malicious surveillance, stealing information, or disrupting operations. These attackers range from amateur hackers, to criminals, to state sponsors. The type of attack could be untargeted malware, denial of service, or an advanced persistent threat.[1]

Top government officials and cybersecurity experts have repeatedly warned about the seriousness of the threat cyber incidents pose to our economic and national security. In January 2012 testimony on worldwide threats before the Senate Select Intelligence Committee, Robert Mueller, then-Director of the Federal Bureau of Investigation, said that cyber threats will surpass the threat of terrorism in the foreseeable future.[2] Former National Security Agency Director General Keith Alexander described the consequences of cyber espionage as the "greatest transfer of wealth in history."[3] Former Director of the National Counterterrorism Center Michael Leiter has described cyber attacks against the United States as "a Pearl Harbor of slow moving deadly gas rather than blowing things up. We are being robbed blind."[4] With respect to economic security, a July 2013 joint Center for Strategic and International Studies-McAfee report estimates as much as a $100 billion annual loss to the U.S. economy with as many as 508,000 U.S. jobs lost or displaced due to malicious cyber activity.[5]

A growing cyber threat affects both the Federal Government and the U.S. economy. According to Department of Homeland Security (DHS) data, the number of cyber incidents reported by Federal agencies to the United States Computer Emergency Readiness Team increased 782 percent between 2006 and 2012, with 48,562 incidents reported in 2012.[6] Symantec estimates that targeted cyber attacks focused on individuals or specific companies increased 42 percent in 2012 compared with the preceding 12 months. Within that increase, targeted attacks specifically aimed at small businesses increased from 18 percent in the same period.[7] Verizon analysis of 2012 data breaches shows that 95 percent of targeted state-affiliated espionage incidents rely on the relatively simple technique of e-mail phishing, and, once attackers have gained access, 66 percent of breaches go undiscovered for months or even years.[8]

National and homeland security officials are especially concerned about cyber attacks targeted at the industrial control systems (ICS)

---

[1] *See e.g.*, Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, February 18, 2013, at http://intelreport.mandiant.com.

[2] Testimony of Robert Mueller, Senate Select Intelligence Committee, *Current and Projected National Security Threats to the United States*, January 31, 2012, at http://www.gpo.gov/fdsys/pkg/CHRG-112shrg74790/pdf/CHRG-112shrg74790.pdf.

[3] Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history'," *Foreign Policy*, July 9, 2012, at http://thecable.foreignpolicy.com/posts/2012/07/09/nsachief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

[4] Erin Mershon, "Deal Possible on Cybersecurity if Senate Can Pass Similar Bill, Rogers Says," *Communications Daily*, September 26, 2013.

[5] James Andrew Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Espionage*, Center for Strategic and International Studies, McAfee, July 23, 2013, at http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

[6] U.S. Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187, February 2013, at http://www.gao.gov/assets/660/652170.pdf.

[7] Symantec, *Internet Security Threat Report*, 2013, at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main—report_v18_2012_21291018.en-us.pdf.

[8] Verizon, *2013 Data Breach Investigations Report*, 2013, at http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

that operate and monitor large physical systems in the United States. The ICS managing some of our country's most critical infrastructure, including the electric grid, oil pipelines, transportation networks, and financial institutions, are now accessible via the Internet and, as a result, could potentially be manipulated or attacked by malicious actors using computers in other parts of the world. The vulnerabilities of our country's critical infrastructure create a potentially serious threat to the American public.[9] Ninety percent of this infrastructure is owned and operated by private entities.[10, 11]

With access to an infrastructure operator's network, attackers could change control parameters to disable or destroy the infrastructure. U.S. infrastructure, as a "system of systems," is potentially vulnerable to cascading damages, such as if an electricity blackout leads to disruptions in water treatment, emergency communications, and oil and gas production. In an op-ed published in the *Wall Street Journal* in 2012, President Obama described such a scenario:

> It doesn't take much to imagine the consequences of a successful cyber attack. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill.[12]

News reports of cyber attacks on critical infrastructure, government systems, and businesses show that destructive attacks are not merely theoretical "red-team" scenarios. In Saudi Arabia, for example, 2012 media reports indicated that a cyber attack on Saudi Aramco, the world's largest exporter of oil, strategically erased data from 30,000 computers on the company's network.[13] More recently, the press has reported sustained attacks on U.S. financial services companies,[14] universities,[15] and energy companies[16] designed to

---

[9] *See e.g.*, Presidential Directive/NSC-63 (May 22, 1998) ("Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.")

[10] National Infrastructure Advisory Council, *Critical Infrastructure Partnership Strategic Assessment*, October 14, 2008, at http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf, p. 16.

[11] Industrial Control Systems Cyber Emergency Response Team, *Control System Internet Accessibility*, ICS-ALERT-10-301-01, October 28, 2010, at https://ics-cert.us-cert.gov/alerts/ICS-Alert-11-343-01A.

[12] Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal*, July 19, 2012.

[13] Wael Mahdi, "Saudi Arabia Says Aramco Cyberattack Came From Foreign States," *Bloomberg*, December 9, 2012, at http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html.

[14] Joseph Menn, "Cyber attacks against banks more severe than most realize," *Reuters*, May 18, 2013, at http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518.

[15] Richard Pérez-Peña, "Universities Face a Rising Barrage of Cyberattacks," *The New York Times*, July 16, 2013, at http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all.

[16] David E. Sanger and Nicole Perlroth, "Cyberattacks Against U.S. Corporations Are on the Rise," *The New York Times*, May 12, 2013, at http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all.

take down websites, steal intellectual property, and destroy data or manipulate infrastructure, respectively. The press itself has also come under attack, including *The New York Times*, which was knocked offline for several hours in August 2013 by the so-called Syrian Electronic Army.[17]

In response to the industry-wide and ever-changing cyber threat, title I of the Cybersecurity Act of 2013 would promote the development of a set of voluntary standards and best practices that critical infrastructure operators in the United States can adopt to improve the security of their systems and lower the risk of a cyber attack that causes serious damage to the United States. Title I would clarify the authority of NIST, the Federal Government's leading technical standards and measurement agency, to support an industry-led effort to develop these voluntary standards and best practices, and ensure this process will be ongoing to provide flexibility to meet evolving threats.

II. CYBERSECURITY RESEARCH AND DEVELOPMENT AND WORKFORCE NEEDS

While warning about the vulnerabilities of our information networks to cyber attacks, policymakers have also expressed concerns that the United States is under-investing in cybersecurity research and not training a sufficient amount of workers capable of defending government agencies and private sector businesses from cyber attacks.

In December 2011, the White House Office of Science and Technology Policy (OSTP) released "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program." The plan sought to strengthen the often piecemeal cybersecurity research and development conducted by Federal agencies under the auspices of the Networking and Information Technology Research and Development (NITRD) Program. Four strategic goals have been set to guide research and development progress: inducing change, developing scientific foundations, maximizing research impact, and accelerating transition to practice.[18]

According to several reports, the Federal and private sector cybersecurity workforce is facing increasing demand and potential shortages. A 2013 study found that, over the past 5 years, demand for cybersecurity professionals grew 3.5 times faster than general information technology jobs and 12 times faster than for all other jobs.[19] A 2012 assessment by the National Initiative for Cybersecurity Education (NICE) in partnership with the Federal Chief Information Officers Council found that nearly 80 percent of Federal cybersecurity workers surveyed were over the age of 40, with the majority nearing retirement age.[20] In 2013, the news reported that

---

[17] Lee Ferran, "Who's The Syrian Group Allegedly Behind The New York Times Cyber Attack?," *ABC News*, August 28, 2013, at http://abcnews.go.com/Blotter/syrian-electronic-army-group-allegedly-york-times-cyber/story?id=20095458.

[18] Executive Office of the President, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,* National Science and Technology Council, December 2011, at http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

[19] Burning Glass Technologies, *Initial Findings on Cyber Security Jobs*, February 2013, at http://www.burning-glass.com/cybersecurity/BGTCyberSecurityReport.pdf.

[20] National Initiative for Cybersecurity Education, *2012 Information Technology Workforce Assessment for Cybersecurity*, March 14, 2013, at https://cio.gov/wp-content/uploads/downloads/2013/04/ITWAC-Summary-Report_04-01-2013.pdf.

the Department of Defense has an intent to expand Cyber Command,[21] yet security clearance and citizenship requirements, let alone education requirements, will make hiring those additional employees challenging. The National Science Foundation's (NSF) Scholarship for Service Program, which serves as a Federal Government pipeline for cybersecurity talent, currently graduates and places an average of just 150 students per year in Federal agencies.[22] Cynthia Dion-Schwarz, former Deputy Assistant Director of the NSF's Computer & Information Science & Engineering Directorate, commented, "The outlook is grim because we are not producing, from an education perspective, the people with the right skills sets to just have the entry-level skills needed in order to make progress in cybersecurity."[23]

Titles II through IV of the Cybersecurity Act of 2013 seek to address these challenges. Title II would task OSTP with coordinating Federal agencies' cybersecurity research and development and would support basic cybersecurity research at NSF, in collaboration with academia and industry. Title III of the bill would authorize cybersecurity education and workforce development initiatives, including competitions and challenges, the scholarship-for-service program, and a study examining the education, training, and certification needs of the cybersecurity workforce. Title IV of the bill would authorize and expand the work of the NIST-coordinated NICE.

SUMMARY OF PROVISIONS

The purpose of S. 1353 is to help improve the security of the Nation from cyber threats by clarifying NIST's statutory authority to facilitate and support the development of a set of voluntary, industry-led standards and best practices to reduce cyber risks to critical infrastructure. The bill would also ensure that the Federal Government supports cutting-edge research, increases public awareness, and improves our workforce to better address cyber threats.

Title I of the bill would update the existing statutory authority of NIST to ensure that the agency will, on an ongoing basis, facilitate and support the development of a voluntary, industry-led set of standards and best practices to reduce cyber risks to critical infrastructure. It also would ensure that the information shared in this process may not be used for regulatory purposes. The set of standards and best practices that would be developed through this process must—

- be voluntary;
- be developed in close and continuous coordination with industry;
- not conflict with or duplicate existing regulatory requirements;

---

[21] Elisabeth Bumiller, "Pentagon Expanding Cybersecurity Force to Protect Network Against Attacks," *The New York Times*, January 27, 2013, at http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html. *See also*, Cheryl Pellerin, "Rogers: Cybercom Defending Networks, Nation," *DoD News, Defense Media Activity*, August 18, 2014, at http://www.defense.gov/news/newsarticle.aspx?id=122949.

[22] Briefing by Victor P. Piotrowski, Lead Program Director, NSF, to Senate Commerce, Science, and Transportation Staff, July 29, 2013.

[23] Amber Corrin, "Desperately seeking cybersecurity pros," *FCW*, October 26, 2012, at http://fcw.com/articles/2012/10/26/cyber-workforce.aspx.

- incorporate voluntary consensus standards and industry best practices and align with voluntary international standards; and
- be technology neutral.

This section also would call on the Comptroller General of the United States to assess the progress, voluntary nature, and adoption of the standards and best practices to reduce cyber risks to critical infrastructure.

Because of its technical expertise and its well-earned reputation as an "honest broker" in the standards development process, NIST is particularly well positioned to coordinate the development of these cybersecurity standards and practices. NIST's role in the development of standards is not that of a regulator, but of a convener and facilitator. NIST brings together knowledgeable players from government and industry and supports their efforts to build consensus around common standards. Industries adopt NIST standards because the standards that emerge from the NIST process consistently have high technical quality and utility. There are many well-documented cases where NIST standards have improved the quality of goods and services produced by U.S. companies while lowering transaction costs and promoting innovation.[24] In addition to the important role it plays in developing standards in the United States, NIST also actively works to harmonize U.S.-based standards with international standards.[25]

Title II of the bill would call for a Federal cybersecurity research and development plan to be developed by OSTP and the coordination of research and development activities at NSF, NIST, other Federal agencies, academia, and the private sector. The bill also would authorize coordinated research to address gaps in knowledge preventing the development of secure technologies. In addition, agencies participating in the NITRD Program would be tasked with supporting research on the science of cybersecurity.

Title III of the bill would call for a National Academy of Sciences study of the current state of higher level cybersecurity education and professional certification; would enable support of innovative competitions and challenges under America COMPETES Act authority to identify, develop, and recruit talented professionals and to stimulate innovation in cybersecurity research and development; and would authorize an existing NSF-led cyber scholarship-for-service program.

Title IV of the bill would call on NIST to continue to coordinate, in conjunction with other Federal agencies, a cybersecurity public awareness campaign, initiatives to support formal cybersecurity education, and an ongoing evaluation and forecast of the workforce needs of the Federal Government. Title IV also would require NIST to develop, implement, and transmit to Congress a strategic plan in support of this program.

---

[24] *See e.g.*, Erik Puskar, *Selected Impacts of Documentary Standards Supported by NIST, 2008 Edition*, NISTIR 7548, January 2009; David Leach and John T. Scott, *The Economic Impacts of Documentary Standards: A Case Study of the Flat Panel Display Measurement Standard (FPDM)*, CGR G2012-0299, December 2011.

[25] Maureen A. Breitenberg, *The ABCs of Standards Activities*, NISTIR 7614, August 2009.

LEGISLATIVE HISTORY

Since Senator Rockefeller became Chairman in early 2009, the Commerce Committee has devoted significant attention to the cybersecurity challenges facing the country. Chairman Rockefeller convened a Committee hearing on March 19, 2009, entitled, "Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response." On April 1, 2009, Chairman Rockefeller and Senator Snowe introduced S. 773, the Cybersecurity Act of 2009. S. 773 would have authorized the President and certain Federal agencies to take steps to protect government information systems and critical infrastructure from cyber attacks. It also would have ordered NIST to develop cybersecurity standards within one year and promoted cybersecurity research, training, and awareness.

After a second hearing, entitled "Cybersecurity: Next Steps to Protect Our Critical Infrastructure," on February 23, 2010, the Committee favorably reported an amended version of S. 773 on March 24, 2010, by voice vote. Although S. 773 was never considered on the Senate floor, portions of the legislation were included in a bipartisan cybersecurity bill, S. 3414, that the Senate considered during the 112th Congress.

In addition to legislation, in the 112th Congress, the Committee continued to actively gather information about the cybersecurity threats to our national and economic security. As part of this effort, on September 19, 2012, Chairman Rockefeller wrote letters to the chief executive officers of the 500 largest companies in the United States requesting information about the companies' cybersecurity practices and their view of how the public and private sectors should be working together to best address cybersecurity risks. More than 300 companies responded to this letter. In a January 28, 2013, memorandum to Chairman Rockefeller summarizing the responses of these companies, Committee staff reported that the companies generally supported strengthening the public-private partnership to address our country's cybersecurity vulnerabilities, but were concerned about legislation that might result in an inflexible, "one-size-fits-all" set of practices that could potentially conflict with existing sector-specific Federal regulations or slow down companies' responses to cyber attacks.[26]

The Committee's cybersecurity work continued in the 113th Congress. After President Obama issued an Executive Order entitled, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013 (Exec. Order No. 13636), the Committee held a joint hearing with the Committee on Homeland Security and Governmental Affairs on March 7, 2013, entitled, "The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security." This hearing examined the development and implementation of the February 12 Executive Order and discussed ways government and industry can work together to protect critical infrastructure from cyber attacks.

Chairman Rockefeller and Ranking Member Thune introduced S. 1353, the Cybersecurity Act of 2013, on July 24, 2013, and on July 25, 2013, the Committee held a hearing entitled, "The Partnership

[26] Memorandum from Democratic Staff to Chairman Rockefeller of the Senate Commerce, Science and Transportation Committee, January 28, 2013, at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=5a85f211-a5c9-4306-9c84-d3a6b88024f6.

Between NIST and the Private Sector: Improving Cybersecurity." This hearing focused on the role NIST was playing in developing the Cybersecurity Framework, called for in the Executive Order, to reduce cyber risks to critical infrastructure. The hearing also examined the broader role NIST plays in developing information security standards and the clarifications of NIST's authority proposed in S. 1353.

On July 30, 2013, the Committee met in open Executive Session and, by voice vote, ordered the bill to be reported favorably with an amendment in the nature of a substitute. Several amendments—one from Senator Klobuchar, one jointly from Senator Klobuchar and Senator Blunt, one from Senator Warner, one from Senator Heinrich, and one from Senator Schatz—were agreed to as part of the substitute amendment.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

S. 1353—Cybersecurity Act of 2013

Summary: S. 1353 would direct several agencies within the federal government to take certain actions to facilitate public-private cooperation on cybersecurity standards, improve research and development in cybersecurity technologies, and further education and public awareness on cybersecurity matters. Several of the bill's requirements pertain to existing or planned programs and initiatives, while others create new requirements or expand the scope of existing efforts.

CBO estimates that implementing S. 1353 would cost $56 million over the 2014–2018 period, assuming appropriation of the necessary amounts. Pay-as-you-go procedures do not apply to this legislation because it would not affect direct spending or revenues.

S. 1353 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of S. 1353 is shown in the following table. The costs of this legislation fall within budget functions 250 (general science, space, and technology) and 370 (commerce and housing credit).

	By fiscal year, in millions of dollars 2014—					
	2014	2015	2016	2017	2018	2014–2018
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Cybersecurity Standards and Public-Private Collaboration:						
Estimated Authorization Level	*	1	*	*	1	2
Estimated Outlays	*	1	*	*	1	2
Cybersecurity Research and Development:						
Estimated Authorization Level	*	14	13	14	13	55
Estimated Outlays	*	2	8	12	12	35
Cybersecurity Education, Training, and Public Awareness:						
Estimated Authorization Level	4	4	4	4	4	20
Estimated Outlays	3	4	4	4	4	19
Total Changes:						
Estimated Authorization Level	5	19	17	18	18	77

	By fiscal year, in millions of dollars 2014—					
	2014	2015	2016	2017	2018	2014–2018
Estimated Outlays	4	7	12	16	17	56

Note: Components may not sum to totals because of rounding. * = less than $500,000.

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted early in 2014, the necessary amounts will be appropriated each year, and spending will follow historical patterns for similar activities.

Cybersecurity standards and public-private collaboration

Title I would codify certain elements of Executive Order 13636 by directing the National Institute of Standards and Technology (NIST) to develop a framework of voluntary standards designed to reduce risks arising from cyberattacks on critical infrastructure that is privately owned and operated. The agency expects to spend about $6 million to develop the standards (the preliminary framework was completed in October 2013) and anticipates spending a similar amount annually to review and update the framework as required by the executive order. Based on information from the agency, CBO estimates that codifying the requirements of the executive order would not significantly increase the agency's costs.

Title I also would require the Government Accountability Office (GAO) to assess progress made by NIST in developing the framework and the private sector in adopting the standards; GAO also would be required to prepare a summary of its findings and report to the Congress every two years. CBO estimates that implementing this provision would cost $2 million over the 2014–2018 period, assuming the availability of appropriated funds.

Cybersecurity research and development

Title II would require the Director of the National Science Foundation (NSF) to review existing infrastructure used to test cybersecurity technologies within one year of the bill's enactment. Based on the results of the review, the NSF would be authorized to award grants to establish additional infrastructure to test cybersecurity technologies. Based on information provided by the agency, CBO estimates that implementing this provision would cost $33 million over the 2014–2018 period, assuming the appropriation of the necessary amounts.

Title II also would require the Director of the Office of Science and Technology Policy (OSTP) to develop a federal cybersecurity research and development plan in consultation with nonfederal entities. Under the legislation, the director would be required to update the plan and report to the Congress every three years. Based on information provided by OSTP, CBO estimates that implementing this provision would cost about $2 million over the next five years.

Cybersecurity education, training, and public awareness

Title III would require the Director of the NSF to contract with the National Academy of Sciences (NAS) to conduct a study of education, training, and certification programs for the development of professionals in the areas of information infrastructure and cybersecurity. Based on information from the NAS, CBO estimates that

implementing this provision of title III would cost $1 million over the 2014–2018 period, assuming appropriation of the necessary amounts.

Other provisions of title III would require the Director of the NSF to continue a scholarship-for-service program to train professionals to meet the cybersecurity needs of federal, state, local, and tribal governments. This title also would require several agencies, including the Department of Commerce, NSF, and the Department of Homeland Security, to support competitions to identify and recruit individuals to enhance innovation in basic and applied cybersecurity that can be used to advance the mission of the agency. Based on information from those agencies, CBO estimates that implementing those provisions would not significantly increase discretionary spending over the 2014–2018 period because those activities are already occurring under current law.

Title IV would require NIST to continue to coordinate a national campaign to increase public awareness of cybersecurity threats. The agency also would be required to develop and implement a strategic plan to guide federal agencies' support of the campaign. Based on information from NIST, CBO expects that implementing those requirements would cost $18 million over the 2014–2018 period, assuming appropriation of the necessary amounts, for personnel and administrative costs.

Pay-As-You-Go Considerations: None.

Intergovernmental and private-sector impact: S. 1353 contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments.

Estimate prepared by: Federal costs: Susan Willie and Martin von Gnechten; Impact on state, local, and tribal governments: J'nell L. Blanco; Impact on the private sector: Marin Burnett.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

The bill would require 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. The bill would also authorize existing research and development activities, support cybersecurity workforce training and education, and support efforts to raise public awareness of the cyber threat. The bill would not subject any individuals or businesses affected by the bill to any additional regulations, as the product of NIST's and industry's work is voluntary.

ECONOMIC IMPACT

The bill would not authorize new funding. It is anticipated that research conducted under the authority of title II and section 301 of the bill may lead to new technologies and solutions to evolving

cyber threats. Section 302 would have a positive impact on the availability of qualified cybersecurity professionals to the Federal Government. Section 401 could also have a positive impact over time by reducing the number of individual victims of malicious cyber activities and associated costs.

PRIVACY

The bill would not have any adverse impact on the personal privacy of individuals.

PAPERWORK

The bill would not increase paperwork requirements for private individuals or businesses. The bill would require three reports from the Federal Government and one study to be carried out by the National Academy of Sciences on behalf of the Federal Government.

The first report would be from the Comptroller General of the United States assessing the progress, voluntary nature, and adoption of the standards and best practices to reduce cyber risks to critical infrastructure. This report would be delivered to the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Energy and Commerce of the House of Representatives, and the Committee on Science, Space, and Technology of the House of Representatives one year after enactment and every two years thereafter for six years.

The second report would be a Federal cybersecurity research and development plan from the Director of OSTP. This plan would be delivered to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives within one year of enactment and every three years thereafter.

The third report would be a strategic plan for the national cybersecurity awareness and preparedness campaign from the Director of NIST. This plan would be delivered to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives within one year of enactment and every five years thereafter.

The National Academy of Sciences study, supported by the Director of NSF, the Director of the Office of Personnel Management (OPM), and the Secretary of Homeland Security, would be 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. This study would be due to the President and Congress within one year of enactment, though it is possible more time may be required for the final draft.

The bill also would require the Director of NSF, in coordination with the Director of OSTP, to conduct a review of cybersecurity test beds in existence on the date of enactment. This review would trigger the awarding of additional grants for test beds if needed to support the research and testing needs of the Federal cybersecurity research and development plan. The Committee envisions further assessments of effectiveness of these grants to be included in annual budget justifications after the initial two years given to allow any new test beds to begin operation.

CONGRESSIONALLY DIRECTED SPENDING

In compliance with paragraph 4(b) of rule XLIV of the Standing Rules of the Senate, the Committee provides that no provisions contained in the bill, as reported, meet the definition of congressionally directed spending items under the rule.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title; table of contents.

This section would provide that the legislation may be cited as the Cybersecurity Act of 2013. This section would also provide the table of contents for the legislation.

Section 2. Definitions.

This section would define three key terms.

Section 3. No regulatory authority.

This section would clarify that no regulatory authority is conferred on any Federal, State, tribal, or local department or agency by the bill.

TITLE I—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

Sec. 101. Public-private collaboration on cybersecurity.

This section would update the existing statutory authority of NIST to ensure that NIST would, consistent with existing authority, on an ongoing basis, facilitate and support the development of a voluntary, non-regulatory, industry-led set of standards and best practices to reduce cyber risks to critical infrastructure. The set of standards and best practices that would be developed through this process: must be voluntary; must be developed in close and continuous coordination with industry; must not conflict with or duplicate existing regulatory requirements; must incorporate voluntary consensus standards and industry best practices and align with voluntary international standards; and must be technology neutral.

The Committee recognizes that several industries are subject to regulatory requirements, standards, and processes pertaining to security: therefore, this process must not duplicate regulatory processes and not conflict with or supercede requirements, mandatory standards, and related process. This limitation, however is not intended to prevent NIST from recognizing existing standards or best practices, or to impose an obligation upon NIST to resolve possible inconsistencies among existing standards and best practices that may be utilized by different entities. The aim of this legislation is not to create a single, one-size-fits-all standard or set of standards; rather, it is to identify on an ongoing basis industry-led standards and best practices that may mitigate dynamic cyber threats and vulnerabilities. Further, information shared with NIST in this process or for purposes of this process may not be used to regulate the activity of any entity.

This section would also require a study and report from the Comptroller General assessing the progress made by NIST in facilitating the standards and best practices to reduce cyber risks to critical infrastructure, the extent to which such standards are voluntary and their development led by industry representatives, and

the extent to which critical infrastructure sectors have adopted the voluntary standards and best practices, among other considerations. The report would be due to the relevant congressional committees one year after enactment and every two years thereafter for six years.

TITLE II—CYBERSECURITY RESEARCH AND DEVELOPMENT

Sec. 201. Federal cybersecurity research and development.

This section would call on the Director of OSTP, in coordination with relevant Federal agencies, to develop a Federal cybersecurity research and development plan to identify and prioritize research needed to meet several key objectives, while recognizing that the Director of OSTP has flexibility in determining additional objectives. The Director of OSTP may coordinate with relevant stakeholders, including industry, academia, and appropriate national laboratories to determine additional objectives. This section would ensure Federal research as part of this plan is not duplicative of private sector efforts. The plan would be updated triennially. This section would also require the Director of NSF to support research to inform computer science programs and professional development, and would add several research areas to NSF's authority to address gaps in knowledge preventing the development of secure technologies. This section would also call on the Director of NSF to evaluate the need for additional cybersecurity test beds and would authorize the Director of NSF, the Secretary of Commerce, and the Secretary of Homeland Security to support further development of test beds if necessary to meet the needs of the national cybersecurity research and development plan. This section would also require the Director of OSTP to coordinate cybersecurity research and development activities across the Federal Government. Agencies would also support research on the science of cybersecurity.

Sec. 202. Computer and network security research centers.

This section would amend existing NSF authority to establish computer and network security research centers, especially criteria related to selection of new centers which would conduct research specific to improving security and resiliency of information infrastructure, reducing cyber vulnerabilities, and anticipating and mitigating consequences of cyber attacks on critical infrastructure. New criteria would also include the ability of research centers to transition new technologies into the private sector or Federal Government, among others. Research areas that centers may pursue would be enhanced in section 201 of the bill.

TITLE III—EDUCATION AND WORKFORCE DEVELOPMENT

Sec. 301. Cybersecurity competitions and challenges.

This section would call on the Secretary of Commerce, Director of NSF, and Secretary of Homeland Security, in consultation with the Director of OPM, to support competitions and challenges to identify, develop, and recruit talented individuals who could secure government and private sector information infrastructure, as well as to stimulate innovation in basic and applied cybersecurity research. This authority would be derived from section 105 of the America COMPETES Reauthorization Act of 2010 (P.L. 111–358;

124 Stat. 3989), which adds section 24 of the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3719). The participating agencies would seek the participation of high school, university, and graduate students, veterans, and other relevant organizations and individuals. This section would call on competitions and challenges to focus on certain skill gaps and would encourage cooperation with existing regional, State, school, and private sector initiatives.

Sec. 302. Federal cyber scholarship-for-service program.

This section would authorize an existing NSF initiative, in coordination with the Director of OPM and Secretary of Homeland Security, to recruit, educate, and develop the next generation of Federal cybersecurity professionals. NSF would support scholarships for students enrolled at institutions of higher education studying for degrees or specialized program certifications in the cybersecurity field, under which a recipient would 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. This section would define agency hiring authority and eligibility for the scholarship, and provide for repayment of the scholarship should a recipient fail to meet the terms of the program as established by the Director of NSF. NSF would evaluate and report periodically to Congress on the success of recruiting and retaining scholarship recipients in the public sector workforce. The Committee believes additional incentives within existing authority, such as loan repayment programs, should be considered by Federal agencies to attract and retain a talented workforce. The Committee will continue to examine the effectiveness of such incentives.

Sec. 303. Study and analysis of education, accreditation, training, and certification of information infrastructure and cybersecurity professionals.

This section would call on the Director of NSF, the Director of OPM, and the Secretary of Homeland Security to jointly contract with the National Academy of Sciences for 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 study would include an evaluation of the knowledge needed for professionals to secure information systems; an assessment of whether existing education, accreditation, training, and certification programs provide the necessary body of knowledge; an evaluation of the state of cybersecurity education at U.S. institutions of higher education; an analysis of barriers to the Federal Government in recruiting and hiring cybersecurity talent; and an analysis of the capacity of U.S. institutions of higher education to provide current and future cybersecurity professionals to meet the needs of the Federal Government, State and local entities, and private sector. The study would be due to the President and Congress within one year of enactment. The Committee recognizes that the National Academy of Sciences released a report in September 2013 entitled "Professionalizing the Nation's Cybersecurity Workforce" and believes that the study in this section should not duplicate existing or prior work in this area.

TITLE IV—CYBERSECURITY AWARENESS AND PREPAREDNESS

Sec. 401. National cybersecurity awareness and preparedness campaign.

This section would call on the Director of NIST, in consultation with relevant Federal agencies, to continue coordination of a national cybersecurity awareness and preparedness campaign. This initiative would include a public awareness media campaign; a campaign to increase the understanding of State and local government and institutions of higher education of effective risk management; support for formal cybersecurity education programs; and initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal Government, among others. This section would call for a strategic plan to guide the awareness and preparedness campaign.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

[15 U.S.C. 271 et seq.]

SEC. 2. ESTABLISHMENT, FUNCTIONS, AND ACTIVITIES.

[15 U.S.C. 272]

* * * * * * *

(c) IMPLEMENTATION ACTIVITIES.—In carrying out the functions specified in subsection (b), the Secretary, acting through the Director may, among other things—

(1) construct physical standards;

(2) test, calibrate, and certify standards and standard measuring apparatus;

(3) study and improve instruments, measurement methods, and industrial process control and quality assurance techniques;

(4) cooperate with the States in securing uniformity in weights and measures laws and methods of inspection;

(5) cooperate with foreign scientific and technical institutions to understand technological developments in other countries better;

(6) prepare, certify, and sell standard reference materials for use in ensuring the accuracy of chemical analyses and measurements of physical and other properties of materials;

(7) in furtherance of the purposes of this Act, accept research associates, cash donations, and donated equipment from industry, and also engage with industry in research to develop new basic and generic technologies for traditional and new products and for improved production and manufacturing;

(8) study and develop fundamental scientific understanding and improved measurement, analysis, synthesis, processing, and fabrication methods for chemical substances and compounds, ferrous and nonferrous metals, and all traditional and advanced materials, including processes of degradation;

(9) investigate ionizing and nonionizing radiation and radioactive substances, their uses, and ways to protect people structures, and equipment from their harmful effects;

(10) determine the atomic and molecular structure of matter, through analysis of spectra and other methods, to provide a basis for predicting chemical and physical structures and reactions and for designing new materials and chemical substances, including biologically active macromolecules;

(11) perform research on electromagnetic waves, including optical waves, and on properties and performance of electrical, electronic, and electromagnetic devices and systems and their essential materials, develop and maintain related standards, and disseminate standard signals through broadcast and other means;

(12) develop and test standard interfaces, communication protocols, and data structures for computer and related telecommunications systems;

(13) study computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes;

(14) perform research to develop standards and test methods to advance the effective use of computers and related systems and to protect the information stored, processed, and transmitted by such systems and to provide advice in support of policies affecting Federal computer and related telecommunications systems;

(15) 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 (as defined under subsection (e));

[(15)**]** *(16)* determine properties of building materials and structural elements, and encourage their standardization and most effective use, including investigation of fire-resisting properties of building materials and conditions under which they may be most efficiently used, and the standardization of types of appliances for fire prevention;

[(16)**]** *(17)* undertake such research in engineering, pure and applied mathematics, statistics, computer science, materials science, and the physical sciences as may be necessary to carry out and support the functions specified in this section;

[(17)**]** *(18)* compile, evaluate, publish, and otherwise disseminate general, specific and technical data resulting from the performance of the functions specified in this section or from other sources when such data are important to science, engineering, or industry, or to the general public, and are not available elsewhere;

[(18)**]** *(19)* collect, create, analyze, and maintain specimens of scientific value;

[(19)**]** *(20)* operate national user facilities;

[(20)] *(21)* evaluate promising inventions and other novel technical concepts submitted by inventors and small companies and work with other Federal agencies, States, and localities to provide appropriate technical assistance and support for those inventions which are found in the evaluation process to have commercial promise;

[(21)] *(22)* demonstrate the results of the Institute's activities by exhibits or other methods of technology transfer, including the use of scientific or technical personnel of the Institute for part-time or intermittent teaching and training activities at educational institutions of higher learning as part of and incidental to their official duties; and

[(22)] *(23)* undertake such other activities similar to those specified in this subsection as the Director determines appropriate.

(d) MANAGEMENT COSTS.—In carrying out the extramural funding programs of the Institute, including the programs established under sections 25, 26, and 28 of this Act, the Secretary may retain reasonable amounts of any funds appropriated pursuant to authorizations for these programs in order to pay for the Institute's management of these programs.

(e) CYBER RISKS.—

(1) IN GENERAL.—In carrying out the activities under subsection (c)(15), the Director—

(A) shall—

(i) 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;

(ii) 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;

(iii) 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 cyber risks;

(iv) include methodologies—

(I) to identify and mitigate impacts of the cybersecurity measures or controls on business confidentiality; and

(II) to protect individual privacy and civil liberties;

(v) incorporate voluntary consensus standards and industry best practices;

(vi) align with voluntary international standards to the fullest extent possible;

(vii) prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes; and

(viii) include such other similar and consistent elements as the Director considers necessary; and

(B) shall not prescribe or otherwise require—

(i) the use of specific solutions;

(ii) the use of specific information or communications technology products or services; or

(iii) that information or communications technology products or services be designed, developed, or manufactured in a particular manner.

(2) LIMITATION.—Information shared with or provided to the Institute for the purpose of the activities described under subsection (c)(15) shall not be used by any Federal, State, tribal, or local department or agency to regulate the activity of any entity.

(3) DEFINITIONS.—In this subsection:

(A) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given the term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

(B) SECTOR-SPECIFIC AGENCY.—The term "sector-specific agency" means the Federal department or agency responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

[15 U.S.C. 7401 et seq.)

SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.

[15 U.S.C. 7403]

(a) COMPUTER AND NETWORK SECURITY RESEARCH GRANTS.—

(1) IN GENERAL.—The Director shall 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. Research areas may include—

(A) authentication, cryptography, and other secure data communications technology;

(B) computer forensics and intrusion detection;

(C) reliability of computer and network applications, middleware, operating systems, control systems, and communications infrastructure;

(D) privacy and confidentiality;

(E) network security architecture, including tools for security administration and analysis;

(F) emerging threats;

(G) vulnerability assessments and techniques for quantifying risk;

(H) remote access and wireless security; [and]

(I) enhancement of law enforcement ability to detect, investigate, and prosecute cyber-crimes, including those that involve piracy of intellectual property[.] *;*

(J) secure fundamental protocols that are integral to inter-network communications and data exchange;

(K) secure software engineering and software assurance, including—

(i) programming languages and systems that include fundamental security features;

(ii) portable or reusable code that remains secure when deployed in various environments;

(iii) verification and validation technologies to ensure that requirements and specifications have been implemented; and

(iv) models for comparison and metrics to assure that required standards have been met;

(L) holistic system security that—

(i) addresses the building of secure systems from trusted and untrusted components;

(ii) proactively reduces vulnerabilities;

(iii) addresses insider threats; and

(iv) supports privacy in conjunction with improved security;

(M) monitoring and detection;

(N) mitigation and rapid recovery methods;

(O) security of wireless networks and mobile devices; and

(P) security of cloud infrastructure and services.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this section on a merit-reviewed competitive basis.

(3) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the National Science Foundation to carry out this subsection—

(A) $35,000,000 for fiscal year 2003;

(B) $40,000,000 for fiscal year 2004;

(C) $46,000,000 for fiscal year 2005;

(D) $52,000,000 for fiscal year 2006; and

(E) $60,000,000 for fiscal year 2007.

(b) COMPUTER AND NETWORK SECURITY RESEARCH CENTERS.—

(1) IN GENERAL.—The Director shall award multiyear grants, subject to the availability of appropriations, to institutions of higher education, nonprofit research institutions, or consortia thereof to establish multidisciplinary Centers for Computer and Network Security Research. Institutions of higher education, nonprofit research institutions, or consortia thereof receiving such grants may partner with 1 or more government laboratories or for-profit institutions, or other institutions of higher education or nonprofit research institutions.

(2) MERIT REVIEW; COMPETITION.—Grants shall be awarded under this subsection on a merit-reviewed competitive basis.

(3) PURPOSE.—The purpose of the Centers shall be to generate innovative approaches to computer and network security by conducting cutting-edge, multidisciplinary research in computer and network security, including **[**the research areas**]** *improving the security and resiliency of information infrastructure, reducing cyber vulnerabilities, and anticipating and mitigating consequences of cyber attacks on critical infrastructure, by conducting research in the areas* described in subsection (a)(1).

(4) APPLICATIONS.—An institution of higher education, nonprofit research institution, or consortia thereof seeking funding

under this subsection shall submit an application to the Director at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the research projects that will be undertaken by the Center and the contributions of each of the participating entities;

(B) how the Center will promote active collaboration among scientists and engineers from different disciplines, such as computer scientists, engineers, mathematicians, and social science researchers;

(C) how the Center will contribute to increasing the number and quality of computer and network security researchers and other professionals, including individuals from groups historically underrepresented in these fields; and

(D) how [the center] *the Center* will disseminate research results quickly and widely to improve cyber security in information technology networks, products, and services.

(5) CRITERIA.—In evaluating the applications submitted under paragraph (4), the Director shall consider, at a minimum—

(A) the ability of the applicant to generate innovative approaches to computer and network security and effectively carry out the research program;

(B) the experience of the applicant in conducting research on computer and network security and the capacity of the applicant to foster new multidisciplinary collaborations;

(C) the capacity of the applicant to attract and provide adequate support for a diverse group of undergraduate and graduate students and postdoctoral fellows to pursue computer and network security research; [and]

(D) the extent to which the applicant will partner with government laboratories, for-profit entities, other institutions of higher education, or nonprofit research institutions, and the role the partners will play in the research undertaken by the Center[.] *;*

(E) the demonstrated capability of the applicant to conduct high performance computation integral to complex computer and network security research, through on-site or off-site computing;

(F) the applicant's affiliation with private sector entities involved with industrial research described in subsection (a)(1);

(G) the capability of the applicant to conduct research in a secure environment;

(H) the applicant's affiliation with existing research programs of the Federal Government;

(I) the applicant's experience managing public-private partnerships to transition new technologies into a commercial setting or the government user community;

(J) the capability of the applicant to conduct interdisciplinary cybersecurity research, basic and applied, such as in law, economics, or behavioral sciences; and

(K) the capability of the applicant to conduct research in areas such as systems security, wireless security, networking and protocols, formal methods and high-performance computing, nanotechnology, or industrial control systems.

(6) ANNUAL MEETING.—The Director shall convene an annual meeting of the Centers in order to foster collaboration and communication between Center participants.

(7) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the National Science Foundation to carry out this subsection—

(A) $12,000,000 for fiscal year 2003;
(B) $24,000,000 for fiscal year 2004;
(C) $36,000,000 for fiscal year 2005;
(D) $36,000,000 for fiscal year 2006; and
(E) $36,000,000 for fiscal year 2007.

○