



Introducing the federal cybersecurity R&D strategic plan



Douglas Maughan,
Bill Newhouse,
and Tomas Vagoun

In December 2011, the White House Office of Science and Technology Policy (OSTP) released the document, “Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and development program,” [1] which provides a framework for a set of coordinated federal strategic priorities and objectives for cybersecurity research. The release of this strategic plan marked an important milestone by the federal government’s research community. It expresses an understanding of key causes of cybersecurity deficiencies and presents research themes with high potential to significantly improve the security of cyber systems and infrastructure. The strategic plan is a culmination of many efforts within the federal government, most notably by the Cyber Security and Information Assurance (CSIA) Senior Steering Group for Cybersecurity Research and Development (R&D),

the CSIA Interagency Working Group of the federal Networking and Information Technology Research and Development (NITRD) Program, and by the Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group.

Leaping ahead on cybersecurity

Focused efforts to develop a federal cybersecurity R&D strategy gained momentum in 2008 with the Leap-Ahead Initiative, a component of the Comprehensive National Cybersecurity Initiative (CNCI) [2]. Pursuant to CNCI, OSTP tasked the NITRD Program with carrying out the R&D goals of this initiative—to coordinate and prioritize R&D efforts and to develop strategies for a portfolio of government R&D activities to pursue high-risk/high-payoff solutions to critical

NITRD Program coordinates federal R&D in computing and cybersecurity

Since 1991, the federal Networking and Information Technology Research and Development (NITRD) Program has been the forum for coordinating interagency research activities in networking, computing, software, cybersecurity, and related information technology areas. Cybersecurity research is coordinated among the agencies in the Cyber Security and Information Assurance (CSIA) Interagency Working Group.

The primary participants are representatives from the Defense Advanced Research Projects Agency (DARPA), the Department of Homeland Security (DHS) Directorate of Science and Technology, the Department of Energy (DOE), the Intelligence Advanced Research Projects Activity (IARPA), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), the National Science Foundation (NSF), the Office of the Secretary of Defense (OSD), and the DoD Service Research Organizations. Along with the CSIA Interagency Working Group, the Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group coordinates research related to national security systems.

The NITRD CSIA R&D Senior Steering Group was established in 2008 in response to the Presidential Comprehensive National Cybersecurity Initiative to define, coordinate, and recommend strategic federal R&D objectives in cybersecurity and to provide a robust conduit for cybersecurity R&D information across the policy, fiscal, and research levels of the government. The CSIA Senior Steering Group is composed of senior representatives of agencies with national cybersecurity leadership positions, including the Office of the Director of National Intelligence, DoD, DHS, NSA, NSF, NIST, the White House Office of Science and Technology Policy, and the Office of Management and Budget.

cybersecurity problems. At the onset, the CSIA Senior Steering Group determined that a government-wide framework for cybersecurity research was needed to provide both the coordination mechanism and the strategic directions for R&D. It was also clear within the CSIA Senior Steering Group that in order to achieve high-payoff, transformational results in cybersecurity, the framework needed to embody

the following principles: the research must focus on root causes of cybersecurity vulnerabilities (not symptoms); the research activities must bring together expertise from a range of disciplines, given that cybersecurity is a challenge with technological, social, and economic aspects; and we must develop enduring cybersecurity concepts to assure trustworthiness of our systems despite changes in technologies and cyber threats.

With these principles in mind, the CSIA Senior Steering Group issued three public requests for input from October 2008 through April 2009, canvassing industry and academia for game-changing ideas that could fundamentally change the cyber environment into one where the rightful users and owners have an advantage over attackers and illicit efforts. Two hundred and thirty-eight responses were received by the CSIA Senior Steering Group. (To view and download copies of the responses, see [3].) The Senior Steering Group's review of the responses gave rise to five prospective game-changing categories: hardware-enabled trust, cyber economics, moving target defense, digital provenance, and nature-inspired cyber health. In August 2009, the NITRD Program and OSTP held the National Cyber Leap Year Summit where some 150 researchers from industry, academia, and government met for four days to examine the five game-changing categories. The Summit provided a forum to review the prospective categories, elevate key ideas, and capture the output in the Co-Chairs' Report [4] and the Participants' Ideas Report [5].

Following the National Cyber Leap Year Summit, the CSIA Senior Steering Group synthesized the five game-changing category reports and established three initial cybersecurity R&D themes: tailored trustworthy spaces, moving target, and cyber economic incentives. These themes were announced [6] at a public event collocated with the 2010 Institute for Electrical and Electronic Engineers Symposium on Security & Privacy. Two months later, the White House released the Office of Management and Budget/Office of Science and Technology Policy's memo to the agency heads on science and technology priorities for the 2012 fiscal year budget [7], highlighting the three cybersecurity R&D themes and directing agencies to utilize the themes in prioritizing cybersecurity R&D budgets and programs. The release of the White House memo accelerated the creation of new programs to focus on the three cybersecurity R&D themes.

Cybersecurity R&D thrusts

With the successful release of the framework for cybersecurity game-changing R&D, the CSIA Senior Steering Group and the CSIA Interagency Working Group began developing the federal cybersecurity R&D strategic plan. Together with accelerating research in areas with game-changing potential, four areas (or thrusts) were defined by the strategic plan:

- ▶ **Inducing change**—utilizing game-changing themes to direct efforts toward understanding the underlying root causes of known threats with the goal of disrupting the status quo; the research themes in the strategic plan include tailored trustworthy spaces, moving target, cyber economic incentives, and designed-in security;
- ▶ **Developing scientific foundations**—developing an organized, cohesive scientific foundation to the body of knowledge that informs the field of cybersecurity through adoption of a systematic, rigorous, and disciplined scientific approach;
- ▶ **Maximizing research impact**—catalyzing integration across the game-changing R&D themes, cooperation between governmental and private-sector communities, collaboration across international borders, and strengthened linkages to other national priorities, such as health IT and Smart Grid; and
- ▶ **Accelerating transition to practice**—focusing efforts to ensure adoption and implementation of the powerful new technologies and strategies that emerge from the research themes and of the activities to build a scientific foundation so as to create measurable improvements in the cybersecurity landscape.

The strategic plan deliberately does not focus on specific technical challenges, such as more secure operating systems. Instead, the plan defines desired end states and future capabilities, which, if achieved, would overcome critical underlying causes of cybersecurity vulnerabilities. By defining the end states, the themes invite a diversity of approaches and encourage innovation across disciplines and sectors. The essence of the strategic plan is to express a vision for the research necessary to develop game-changing technologies that can neutralize the attacks on the cyber systems of today and lay the foundation for a scientific approach that better prepares the field to meet the challenges of securing the cyber systems of tomorrow. Altogether,

the plan provides guidance for federal agencies, researchers, and the public on how to prioritize research activities to achieve the greatest impact.

Efforts to develop scientific foundations in cybersecurity

In conjunction with the process to formally release the strategic plan, the federal agencies with R&D activities in cybersecurity began to introduce programs to pursue the goals outlined within each of these thrusts. In support of the thrust embodying the development of scientific foundations are representative R&D activities such as:

- ▶ **The Air Force Office of Scientific Research (AFOSR) 2011 Science of Security (SoS) Multidisciplinary Research Program of the University Research Initiative (MURI).** The objective of the AFOSR 2011 SoS MURI is to begin the development of an architecture or first principle foundation to define cybersecurity. The intent is to discover and define basic system properties that compose system security and other useful attributes in a manner that allows system properties to be verified and validated through theoretical proof and/or experiment.
- ▶ **NSA SoS lablets.** NSA support to academic lablets is focused on the development of a science of cybersecurity and a broad, self-sustaining community effort to advance it. A major goal is the creation of a unified body of knowledge that can serve as the basis of a trust engineering discipline, curriculum, and rigorous design methodologies. The results of SoS lablet research are to be extensively documented and widely distributed through the use of a new, network-based collaboration environment. The intention is for that environment to be the primary resource for learning about ongoing work in security science and to be a place to participate with others in advancing the state of the art.
- ▶ **The Army Research Laboratory (ARL) science for cyber portfolio.** The goal of ARL's science for cyber research portfolio is to examine a number of issues underlying cybersecurity and to develop novel theoretical constructs on which future cybersecurity advances can be based. The program explores models for the representation of cybersecurity, develops ensemble techniques for

improved detection of attacks, and investigates behavior as a fundamental indicator in detection and analysis. In particular, the research program focuses on theories and models that will lead to more effective intrusion detection techniques.

- ▶ **The National Science Foundation (NSF) Team for Research in Ubiquitous Secure Technology (TRUST)/Secure and Trustworthy Cyberspace (SaTC) Program.** TRUST, established as an NSF Science and Technology Center, focuses on addressing technical, operational, privacy, and policy challenges via interdisciplinary projects that combine fundamental science and applied research to deliver breakthrough advances in trustworthy systems in “grand challenge” areas such as the science of cybersecurity. In this area, TRUST researchers are developing a science base for security, with hopes to ultimately leverage these views in revising course content and embodying this theory in tools for system developers. Similarly, NSF’s SaTC program is focused on making cyberspace secure and trustworthy. Research in cybersecurity must “change the game,” check the misuses of cyber technology, bolster education and training in cybersecurity, establish a science of cybersecurity, and transition promising cybersecurity research into practice. The program recognizes that cyberspace will continue to grow and evolve and that advances in the sciences and technologies must grow and evolve as well, creating new “leap-ahead” opportunities.

The research in support of the strategic plan thrusts represents an increasing portion of the CSIA R&D budgets across federal agencies. This also translates into greater support of national priorities, such as health IT or Smart Grid, where key cybersecurity challenges can be addressed by focusing R&D activities within the framework of the thrusts.

Going forward, the execution of the strategic plan continues to be a collaborative process among a group of stakeholders: OSTP, responsible for policy and budgets; the CSIA Senior Steering Group, responsible for strategic directions; the CSIA Interagency Working Group, responsible for coordinating R&D activities; the SCORE Interagency Working Group, responsible for coordinating with R&D for national security systems; the federal agencies with cybersecurity R&D responsibilities; and the private sector. After a deliberate

and thoughtful process, the nation’s cybersecurity research community can focus its energy and resources on a shared vision of a trustworthy cyberspace. 

About the authors

Dr. Douglas Maughan is the cybersecurity division director in the Homeland Security Advanced Research Projects Agency within the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). Dr. Maughan has been at DHS since October 2003 and is directing and managing the cybersecurity R&D activities and staff at DHS S&T. His research interests and related programs are in networking and information assurance.

Prior to his appointment at DHS, Dr. Maughan was a program manager at the Defense Advanced Research Projects Agency (DARPA) in Arlington, Virginia. Prior to his appointment at DARPA, Dr. Maughan worked for NSA as a senior computer scientist and led several research teams performing network security research. Dr. Maughan received bachelor’s degrees in computer science and applied statistics from Utah State University, a master’s degree in computer science from Johns Hopkins University, and a PhD in computer science from the University of Maryland, Baltimore County.

Bill Newhouse is a cybersecurity program lead in the Computer Security Division, one of six divisions in the Information Technology Laboratory at the National Institute of Standards and Technology (NIST). Newhouse represents NIST in several collaborative efforts including (1) the National Initiative for Cybersecurity Education, (2) a partnership with DHS and the financial sector to develop and test innovative cybersecurity technologies and processes, and (3) as a member of federal interagency cybersecurity R&D committees.

Before coming to NIST in 2010, Newhouse spent five years in the Office of the Secretary of Defense where he focused on the cybersecurity and information assurance R&D portfolio, first with the assistant secretary of defense for research and engineering and then with the assistant secretary of defense for Networks and Information Integration (NII). While in NII, he championed Defense Venture Catalyst Initiative workshops to focus on cybersecurity

solutions from innovative companies. He is an electrical engineering graduate of both the Georgia Institute of Technology and George Washington University and has been with the federal government for over 25 years, beginning his career as a cooperative education student at NSA in 1986.

Dr. Tomas Vagoun provides subject matter expertise, technical leadership and management, and guidance to the Networking and Information Technology Research and Development (NITRD) Program in the areas of cybersecurity and information assurance and cybersecurity research and development. He supports the groups' monthly meetings and workshops, to include identifying opportunities for coordination and

collaboration within the NITRD Program. Dr. Vagoun also assists in the writing and editing of technical reports and planning documents (e.g., National Science and Technology Council federal plans, workshop reports, and the annual supplement to the president's budget [8]).

Before joining the National Coordination Office for the NITRD Program, Dr. Vagoun led the implementation of software development projects for major federal civilian and defense agencies. Dr. Vagoun received an MS and BS in computer science from West Virginia University and a PhD in information systems from the University of Maryland.

References

[1] Chopra A, Schmidt H. "Federal cybersecurity R&D strategic plan released. *The White House Blog*. 2011 Dec 06. Available at: <http://www.whitehouse.gov/blog/2011/12/06/federal-cybersecurity-rd-strategic-plan-released>

[2] National Security Council. "The comprehensive national cybersecurity initiative." Available at: <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>

[3] Responses to the CSIA Senior Steering Groups requests for input available at: http://www.nitrd.gov/fileupload/files/NCLY_submissions_public.pdf

[4] Chong F, Lee R, Acquisti A, Horne W, Palmer C, Ghosh A, Pendarakis D, Sanders W, Fleischman E, Teufel III H, Tsudik G, Dasgupta D, Hofmeyr S, Weinberger L. "National cyber leap year summit 2009: Co-chairs report. 2009 Sep 16. Available at: http://www.nitrd.gov/fileupload/files/National_Cyber_Leap_Year_Summit_2009_CoChairs_Report.pdf

[5] "National cyber leap year summit 2009 participants ideas report: Exploring paths to new cyber security paradigms. 2009 Sep 16. Available at: http://www.nitrd.gov/fileupload/files/National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf

[6] Wing J, Landwehr C, Muoio P, Maughan D. "Toward a federal cybersecurity research agenda: Three game-changing themes." 2010 May 19. Available at: <http://www.nitrd.gov/fileupload/files/NITRDCybersecurityR&DThemes20100519.ppt>

[7] Orszag P, Holdren J. Memorandum for the heads of executive departments and agencies: Science and technology priorities for the FY 2012 budget. 2010 Jul 21. Available at: <http://www.whitehouse.gov/sites/default/files/microsites/ostp/fy12-budget-guidance-memo.pdf>

[8] National Coordination Office for Networking and Information Technology Research and Development. "The Networking and Information Technology Research and Development program: Supplement to the Presidents Budget FY 2013." 2012 Feb. Available at: <http://www.nitrd.gov/PUBS/2013supplement/FY13NITRDSupplement.pdf>