Submissions to the

Request for Comments (RFC) – Federal Cybersecurity Research and Development Strategic Plan

1/14/13

Tomas Vagoun, vagoun@nitrd.gov

RFC: Published in the Federal Register, Vol. 77, No. 227, Monday, November 26, 2012

Deadline for submissions: January 11, 2013

Submissions (in chronological order received):

1. Amit Sahai, Professor, Department of Computer Science, University of California, Los Angeles
2. Cyber Security Research Alliance (CSRA)
3. U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM)
4. John Franco, et al, Computer Engineering, University of Cincinnati
5. Katherine Yelick, Associate Laboratory Director for Computing Sciences, Lawrence Berkeley National Laboratory
6. John S. Jolly, VPGM, Cyber Systems Division, General Dynamics |Advanced Information Systems
7. Electronic Privacy Information Center (EPIC)
8. Society for Industrial and Applied Mathematics (SIAM)
9. Timothy Molino, Director, Government Relations, BSA/The Software Alliance

Request for Comments (RFC) – Federal Cybersecurity Research and Development Strategic Plan

AGENCY: The National Coordination Office (NCO) for Networking Information Technology Research and Development (NITRD).

ACTION: Request for Comments (RFC)
FOR FURTHER INFORMATION, CONTACT: Tomas Vagoun at vagoun@nitrd.gov or (703) 292-4873.
DATES: To be considered, submissions must be received by December 19, 2012.
SUMMARY: This Request For Comments (RFC) is issued by the Cyber Security and Information Assurance Research and Development Senior Steering Group (SSG) of the Federal Networking and Information Technology Research and Development (NITRD) Program. The SSG is preparing a report to provide an update on technological developments in Federal cybersecurity research and development since the release of the 2011 Federal Cybersecurity Research and Development Strategic Plan (the strategic plan). Also, in light of the ever evolving technological landscape of cybersecurity, and as input to its follow-on report, the SSG seeks comments on the progress over the past year in the research areas identified in the strategic plan, the strategic plan's impact in orienting private sector cybersecurity research and development activities, the successes and challenges in achieving the technological objectives outlined in the plan, and on any nascent or emerging areas in cybersecurity research and development that warrant further focus. Additionally, the comments will be used by the SSG in its assessment of future needs and directions in Federal cybersecurity research and development. Comments are to be submitted to cybersecurity@nitrd.gov.

SUPPLEMENTARY INFORMATION: Continued cybersecurity research and development is critical to ensuring that we are on track as a Nation to develop innovative tools and capabilities to address cybersecurity threats. In December 2011, the White House Office of Science and Technology Policy (OSTP) released the "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," a framework for a set of coordinated Federal strategic priorities and objectives for cybersecurity research. (http://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=39)
The strategic plan was developed under the leadership of the Cyber Security and Information Assurance Research and Development Senior Steering Group (SSG) of the Federal Networking and Information Technology Research and Development (NITRD) Program. It identifies key cybersecurity research and development themes that are shaping and facilitating a coordinated Federal research and development agenda to engender game-changing technologies. With this overarching template, the federal scientific community has been focusing on a common set of problems. The strategic plan is being executed by all of the agencies conducting and funding Federal cybersecurity research, including DARPA, Department of Homeland Security, Department of Energy, IARPA, National Institute of Standards and Technology, National Security Agency, National Science Foundation, and the Department of Defense. Input from industry, academia, and other stakeholders during the development of the strategic plan contributed

greatly to the formulation of Federal research directions in cybersecurity. Guided by this plan, many research activities, initiatives, and solicitations have already been launched by Federal agencies in all areas defined by the plan.

In an effort to continue to evolve Federal strategic directions in cybersecurity research, the SSG seeks comments to gain a better understanding of the plan's impact. Furthermore, the SSG seeks input regarding prospective areas in cybersecurity research and development that might benefit from coordinated support by Federal agencies. To assist with its report, the SSG is requesting that interested parties submit written comments. We welcome comments from all interested parties, including, but not limited to, academia, private industry, and all levels of government. We seek comments on the following questions in relation to the strategic plan:

1) Research Themes of the Strategic Plan:
(a) Do the research themes need to be refined or enhanced? If so, in what way?
(b) What are the research, development, implementation, transition-to-practice, or other challenges that need to be overcome to achieve the goals under each theme?
(c) Are there areas in cybersecurity research not addressed by the strategic plan that should be? If yes, what are they, why are they important, and what advances in such areas are needed to improve the security, safety, and trustworthiness of cyberspace?

2) Activities that Advance the Strategic Plan:
(d) What activities are you or your organization undertaking that support the objectives of the strategic plan? Please include a brief description of initiatives, use-cases, capabilities, technologies, and/or achievements.
(e) How might your organization utilize the research outcomes?

3) Sustainable Progress:
(f) What interactions, relationships, campaigns, or targeted assistance would support a sustainable process to drive changes envisioned by the research themes?
(g) What engagements among Federal agencies, government labs, industry, and universities are particularly effective in enabling rapid progress in the development of solutions?

To further enhance discussions related to cybersecurity research and this RFC, the Government will webcast a session on Federal cybersecurity research and development during the National Science Foundation's Secure and Trustworthy Cyberspace Principal Investigators Meeting. The session and the webcast will take place on November 27, 2012, from approximately 1:00pm-3:00pm EST. Additional instructions will be available at http://cps-vo.org/group/satc.

SUBMISSION INSTRUCTIONS:

Submission email: submit your comments to cybersecurity@nitrd.gov
Submission deadline: to be considered, submissions must be received by December 19, 2012

To the extent applicable, when addressing a particular question included in this request for comments, comments should reference the relevant number associated with the question. Comments submitted will be made available to the public online or by alternative means. For this reason, do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. In accordance with FAR 15.202(3), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFC.

Submitted by the National Science Foundation for the National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD).

From: Amit Sahai [mailto:amitsahai@gmail.com]
Sent: Thursday, December 06, 2012 12:48 AM
To: Cyber Security
Subject: Comment on National Cybersecurity R&D Strategic Plan

The National Cybersecurity R&D Strategic Plan does an excellent job in identifying areas that need significant investment. However, when attacking new problems, most of the time it makes sense to build upon what is already working:

There is little dispute that the strongest links in cybersecurity infrastructure are the ones that can be protected by current **cryptographic** methods, such as public-key encryption, where security is engineered **mathematically**. A general rule of thumb is that the attacker will not bother to attack the crypto, because there are much easier attack vectors available via software and human factors. Because of the belief that crypto already "does its part" so well, surprisingly cryptography is only mentioned once in the entire National Cybersecurity R&D Strategic Plan.

What this fails to adequately recognize is that the **scientific foundations** of cryptography provide significant opportunities to **leverage novel cryptographic protocols** to harden protections that are currently provided only by software engineering. One notable example concerns access control: The most common solution to access control inherently requires a **trusted server,** in the sense that the software of the server is assumed to provide protection either to all sensitive documents themselves, or to a **secret key** stored by the server. For decades, this was considered an inevitable aspect of access control. Recently, however, the notion of **Attribute-Based Encryption** was proposed (by Brent Waters and myself), and provided a way to use novel cryptographic methods so that the server **need not be trusted to protect any secrets at all**. Thus, Attribute-Based Encryption is an example of a cryptographic innovation that significantly redraws the playing field, making the game much harder for the attacker. It does so most notably **by taking a security concern that was long considered the exclusive domain of software security, and moving it to the domain of cryptography.**

I urge the SSG to revise the National Cybersecurity R&D Strategic Plan to include a greater exploration of the role that the highly evolved and successful field of cryptographic design can play in addressing the central challenges of cybersecurity. I would be happy to offer any assistance that I can provide to this effort.

Thank you,
Amit Sahai
(PI on multiple NSF Awards related to Cybersecurity, PI on DARPA PROCEED grant)

Amit Sahai
Professor
Department of Computer Science
University of California, Los Angeles

CSRA Comments on "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program"

Prepared for:

The National Coordination Office for Networking and Information Technology Research and Development

Prepared in Response to:

The National Science Foundation's Request for Comments--Federal Cybersecurity Research and Development Strategic Plan, Federal Register, Vol. 77, No. 227 (November 26, 2012), FR Doc. 2012-28481 Filed 11-23-12

Presented on behalf of CSRA by:
Lee Holcomb, President
Cyber Security Research Alliance
401 Edgewater Place, Suite 600
Wakefield, MA 01880
781-876-8860
www.cybersecurityresearch.org

December 19, 2012

Table of Contents

About CSRA 3

Acronyms 4

(1) Research Themes of the Strategic Plan: 5

(a) Do the research themes need to be refined or enhanced? If so, in what way? 5

(b) What are the research, development, implementation, transition-to-practice, or other challenges that need to be overcome to achieve the goals under each theme? 6

(c) Are there areas in cybersecurity research not addressed by the strategic plan that should be? If yes, what are they, why are they important, and what advances in such areas are needed to improve the security, safety, and trustworthiness of cyberspace? 8

(2) Activities that Advance the Strategic Plan: 8

(d) What activities are you or your organization undertaking that support the objectives of the strategic plan? Please include a brief description of initiatives, use-cases, capabilities, technologies, and/or achievements. 8

(e) How might your organization utilize the research outcomes? 9

(3) Sustainable Progress: 9

(f) What interactions, relationships, campaigns, or targeted assistance would support a sustainable process to drive changes envisioned by the research themes? 9

(g) What engagements among Federal agencies, government labs, industry, and universities are particularly effective in enabling rapid progress in the development of solutions? 10

About CSRA

The Cyber Security Research Alliance, Inc. (CSRA) is an industry-led, non-profit consortium focused on research and development (R&D) strategy to address evolving cyber security environment through partnerships among government, industry, and academia. This forum was established in response to the growing need for increased public-private collaboration to address R&D issues in cyber security. The founding members of the CSRA are Advanced Micro Devices, Inc., Honeywell International, Inc., Intel Corporation, Lockheed Martin Corporation, and RSA, the Security Division of EMC.

CSRA is organized as a non-profit corporation, operated as a business league (professional association) within the meaning of Section 501(c) (6) of the Internal Revenue Code of 1986, as amended. It falls under the National Association of Insurance Commissioners (NAIC) code- 813910 (Business Associations). CSRA was incorporated in 2012. More information on CSRA is available at http://www.cybersecurityresearch.org/

Acronyms

ARL – Applied Research Laboratory

CERIAS – Center for Education and Research in Information Assurance and Security

CSRA – Cyber Security Research Alliance

ESF – Enduring Security Framework

NAIC – National Association of Insurance Commissioners

NCLY – National Cyber Leap Year

NSRC – Network and Security Research Center

R&D – Research and Development

(1) Research Themes of the Strategic Plan[1]:

Designed-In Security - Builds the capability to design, develop, and evolve high-assurance, software-intensive systems predictably and reliably while effectively managing risk, cost, schedule, quality, and complexity. Promotes tools and environments that enable the simultaneous development of cyber-secure systems and the associated assurance evidence necessary to prove the system's resistance to vulnerabilities, flaws, and attacks. Secure, best practices are built inside the system. Consequently, it becomes possible to evolve software-intensive systems more rapidly in response to changing requirements and environments.

Tailored Trustworthy Spaces - Provides flexible, adaptive, distributed trust environments that can support functional and policy requirements arising from a wide spectrum of activities in the face of an evolving range of threats. Recognizes the user's context and evolves as the context evolves.

Moving Target -Enables us to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency.

Cyber Economic Incentives - Develops effective incentives to make cybersecurity ubiquitous, including incentives affecting individuals and organizations. Incentives may involve market-based, legal, regulatory, or institutional interventions. Recognizes that sound economic incentives need to be based on sound metrics, including scientifically valid cost risk analysis methods, and to be associated with sensible and enforceable notions of liability and care. Requires advances in understanding the motivations and vulnerabilities of both markets and humans, and how these factors affect and interact with technical systems.

(a) Do the research themes need to be refined or enhanced? If so, in what way?

Vertical and Horizontal Themes. The themes cover a wide range of topics and at a high-level. It would be helpful to categorize the topics of each theme within the Strategic Plan to address technical depth (vertical) and cross-cutting domain breadth (horizontal). This way, creation and maturity of design-in security resources (personnel, processes, best practices, and tools) for all innovation would be encouraged and applicable to R&D requirements. Additionally, economic viability and necessary incentives for new technologies could be realistically and logically assessed.

Need for Foundational Research. While the themes provide a helpful framework for bringing game changing innovation to cybersecurity, additional investment in foundational research is needed to address these grand challenges. Advances are needed in:

- Well-defined languages to address the trust and run-time real-time integrity
- Reliable metrics
- Run-time assurance principles

Cross platform trust and trust composition are areas that are still developing. The meaning of "assurance of software execution under established policy for multiple owners, systems, and

[1] See http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

context" still needs to be established. Ability to transfer assurance mechanisms and policy from one computing and physical environment to another needs to be examined. Finally, developing empirical science as a foundation for the new generation of technologies and solutions in cybersecurity needs to continue as the key objective.

New Multidisciplinary Areas. Health inspired security solutions continue to offer interesting insights into cybersecurity innovation and could lead to the development of the new generation of secure computing. Approaches to self-healing of systems or DNA-based cryptography continue to appear promising.

Future Threat Horizons and New Technologies. In order to formulate technology requirements and invent new technologies, a fundamental understanding of threats in different environments is necessary, and these are not yet available. Thus, requirements for the new generation of technologies remains unknown. In this regard, additional approaches to analytics are needed. Looking at collection, processing, and response, collection is the only area making progress. New ways are needed to mine and organize data, analyze information, and identify trends in ways that will help formulate new technology requirements.

Research on Data. Data security and access to data constitute an important sub-theme that needs to be addressed. Additionally, research on global computing and Internet infrastructure, incentives necessary to support and improve it as well as related models of governance, balancing global and local uses, constitute interesting and necessary aspects of research.

Study of Research Incentives and Models. Research in cybersecurity and especially research collaboration is influenced by the system of incentives in different communities. In order to support collaboration, the system of incentives needs to be revised to be compatible with desired models of operation. But prior to proposing incentives, the current system of motivations needs to be studied. A study of incentives would be an important addition to this strategy as part of one of the Research Themes already defined.

(b) What are the research, development, implementation, transition-to-practice, or other challenges that need to be overcome to achieve the goals under each theme?

Improving Transition to Practice. Transition to practice is a critical element in the technology development process that requires strong collaboration among government, industry, and academia. Adoption and transition mechanisms should be part of the development of new technologies from R&D to product. This would require investment of resources in the research and development phase to facilitate potential adoption of new technologies in order to make R&D initiatives more relevant to the real world. Science and technology organizations in the government need to define a process and targets to support transition R&D. A more structured approach will improve the connection of R&D results to future solutions.

Organizations like CSRA could help outlining such processes and associated success metrics. CSRA was established to enhance collaboration in cybersecurity research and development and develop new collaboration models to accelerate innovation and time to market for new technologies. CSRA brings industry views and expertise to cybersecurity R&D community.

Considering Security in Context. Building security features independently of the technology, organizational, and societal context, in which these security features will be used doesn't lead to success. Usability, economic consideration, the positioning of a solution or a technology have to be considered at an early stage. Improving the framework to take cybersecurity context into consideration promises positive impact on future adoption.

The Strategic Plan needs to be augmented with a holistic action plan that addresses not only technology, but also, people and processes. For example, an effort is needed to study personnel across the entire system lifecycle including, but not limited to, system designers, architects, developers, integrators, installers, maintainers, users/consumers and disposers. Today, there is research focused on users/consumers, but less on the other personnel that often may make key decisions for technologies deployed today. Multi-stakeholder working groups are needed to define the objectives of such studies and the types of inter-disciplinary approaches that need to be brought to bear to first document and analyze the problems and then develop effective solutions.

Effort is needed to develop approaches to process that improve the alignment of cybersecurity R&D with industry practices in system concept, design, test, development, integration, operations, and retirement, including:

1) Technology transfer models adopted by various industry sectors and segments,
2) Business models and incentives,
3) System and software development methods, and
4) System configuration and maintenance

Today, academia is motivated by disruptive technology transfer models where game changing ideas can be commercialized with relatively small amounts of investment via startup companies. While this approach creates many successes, there are many failures as well. To augment this model, increased emphasis may be placed on other technology transfer models where solutions need to be integrated into existing industry products and services for sustaining impact. Such multi-stakeholder models still need to be defined.

The Strategic Plan emphasizes key aspects of cyber incentives, but these should not be studied in isolation as a separate research topic. Instead, principles and practices in this area should be developed and used in all research projects to support varied paths to commercialization and related infrastructure and ecosystem support. In this regard it would be helpful to identify the need to address cybersecurity across the development lifecycle.

Knowledge repositories such as U.S. Department of Homeland Security's "Build Security In"[2] are also extremely valuable in realizing sweeping changes across the industry. Innovation is in this area that provides practitioners with simple tools to institutionalize cybersecurity considerations are needed. Lastly, solutions that allow "secure by default" capabilities can address key gaps that exist in configuration and maintenance of systems.

[2] See https://buildsecurityin.us-cert.gov/bsi/home.html

(c) Are there areas in cybersecurity research not addressed by the strategic plan that should be? If yes, what are they, why are they important, and what advances in such areas are needed to improve the security, safety, and trustworthiness of cyberspace?

Critical Infrastructure Protection. The Strategic Plan is both broad and specific in its identification of challenges and approaches to address those challenges. That said, one area that needs more emphasis is critical infrastructure protection. There is broad discussion on the vulnerabilities, cyber attack vectors, and potential consequences if our nation's critical infrastructure is compromised.

The Strategic Plan mentions critical infrastructure and identifies representative priorities in Health Information Technology, Smart Grid, Financial Services, and Transportation. However, the Strategic Plan falls short of identifying and addressing all of the relevant critical infrastructures that impact safety, security, and quality of life for U.S. citizens. Two enhancements would add value in this context. First, an enumeration of critical infrastructures of interest, for example, the critical infrastructure sectors identified by DHS[3] could serve as a starting point for a holistic picture. Second, a focused effort to identify fundamental research challenges that need to be addressed for game changing impact on these critical infrastructure systems needs to begin. This includes multi-disciplinary research that balances priorities between security, safety, reliability, and timeliness for these systems. Metrics, trust composition, cross-domain trust, real-time and run-time integrity assessment as well as usable models for transition to practice, design of secure system, and ecosystem enablement will all be helpful in moving cybersecurity R&D forward.

(2) Activities that Advance the Strategic Plan:

(d) What activities are you or your organization undertaking that support the objectives of the strategic plan? Please include a brief description of initiatives, use-cases, capabilities, technologies, and/or achievements.

CSRA Activities. CSRA's mission is compatible with the needs to execute this strategic plan. In April 2012, in anticipation of the formation, CSRA conducted a workshop with government, industry, and academic participants to develop foundations for CSRA's technical approach. Creating awareness of the models already in existence and involving all stakeholders in a discussion will be instrumental in bringing the community of research and community of practice closer together. CSRA is structured to address collaboration between government, industry, and academia to help align their priorities in cybersecurity R&D.

Industry Activities. Industry already supports academic research through a variety of models, from direct collaboration within institutes and technology centers to funding academic research that looks at fundamental security features for the next generation of the technologies, for example, CyLab at Carnegie Mellon University[4], The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University[5], Network and Security Research Center (NSRC)[6] and Applied

[3] See http://www.dhs.gov/critical-infrastructure-sectors
[4] See http://www.cylab.cmu.edu/
[5] See http://www.cerias.purdue.edu/
[6] See http://nsrc.cse.psu.edu/

Research Laboratory (ARL)[7] at Pennsylvania State University, and Georgia Tech Research Institute[8]. The collaboration models already include some possibilities for co-investment or additional input by other companies, but they are disconnected from the government funding process.

(e) How might your organization utilize the research outcomes?

Industry Views. Industry expects cybersecurity R&D to provide viable results to inform future research and product development. Broad themes and collaboration permit to bring awareness of disparate security features and enable an ecosystem to support greater security. Research results should provide a rationale for developing products in a certain way that is connected to the threat environment and trends in threats and attacks. R&D advances to products based on sound business cases that yield products that can be commercialized and realize a reasonable profit.

Commercial Impact. Commercial impact is critical to address cybersecurity needs and gaps identified in the Strategic Plan. Such impact can come in many forms including but not limited to new tools, methods, technologies, processes, standards, and policies. CSRA brings diverse industry needs and perspectives to this problem space to help broader understanding of the issue.

(3) Sustainable Progress:

(f) What interactions, relationships, campaigns, or targeted assistance would support a sustainable process to drive changes envisioned by the research themes?

Today, disjointed communities develop security features that are not designed to work end-to-end. Improving interaction between disjointed communities to support lifecycles of security features (e.g., in hardware, software, and networks) is essential. Workshops where learning could be shared are a good mechanism to support this. Both specialized and broader ecosystem related workshops are useful. Multidisciplinary workshops with multiple industry sectors involved are helpful. Workshops should be working sessions leading to collaborative projects or more focused research agendas.

Existing industry approaches to build cross-cutting channels to address broader cross-cutting issues should be leveraged. Broader stakeholders' participation is helpful to success. In addition to technology discussions, these mechanisms could create requirements to support adoption of productive technologies and evaluate their economic viability as well as other features necessary for broad adoption. Improved information sharing by government and industry of current and evolving threats is a key component to prioritizing and focusing critical cybersecurity R&D efforts. Targeted briefings, whitepapers, and knowledge repositories on the threats would raise awareness among technology researchers, implementers, and adopters to enable a push and a pull of the developed solutions into the marketplace. Offense (operations) should inform defense (developers) of threats and attacks in order for defense to develop controls to defend environments. A clear understanding of the current and evolving threat landscape could incentivize adoption of mitigating controls and

[7] See http://www.arl.psu.edu/
[8] See http://www.gtri.gatech.edu/

new solutions. Testbeds and other efforts to support the emergence of the ecosystem are helpful. Targeted threat analysis and development of usable metrics are important activities. Research results need to provide support for early research results in industry and lead to broader collaboration opportunities. It will also be helpful if methods and requirements for the correct uses of technologies are documented and broadly available, to ensure practical outcome for the research results.

(g) What engagements among Federal agencies, government labs, industry, and universities are particularly effective in enabling rapid progress in the development of solutions?

Efforts like the National Cyber Leap Year (NCLY) Summit[9], the Semiconductor Research Corporation (SRC)[10], Enduring Security Framework (ESF), and similar programs are useful in building the community to work on cybersecurity challenges and hard problems in a new way. Developing models that will bring awareness of existing collaboration models of industry and academia to government and academia will be necessary to amplify investment in research themes, speed up introduction of the new solutions, enable the future ecosystems, and ensure that already existing technologies and solutions could be leveraged and introduced in practice.

[9] See http://www.nitrd.gov/leapyear/
[10] See http://www.srcinc.com/

usacm ACM US Public Policy Council

RESPONSE TO REQUEST FOR COMMENT
Federal Cybersecurity Research and Development Strategic Plan
77 FR 70483
DOCUMENT NUMBER 2012-28481
U.S. NATIONAL SCIENCE FOUNDATION

RESPONSE FILED BY:
U.S. PUBLIC POLICY COUNCIL OF THE ASSOCIATION FOR COMPUTING MACHINERY

On behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM) we are submitting the following comments in response to the Request for Comment by the National Science Foundation on the Federal Cybersecurity Research and Development Strategic Plan ("Strategic Plan").

With over 100,000 members, the Association for Computing Machinery (ACM) is the world's oldest and largest educational and scientific computing society. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. Our comments are informed by the research experience of our membership. Should you have any questions or need additional information, please contact our Public Policy Office at 212-626-0541 or at acmpo@hq.acm.org.

We appreciate the attention of the National Science Foundation on checking on the progress of the field and mapping that against the Strategic Plan. We recognize the difficulty of coordinating research across so many different agencies, resulting in what many may consider an overly broad plan that could use more specifics. Cybersecurity is much more than a series of technically-oriented research questions, and it is important that strategic plans and the associated research include, among other things:

- Training that integrates the results of research to help the workforce adopt new technologies and practices.
- Human subjects research to understand why the public does (or does not) adopt various cybersecurity technologies and practices.
- Privacy research that addresses both how the public perceives privacy in the context of cybersecurity and how new cybersecurity technologies and practices can integrate privacy.

Answers to specific questions in the RFC

(1) Research Themes of the Strategic Plan

The strategic plan is vague on how its priorities are to be implemented. USACM's assumption is that a goal of the plan is to ensure that the priority areas outlined in the research themes are given due attention by covered agencies. We also assume that the priorities outlined in the plan are not intended to define all necessary research in the field,

and recommend that the plan (and any accompanying guidance) note that the priorities are not intended to exclude computing and information technology research that does not fall under one of the priorities.

(a) Do the research themes need to be refined or enhanced? If so, in what way?

Most of the research themes outlined in the plan are well-founded and have demonstrated promise in the laboratory and the research literature. However, the theme of Nature-Inspired Solutions is not similarly well founded,[1] and is insufficiently mature to allow for actionable goals in the context of cybersecurity. While some cybersecurity topics have realized a research advantage by identifying natural defenses and porting relevant concepts to cybersecurity solutions, those results apply to narrow niches. Additionally, there is a significant research literature going back nearly two decades that may not have been adequately examined in addressing the current theme.

It is important to ensure that research findings can be communicated to as many people that can use it as possible. However, that need must be balanced against ensuring an appropriate balance amongst short-, medium- and long-term research. Some in the research community have expressed concerns that there can be too much emphasis on transition-to-practice activities.

(c) Are there areas in cybersecurity research not addressed by the strategic plan that should be? If yes, what are they, why are they important, and what advances in such areas are needed to improve the security, safety, and trustworthiness of cyberspace?

While national security is mentioned in the plan, the growth in that sector of cyberspace suggests it could use additional emphasis. For example, there is intense interest, and some cases of implementation, in offensive cyber efforts or cyber retribution against attackers. There is no corresponding basic research to ground such efforts. The ability or limitations in confidently identifying perpetrators; capabilities and limitations in controlling and estimating collateral damage; and economic impacts and liability issues of offensive cyber efforts are just a few of the important basic research questions raised by national security concerns. Research on these questions would have application outside of the national security context. There is increasing attention within the federal government on developing a national doctrine for cyberspace, and should that take shape, it would be useful to have a research foundation to rely on.

Related to the above, we urge that research be directed to efforts to enhance civilian law enforcement related to cybersecurity. Most of the unlawful behavior in cyberspace (past, present, and near future) appears to be non-military in origin, and cybersecurity research and development should be balanced to reflect activity in the field. Finding ways to apply

---

[1] Relevant explorations of the limitations of this approach can be found in section 5 of the unclassified JASON Report "Science of Cyber-Security," November 19, 2010. Accessible at http://www.nitrd.gov/fileupload/files/JSR10102Science_of_cyber20101128.pdf

civilian investigation and law enforcement to acts both large and small, and work with international partners, are needed. There is a distinction between cybersecurity related to law enforcement goals and cybersecurity related to national security goals, and this should be reflected in research priorities.

Additionally, we encourage consideration of privacy issues across the cybersecurity research spectrum. There needs to be attention focused on minimizing exposure and/or derivation of personal and private information in all aspects of information systems research: cloud computing, big data research, mobile computing, data mining and discovery, cyber security, law enforcement, and more. Understanding -- and addressing -- the tensions between enhanced discovery and protecting privacy should be a major focus of research.

(2) Activities that Advance the Strategic Plan:

(d) What activities are you or your organization undertaking that support the objectives of the strategic plan? Please include a brief description of initiatives, use-cases, capabilities, technologies, and/or achievements.

Our members conduct their own research and engagement activities that we cannot effectively capture in these comments. USACM, through the Association for Computing Machinery, is participating as a member of the Identity Ecosystem Steering Group established to implement the National Strategy for Trusted Identities in Cyberspace. While the group is still standing up as an organization, ensuring that there is a way of supporting and communicating relevant research is an important thing that the Steering Group has yet to do.

(3) Sustainable Progress:

(f) What interactions, relationships, campaigns, or targeted assistance would support a sustainable process to drive changes envisioned by the research themes?
(g) What engagements among Federal agencies, government labs, industry, and universities are particularly effective in enabling rapid progress in the development of solutions?

One of the best means of sharing knowledge within the computing community, and especially between researchers and practitioners, is the scientific meeting or conference. Given recent Office of Management and Budget guidance that severely curtails agency participation in conferences (and pending legislation that would impose similar restrictions), we are concerned that this important tool could be lost, or at least impaired. We recommend that research agencies like NSF do what they can to demonstrate to OMB and other relevant entities that such conferences are an important part of their mission, and deserve exemption from such conference restrictions.

To: Cyber Security and Information Assurance R&D Senior Steering Group

From: John Franco (Computer Engineering - franco@gauss.ececs.uc.edu) on behalf of Richard Harknett (Political Science - harknerj@ucmail.uc.edu),
Dharma Agrawal (Computer Science - dharmaagrawal@gmail.com),
Raj Bhatnagar (Computer Engineering - bhatnark@ucmail.uc.edu),
Prabir Bhattacharya (Computer Science - bhattapr@ucmail.uc.edu)
at the University of Cincinnati

Re: Request for comments, Federal cybersecurity R&D strategic plan

The following are comments from several faculty housed in a variety of departments at the University of Cincinnati. These comments represent a wide range of views and perspectives and reflect a deep concern for and interest in the field of cybersecurity at the university.

Summative Comment (response to question 1b)

The strategic plan's sound basis for directing R&D recognizes the importance of an interdisciplinary approach to research as critical to cybersecurity. While each theme does specify key research challenges, greater attention might be directed to the organizational and disciplinary roadblocks that exist to true interdisciplinary approaches and researching how to overcome those institutional impediments. Investment (incentives) in changing how we approach computer-based research needs emphasis, otherwise we will continue to have separate tracks of engineering, behavioral, economic, and political analysis. This is not a synthesis challenge, but an integration challenge. Technical solutions in isolation of these other areas of analysis will be flawed in their security outcome. Emphasis on best practice analysis for university-based reorganization and private-public coordination would support the strategic plans underlying assumption that interdisciplinary approaches are necessary. Section Four's goals would be advanced through improvement of mechanisms to disseminate such organizational best practices in achieving true interdisciplinary research in cybersecurity.

Designed-in Security (response to questions 1a, 1b, 1c)

The research challenges identify "team and supply chain practices to facilitate composition of assurance in the supply chain" and "Economics to improve motivation for use of tools through measurement of improved reliability and security" without explicit mention of regulatory analysis. The legal and policy context for both of these challenges needs examination.

Second, behavioral analysis of the unintended consequences of greater automation needs to be fostered. Greater automation will be a necessary component for successful designed-in security. However such technical solutions, particularly in environments in which they are adopted primarily for cost-saving efficiencies, rather than enhanced security can lead to a level of lower monitored reliance, which in turn may exacerbate, rather than reduce, single-point failure vulnerability into the overall system. Integration of behavioral analysis of unintended consequences of automation needs to supplement the technical development

research in this theme and might receive greater emphasis.

Information Assurance (response to questions 1a, 1b, 1c)

People entrusted to develop code are often not an optimal match for the tasks they have been given and the pressures of the environment they work in often cause them to underperform. On the one hand they may have an excellent feel for the interface to the machinery they are asked to code but on the other hand they may not feel appreciated, may not fully appreciate the magnitude of the consequences of mistakes in sections of code, and time constraints may force insufficient analysis of systems before they are deployed. A further complication is that many coding jobs are entry level with the expectation of promotion a few years away. Due to these and other factors, such as the need to quickly get numbers up for a project, code may not be developed, tested, and validated adequately. There are many well-known examples of system failures that could have been avoided if they had been audited more rigorously.

There is some promise that commercially available tools, such as Coverity, can be of significant help. Such tools have been tried with limited success. Currently, it seems that no tool can meet the needs of developers in all situations. Very powerful tools exist or are under development but trained experts are required to use the tools properly and it may take years to develop such expertise. Most companies appear to be unwilling to create, let's call them evaluation groups, that would serve the needs of the entire company by using the currently best tools to formally verify systems before deployment.

One way to improve the situation is to reduce and even eliminate the need for humans in writing executable code. This may be assisted as follows:

- Create languages whereby a developer writes a complete specification for the operation of a system, and presses a button starting the automatic process of producing code. This idea is not new and some support has been given to the development of, for example, Cryptol from Galois Systems. Cryptol has proven to be successful in verifying properties of cryptographic systems and even compiles the specification to VHDL but is nowhere near ready for general use. Its success is due to being built on top of the side-effects free functional language Haskell.

  Of course, the specifications created for such languages have to be validated. To help with this, libraries of "validated" specifications could be maintained, say by the US government. The specification languages would be designed to be modular to allow already "validated" sub-specifications to be used in a final specification.

  These languages would be taught alongside C, C++, and Java at first.

  So-called *Correct by Construction* approaches to software development have similar aims and use formal methods to achieve acceptable levels of commercial risk.

  This research and development direction should probably be a primary focus in a long-term strategy for insuring confidence in deployed code. This comment is a response to questions 1a (refinement of theme) and 1b (the challenge of success in an industrial environment that is not likely to change).

- The aforementioned languages will necessarily have access to and may even contain automated low-level verification tools such as SAT and SMT solvers. Simultaneously with the development of higher level languages there should be basic research aimed at improving solver design so that solver performance is more uniform, predictable, and practical over a wide range of input structures. Solver technology improvements over the last 15 years have been nothing short of astounding in support of feasible model checking and equivalence checking to name two tasks that future languages will need to support. The separation between pessimistic theoretical results ($\mathcal{NP}$-completeness) and performance of solvers in practice is continually getting wider but it still cannot be said that all the fundamental tasks associated with formal methods scale efficiently for all input structure types. Yet that is what is required to achieve the goal of provable or at least high confidence information assurance.

  Therefore, it is suggested that basic research aimed at understanding the nature of hard inputs for various solver technologies and using such information to develop new solver refinements and technologies should be an important direction for cybersecurity advancement. This is a response to questions 1a, 1b, and 1c.

Although there are several formal methods R&D directions that can be identified and that deserve support, the above emphasize the need for effective automated tools in an industrial environment where most applications personnel are not expected to spend a career in development and should not rely on a central evaluation unit for help. A switch to an industrial environment such as the one at Rockwell-Collins is not seen as likely for most organizations.

Tailored Trustworthy Spaces (response to questions 1a, 1c)

This section does not mention behavioral and policy research that will be necessary to identify the interface dynamics that will make people choose greater security over ease and convenience. Private sector industry and markets will not gravitate toward encouraging use of more secured levels, if that demand does not permeate the market from individual consumers; however, those consumers are very unlikely to make such demands when the market's main driver is a model focused on customizable convenience under which security degrades. This classic chicken and egg dynamic needs to be integrated into the technical research pathways under development in this theme. The wireless focus is key and a perfect exemplar of how behaviorally the model of customized convenience is driving both technical and behavioral developments at the expense of security.

This raises an underdeveloped element in the theme as well, namely viewing the education component of cybersecurity as primarily a dissemination mechanism (mentioned in section 4), rather than a behavioral shaping mechanism. The "shared responsibility" premise of the federal government's overall cybersecurity framework continues to lack penetration in society at large, where there remains no formation of a public good model or civic duty context to contribute to cybersecurity (it remains a private interest). This theme would benefit from encouraging sophisticated research into the effectiveness of cyber-education and what practices need adjustment, particularly as both technical and behavioral developments continue apace.

Information Assurance - database integrity in the cloud (1a-1c)

Important information is now being stored digitally instead of on paper mainly because it has originated in digital form. How best to store this information is an unsolved question which it is vital to answer because important data is likely the target of some group with malicious intentions to destroy, modify, or acquire the information. The problem is becoming more difficult to solve as more data becomes stored "in the cloud." The following are some of the technical issues that should be researched.

- Data management in the cloud must be automated. The size of the cloud allows for redundancy that is needed to keep data safe but what exactly needs to be done to detect and repair malicious attacks on the data?
- If data in the cloud can be accessed by almost anyone with sufficient technical expertise, how can attackers be prevented from mining multiple databases to synthesize information that should be private or classified?

Moving Target - (response to questions 1a, 1c)

It is unclear that the research challenges specified under the Moving Target theme include behavioral studies of organizational management techniques, strategic culture and organizational change. The theme rightly acknowledges the challenge to conventional wisdom of the premise that added complexity will enhance security. Large organizations, such as militaries for example, have strategic cultures that rest of doctrines, which while tactically flexible, prove to be organizationally much less so. Research from the security studies literature on organizational culture could be emphasized or mentioned here.

A second important element missing is any recognition that the United States as an actor will not always be solely on the defense in cyberspace. Research into the interface of offensive and defensive operations needs be encouraged. The potential for blowback within the system, for example, could be high without strong coordination models.

A third element is research into the differing technical requirements to sustain defense from that required to support law enforcement. An element of cybersecurity will be the enforcement of law over time (be it criminal or civil). How can systems "move" and adapt, and yet retain sufficient stability to offer support of evidence necessary under cyber-related laws for prosecution of crimes.

Fourth, research into systems that can support intelligence-gathering simultaneously with defense needs to be encouraged. In many ways, current practices require a tradeoff between one and the other.

Cybersecurity will not always be advanced through defense alone and thus technical systems need to be able to support other strategies such as offense, intelligence-gathering, and law enforcement.

Wireless Mobile Networks - (response to questions 1a-1c)

An efficient mechanism that supports the use of a shared symmetric key between sender and receiver for fast encryption/decryption and with low overhead. The key should never

be exchanged, but pre-distributed in a strategic way such that at least two keys are common between any sender and receiver pair. This technique will be especially applicable to cellular phones, tablets, ad hoc and sensor networks, wireless mesh networks and 4G LTE networks. It will facilitate efficient, secure communication while maintaining the simplicity of the encryption/decryption processes.

To ensure resiliency, the shared keys need to be changed dynamically. This can be done using bi-variate polynomials that change keys as and when needed. Further enhancement is needed such that the bi-variate polynomials can be changed.

Recalculation of a common shared key is normally necessary whenever membership changes as users enter and leave a mobile network. This is essential for both forward and backward secrecy in the network. Research is needed to develop systems supporting mobile networks that accommodate a varying degree of security over an underlying scheme as per requirements. Further work is needed to investigate the resiliency of such complex systems in various applications of wireless devices.

Activities that Advance the Strategic Plan - (response to questions 2d-2e)

The following are examples of research at the University of Cincinnati and a partnership with industry that address issues in cybersecurity.

- *Research into the nature of computation of SAT solvers* (2d)

  This has led to a theoretical understanding of DPLL algorithms and identification of some efficiently solvable classes of Satisfiability. Such an understanding has been instrumental in producing evermore efficient and robust SAT solvers. Such solvers are at the core of fast-improving ideas for formal methods tool implementation. More recently, a SAT-solver was developed based on non-conventional principles, employing a new structure called a SMURF (State Machine Used to Represent Functions). The novelty of that solver is its ability to deal efficiently with constraint sets that are known to be hard for DPLL solvers. Current work aims to solve difficult problems by adding *unsafe* constraints (these are not inferred and are determined from an analysis of solutions rather than an analysis of problem structure) before search to keep search space size small and then retracting them when it is clear that search space size will not increase significantly when doing so. Current work also aims to make use of ACL2 for anomaly detection by pairing it with weakest precondition technology. The above efforts have been supported by the AFOSR, ONR, and NSA.

- *Research into the security of mobile networks* (2d)

  Secured communication in wireless and mobile systems has been considered as the problem of providing security in multiple layers based on the level of complexity. A distributed 2-D array of keys supports a common key between any two adjacent wireless devices. Under an AFOSR STTR grant, a 3-D extension was developed to provide a reduction in the number of keys needed for a given size network. To make the keys change dynamically, bi-variate polynomials are used as an element of 2-D and 3-D keys. For secured group communication, multivariate polynomials are used to address the resiliency problem in wireless mesh networks. This also enables backwards and forward secrecy when group communication is used in 4G-LTE networks.

- *Research on policy* (2d)

  Faculty have engaged and published in both conceptual framework analysis for strategy development and legislative analysis of Congressional bills considered over the past few years. Current research is examining fundamental security dynamics that relate directly to the research challenges denoted in the "deep nature of cyberspace" section of the strategic plan.

- *Other areas of research* (2d)

  Faculty have explored other areas that touch on cybersecurity. These include steganography, the security of database systems, Middleware security, java security, android phone security, and quantum resistant cryptosystems.

- *Cybersecurity in the Curriculum* (2e)

  At the University of Cincinnati, several disparate departments including Political Science, Criminal Justice, Information Technology, Electronic and Computer Systems, Computing Sciences and Informatics, and Mathematics, have independently either created or have partially created cybersecurity programs. It has now been recognized that these should be jointly coordinated along with other programs where interdisciplinary cooperation will benefit the faculty and students of the cooperating departments. To this end an Institute for Computing Sciences and Technologies has been proposed.

  Political Science, Criminal Justice, and Information Technology have implemented a Certificate Program at the undergraduate level allowing cross-acceptance of elective credits, so majors in those three departments can easily fulfill a certificate in cybersecurity course sequence. The objective will be to expand this cooperation to relevant majors in Engineering and Information Systems. This course coordination will enable better research coordination in advancing, particularly, the goals of the Developing Scientific Foundations thrust with a focus on conceptual modeling.

  Independently, the School of Electronic and Computer Systems and the School of Computing Sciences and Informatics have established a masters program in computer security in cooperation with a large defense contractor's electronic systems facility in a suburb of Cincinnati. Some of the contractor's employees are students in the program and some are adjunct faculty. The adjuncts teach Malware Analysis, Big Data Analysis, and Network Exploitation. The university faculty teach Network Security, Cryptography, Computer Security, Formal Methods, Data Base Systems, and Middleware security. Regular university students may take these courses but some are available only to US citizens.

  Some of the contractor's students have elected to write a masters thesis. As students, they are usually granted a little extra time to complete their studies and theses. This affords the opportunity to explore some ideas that they would otherwise might not be able to. As an example, one student is working on new ways to protect against a relatively new attack vector called Return Oriented Programming (ROP) attacks and is developing a new protection scheme by which return addresses in memory are encrypted. Another student is developing a scheme for automated exploitation generation having been inspired by the work of Brumley at CMU.

Accelerating Transition to Practice - (response to question 2d)

The University of Cincinnati has created a new mechanism, the University of Cincinnati Research Institute, to facilitate coordination of base research with industry partners. This model will be an institutional support for potential work on cybersecurity.

COMPUTING SCIENCE DIRECTORATE, LAWRENCE BERKELEY NATIONAL LABORATORY

December 19, 2012

SUBJECT: **Berkeley Lab Response to SCORE Request for Comments**

This is the Berkeley Lab response to the Request for Comments issued by the Cyber Security and Information Assurance Research and Development Senior Steering Group of the Federal Networking and Information Technology Research and Development (NITRD) Program. This response addresses:

- Question #2: identifying activities that LBNL is undertaking to support the objectives of the PCAST Strategic Plan for Federal Cybersecurity Research and Development, and
- Question #3, recommending interactions, relationships, and engagements for sustainable progress in advancing the strategic research themes.

Response to Question #2d:

Berkeley Lab has a long history of computer security research and development, dating back at least to the development of the Bro intrusion detection framework [Pax99] and security components of the IPv6 networking protocol. It also operates a number of key DOE user facilities, including the National Energy Research Scientific Computing Center (NERSC), and the Energy Sciences Network (ESnet), as well as variety of cyber-physical systems including the Advanced Light Source (ALS). Thus Berkeley Lab is a consumer and beneficiary of key cybersecurity technologies and also a target. The necessary openness of the Berkeley Lab's facilities and their visibility internationally, makes them a particularly tempting and active target, even in comparison to many other national labs.

Along with key, close collaborators at UC Berkeley, UC Davis, and the International Computer Science Institute (ICSI), Berkeley Lab has addressed a variety of computer security research and development challenges. These include:

- collaborations with UC Berkeley and ICSI, that resulted in the Bro IDS [Pax99], a key operational capability deployed at the Berkeley Lab (including NERSC and ESnet), and at Argonne National Laboratory;
- collaborations with UC Davis to perform basic, use-inspired research addressing areas including the insider threat [BEF10], data sanitization [BCP10], process modeling of elections [SEC10], security of high-performance computing [WEPB12,WPB13], control system security [LWM12], "clean slate" solutions [PTB12], and Byzantine fault tolerance [DPL12, DZPL12].

Each of these research areas involve key "science of cybersecurity" themes, including formal methods, the development of metrics, sound measurement techniques, and augmenting technical solutions with social sciences. We believe that these efforts have been highly effective by employing highly skilled academic and national laboratory researchers to address cybersecurity challenges at major national laboratory facilities such NERSC and ESnet. These facilities provide a research environment where attacks can be examined, and solutions potentially prototyped, deployed, and examined in practice solutions. The Bro IDS, data sanitization, HPC security, and network resilience all demonstrate this lifecycle.

Response to Questions #3 f,g:

Sustainable progress in both basic and applied cybersecurity research will be enabled by continued and increased federal support for partnerships that bring the best researchers in academia and the national laboratories together. This assertion is supported by our experiences as articulated in the response to Question #2, above. Many of the nation's critical scientific user facilities are located at national laboratories, and face cybersecurity challenges. These facilities provide a research environment where attacks can be examined, and solutions potentially prototyped, deployed, and examined in practice solutions. Both the national laboratories and universities have highly qualified researchers who are equipped to address these cybersecurity challenges. Partnerships between the laboratories and universities have been highly effective in the past, and we expect this to continue in the future.

Sincerely,

Katherine Yelick
Associate Laboratory Director for Computing Sciences
Lawrence Berkeley National Laboratory

cc: Greg Bell, Scientific Networking Division Director and Head of ESnet, LBNL
David Brown, Computational Research Division Director, LBNL
Sudip Dosanjh, NERSC Division Director, LBNL
Deb Agarwal, Advanced Computing for Science Department Head, LBNL
Sean Peisert, Research Scientist, LBNL

References

[BCP10] M. Bishop, J. Cummins, S. Peisert, A. Singh, D. Agarwal, D. Frincke, & M. Hogarth, "Relationships in Data Sanitization: A Study in Scarlet," *Proc. of the New Security Paradigms Workshop*, 2010.

[BEF10] M. Bishop, S. Engle, D. Frincke, C. Gates, F. Greitzer, S. Peisert, S. Whalen, "A Risk Management Approach to the 'Insider Threat,'" *Insider Threats in Cybersecurity*, pp. 115–138, Springer, 2010.

[DPL12] S. Duan, S. Peisert, and K. Levitt, "*h*BFT: Fast Byzantine Fault Tolerance With Optimal Resilience," working paper (in review), 2012.

[DZPL12] S. Duan, H. Zhang, S. Peisert, and K. Levitt, "BChain: A Family of Practical Byzantine Fault-Tolerant Protocols," working paper, 2012.

[LWM12] X. Li, Z. Wang, V. Muthukumar, A. Scaglione, C. McParland, and S. Peisert, "Networked Loads in the Distribution Grid," *Proc. of the APSIPA Annual Summit & Conference*, 2012.

[Pax99] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," *Computer Networks*, 31(23):2435–2463, 1999.

[PTB12] S. Peisert, E. Talbot, and M. Bishop, "Turtles All The Way Down: A Clean-Slate, Ground-Up, First-Principles Approach to Secure Systems," *Proc. of the New Security Paradigms Workshop*, 2012.

[SEC10] B. I. Simidchieva, S. J. Engle, M. Clifford, A. C. Jones, S. Peisert, M. Bishop, L. A. Clarke, and L. J. Osterweil, "Modeling Faults to Improve Election Process Robustness," *Proc. of the 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Computing*, Aug. 2010.

[WEPB12] S. Whalen, S. Engle, S. Peisert, and M. Bishop, "Network-Theoretic Classification of Parallel Computation Patterns," *Int'l J. of High Performance Computing Applications*, 26(2):159–169, 2012.

[WPB13] S. Whalen, S. Peisert, and M. Bishop, "Multiclass Classification of Distributed Memory Parallel Computations," *Pattern Recognition Letters*, 34(3):322–329, Feb. 2013.

GENERAL DYNAMICS
Advanced Information Systems

December 18, 2012

Mr. Tomas Vagoun
National Coordination Office
Networking Information Technology Research and Development

Dear Sir:

The document "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program" provides a vision for the direction of federally-funded cybersecurity research in the United States. Given the complex nature of the cybersecurity problem, this vision is necessary; as computational systems tend to integrated, so too must the ultimate goal of research efforts. It is important that such a planning document be holistic in order to meet the needs of the Nation, and to this end, it must have the authority to overrule the more parochial interests of participants. In this note, we will comment only on the research themes presented in the document that we reinforce in our broad collection of activities supporting the USG and commercial sector.

Re: Question 1

The theme of Designed-in Security addresses how to make software and hardware inherently more secure, and we continue believe that this remains to be of critical importance given the need to support supply chain trust and infrastructure provisioning. Such methods are generally based on pure logic and have both significant theoretical, and computationally-intensive, underpinnings. One of the challenges in this area is to make them practical, broadly applicable, and to integrate their use into our development processes; However, as adversaries who launch malware against us use continuously changing attack vectors within the codebase, we should point out that Designed-in Security is likely an evolutionary processes as well. To this end, we agree that the goal of 'attack-resistant' versus 'attack-proof' software systems needs to be maintained as the emphasis of this research theme.

Re: Questions 1c, 2, 3

General Dynamics Advanced Information Systems is closely aligned to the focus area entitled "Deep Understanding of Cyberspace" and believes there remain large gaps in our ability to obtain large-enterprise, cyber situational awareness. Throughout our cybersecurity work for the USG and commercial

2721 Technology Drive
Annapolis Junction, MD 20701
Tel: 240 456 5500
Fax: 240 2942236
www.gd-ais.com

sectors, as well in protecting our own enterprise, the velocity and quantity of the sensor data we gather challenges our ability to process it in a completely and timely manner. Difficulties in finding suitable Enterprise-wide solutions as well as human resources who are both data scientists as well as cyber forensics experts have stimulated our creation of an IRAD project that is apropos to the "Deep Understanding of Cyberspace" activity. In our work we are providing analytics for detection of cyber incidents and real-time situational awareness, utilizing distributed storage and computational capability of the scale required to process all network sensor information from large-scale Enterprise environments. The program aims to support, or reinforce, human reasoning and existing signature detection techniques with advanced adaptive pattern discovery and anomaly detection. We are striving to supplement analyst's workflow based on an analyst's reasoning with intelligent assistance from machine learning. By implementing data fusion techniques for evidence correlation with the application of models for incident understanding, our analytics will enable detection of stealthy threat processes amid the large volume of nominal processes. Visualizations to provide situational awareness and understanding of nominal and threat processes are also being developed.

Experience in this research project suggests that understanding what is nominal (in order to declare true cyber incidents) in a large-scale enterprise system in terms of the conventional sensor data types received is not likely to be achieved by purely statistical or machine learning methods. Common complications exist because management of the service and network infrastructure is, for the sake of efficiency, frequently done in a distributed fashion and in a manner in which transparency of operation is not a high-priority goal. To this end, GD-AIS believes that stronger policy and regulation go hand-in-hand in achieving the goal of greater cybersecurity, and therefore, we believe the Cyber Economic Incentive (CEI) research theme continues to be essential and critical to the strategic plan.

However, we have observed how the Government and companies research technologies, acquire solutions, and integrate them into an overall architecture, and we believe that the various acquisition processes do not necessarily match the operations tempo of the evolving threat environment. Without adopting more agile contracting methods, we fear that the Government and Industry will remain behind the evolving threat curve. How to incentivize good cybersecurity practices is clearly part of CEI, but it's not clear how the realities of today's USG acquisition processes are to be addressed, or included, within this research theme given it is very dissimilar to the commercial marketplace.

It is noteworthy that every research theme, and the scientific foundations section as well, emphasizes "development of models." In all cases such models must ultimately be applied to working software, and in some cases this may be difficult to do (note again our above comments in which we stated a difficulty in finding cybersecurity experts who are data scientists). In order to efficiently translate the knowledge represented by these models into software, it should be required that models be expressed in such a way

as adaptable to the software development process. This entails a degree precision of content and uniformity of expression that should be enforced on the producers of such models. Research in the general means of applying models to computation should be made use of here. Additional work to bridge the gap between abstract conceptual models and software capabilities in modeling, such as object-oriented languages and data schemas, may be needed.

Lastly, the Strategic Plan addresses a large number of ideas on the single topic of cybersecurity, without really addressing questions of overlap, inter-working, or interfaces. The introduction of a holistic research theme that investigates what revolutionary cyber ecosystems can possibly attain (versus *evolutionary* cyber ecosystems) is likely needed.

Sincerely,

John S. Jolly, VPGM
Cyber Systems Division
General Dynamics |Advanced Information Systems

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE CYBER SECURITY AND INFORMATION ASSURANCE RESEARCH AND DEVELOPMENT SENIOR STEERING GROUP OF THE FEDERAL NETWORKING AND INFROMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

"Request for comments regarding Federal Cybersecurity Research and Development Strategic Plan"

December 19, 2012

By notice published on November 26, 2012, the Cyber Security and Information Assurance Research and Development Senior Steering Group ("SSG") of the Federal Networking and Information Technology Research and Development ("NITRD") Program announced a request for comments on the progress of the 2011 Federal Cybersecurity Research and Development Strategic Plan ("Strategic Plan").[1] The Strategic Plan was developed by NITRD agencies in an effort to create a new cybersecurity strategy based on a coordinated set of research priorities characterized by four strategic goals: (1) Inducing Change; (2) Developing Scientific Foundations; (3) Maximizing Research Impact; and (4) Accelerating Transition to Practice.

EPIC supports various efforts of the Strategic Plan. Specifically, EPIC supports efforts to anonymize data to protect the privacy of users as researchers work towards better data models of cyber economic incentives.[2] These measures minimize risks to privacy resulting from the misuse of personally identifiable information. We also support the

[1] 77 Fed. Reg. 70483 (Nov. 26, 2012).
[2] *See, e.g.*, Executive Office of the President National Science and Technology Council, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, 10 (Dec. 2011) [hereinafter *Strategic Plan*].

preservation of anonymous web access within Trusted Tailored Spaces.[3] This technique allows individuals to obtain access to information without the risk of tracking and profiling. In addition, EPIC backs the Strategic Plan's call to promote privacy and focus on privacy-enhancing technologies within the context of "trusted identities."[4] EPIC has additional recommendations to improve the Strategic Plan to better protect privacy and civil liberties.

Pursuant to this request, the Electronic Privacy Information Center ("EPIC") recommends that the SSG incorporate the following recommendations into the Strategic Plan: (1) narrowly define "threat"; (2) fully adhere to the Privacy Act of 1974 and the Freedom of Information Act; (3) actively incorporate genuine privacy-enhancing technologies ("PETs") into new technologies and protocols; and (4) acknowledge the OECD Security Guidelines.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus on emerging civil liberties issues and protecting privacy, the First Amendment, and constitutional values. EPIC has a long history of promoting transparency and accountability for cybersecurity and government data collection programs, specifically through the enforcement of the Privacy Act and the Freedom of Information Act.[5] Transparent cybersecurity programs are crucial to the public's ability to monitor the government's national security efforts and ensure that federal agencies respect privacy

---

[3] *Id*. at 7-8.
[4] *Id*. at 12-13.
[5] *See EPIC v. NSA*, 678 F.3d 926 (D.C. Cir. 2012); EPIC, Cybersecurity Privacy Practical Implications, http://epic.org/privacy/cybersecurity/; EPIC, *EPIC v. NSA – Cybersecurity Authority*, http://epic.org/privacy/nsa/epic_v_nsa.html; EPIC, Comments of the Elec. Privacy Info. Ctr. to the Cyber Security and Information Assurance Research and Development Senior Steering Group of the Federal Networking and Information Technology Research and Development Program: Request for Comments, Dec. 19, 2012, *available at* http://epic.org/privacy/cybersecurity/EPIC-DOD-Cyber-Security-Comments.pdf.

rights and comply with their obligations under the Privacy Act. EPIC further supports techniques that improve both privacy and security.

I. The Strategic Plan Should Narrowly Define "Threat"

The Strategic Plan makes numerous references to "threats" without fully identifying what constitutes a threat.[6] The Strategic Plan references the "Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002" as a resource for "further data on the size and nature of threats,"[7] yet even this document fails to adequately define and narrow the term "threats." Such an open-ended and broad use of the word "threat" does not properly narrow the Strategic Plan's cybersecurity research objectives to relevant cybersecurity problems. EPIC objects to these particularly broad usages because they increase the risk of innocuous online activities being classified as "threats"—thereby providing the pretext for the collection of user data. Therefore, SSG needs to refine and clarify the definition of cyber "threat"

II. There is a Considerable Public Interest in the Transparency of Government Cybersecurity Activities

The challenges of cybersecurity touch upon a number of critical areas including healthcare, energy, financial services, and defense; and the efforts by the government to increase cybersecurity affect every citizen in the United States.

---

[6] *See, e.g.*, *Strategic Plan* at 1-4, 7, 9-10, 13-14.
[7] *Strategic Plan* at 2 n.3.

On May 29, 2009, President Barack Obama announced the Administration's plan to address the growing issue of digital information security.[8] Discussing the plan in 2010, Cybersecurity Coordinator Howard Schmidt emphasized the importance of transparency:

> Transparency is particularly vital in areas, such as the [Comprehensive National Cybersecurity Initiative], where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity. Transparency provides the American people with the ability to partner with government and participate meaningfully in the discussion about how we can use the extraordinary resources and expertise of the intelligence community with proper oversight for the protection of privacy and civil liberties.[9]

Transparency and accountability in cybersecurity research, development, and implementation will allow the public to participate in the ongoing cybersecurity debate as it develops and encourage government agencies to be mindful of the privacy and civil liberties of citizens of the United States.

III. The 2011 Federal Cybersecurity Research and Development Strategic Plan Should Fully Adhere to the Privacy Act and Freedom of Information Act

The Strategic Plan provides an overarching set of coordinated research priorities for a number of federal agencies including the Department of Homeland Security, National Security Agency, and Defense Advanced Research Projects Agency. Many of these agencies, through their agency work, collect various personal information on individuals that is subject to the Privacy Act of 1974.

---

[8] *See, e.g.*, Data Accountability and Trust Act (DATA), H.R. 1707, 112th Cong. (2011) (introduced by Rep. Rush (D-IL)); Secure and Fortify Electronic Data Act (SAFE Data Act) H.R. 2577, 112th Cong. (2011) (introduced by Rep. Bono Mack (R-DA)).

[9] Howard A. Schmidt, *Transparency Cybersecurity*, NAT'L SEC. COUNCIL (Mar. 2, 2010), http://www.whitehouse.gov/blog/2010/03/02/transparent-cybersecurity.

The Privacy Act of 1974 places extensive obligations on federal agencies that collect and use personal information.[10] Research and Development ("R&D") under the Strategic Plan that may collect and use personal information should not be exempted from the obligations under the Privacy Act of 1974. In addition to the Privacy Act, participants in the Strategic Plan should fully adhere to the openness requirements of the Freedom of Information Act ("FOIA"). EPIC emphasizes that FOIA's purpose is to facilitate transparency by providing public oversight of government operations. Therefore participants in the Strategic Plan should only apply FOIA exemptions when they are absolutely necessary.

IV. Privacy Protections are Vital to Cybersecurity

The incorporation of privacy safeguards is vital to cybersecurity. Robust privacy protections promote cybersecurity in a number of ways. Proper privacy protections, including adequate data protection and avoiding unnecessary sharing of personal information, limit exposure to a cyberattack or other type of breach and minimize the risk to individuals when such attacks occur.

Protecting individual's privacy keeps cybersecurity efforts focused on robust efforts to secure cyberspace, prevent attacks, and minimize damage and disruption when attacks do occur. As noted, EPIC supports the Strategic Plan's commitment to anonymity and privacy and emphasizes the need for the development of genuine privacy-enhancing technologies that minimize or eliminate the collection of personally identifiable information where possible. Furthermore, in an effort to protect personal privacy and maintain the open and free flow of information, EPIC recommends the Strategic Plan

[10] 5 U.S.C. § 552a (2006).

acknowledge the Organisation for Economic Co-operation Development ("OECD") Security Guidelines.[11] These principles include:

- Awareness;
- Responsibility;
- Response;
- Ethics;
- Democracy;
- Risk Assessment;
- Security Design and Implementation;
- Security Management and;
- Reassessment.[12]

In particular, EPIC emphasizes the need for recognition of the Democracy Principle, which states "[t]he security of information systems and networks should be compatible with essential values of a democratic society."[13]

V. Conclusion

As the Strategic Plan moves forward, the agencies involved in the plan must uphold their obligations under the Privacy Act and the Freedom of Information Act. EPIC urges the National Coordination Office for Networking Information Technology Research and Development to adopt the recommendations to the Strategic Plan suggested above.

Respectfully Submitted,

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Administrative Law Counsel

Jeramie D. Scott
EPIC National Security Fellow

---

[11] Organisation for Economic Co-operation Development, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002), *available at* http://www.oecd.org/internet/interneteconomy/15582260.pdf.
[12] *Id*.
[13] *Id*.

SOCIETY for INDUSTRIAL and APPLIED MATHEMATICS

3600 Market Street, 6th Floor
Philadelphia, PA 19104-2688 USA
Phone +1-215-382-9800
Fax +1-215-386-7999
www.siam.org • siam@siam.org

SIAM Response to the Networking and Information Technology Research and Development Program's Cybersecurity R&D Report

December 2012

The Society for Industrial and Applied Mathematics (SIAM), a 14,000-member organization representing applied mathematicians and computational scientists and engineers in all sectors, appreciates the opportunity to provide feedback on the Networking and Information Technology Research and Development (NITRD) Program's report, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*. Cybersecurity is an area of growing national concern, and the federal government must continue its strong emphasis on developing innovative R&D programs and initiatives to combat future cyber attacks.

To overcome the challenges of cybersecurity, we must be able to understand the dynamics of complex systems that make up our modern cyberinfrastructure. Understanding these systems will help mitigate risks, facilitate the development of controls and strategies to make systems more secure, and allow for the design of new tools.

Computational sciences and applied mathematics play a crucial role in understanding complex systems. Key tools that must be further developed include predictive modeling and simulation of complex systems, mathematical analysis of the behavior of complex systems, and using models of complex systems to inform policy makers. Specific challenges mentioned in the report where computational science and applied mathematics play a key role in understanding complex systems include:

- Methods for detecting flaws in software through static and dynamic analysis (p.5)
- Mathematically sound techniques to support combination of models and composition of results from separate components (p. 6)
- Least-privilege separation kernels to ensure separation and platform trust in untrustworthy environments (p.7)
- Data protection tools, access control management, and monitoring and compliance verification mechanisms to allow for informed trust of the entire transaction path (p.7)
- Develop abstractions and methods that will enable scientific reasoning regarding MT [Moving Target] mechanisms and their effectiveness (p.8)
- Understand the effect of randomization of individual components on the behavior of complex systems, with respect to both their resiliency and their ability to evade threats (p.9)
- Develop a control mechanism that can abstract the complexity of MT systems and enable sound, resilient system management (p.9)
- Enable the adaptation of MT mechanisms as the understanding of system behavior matures and our threat evolves (p.9)
- A control theory for maintaining security in the presence of partially successful attacks (p.11)
- Quantifiable, forward-looking security metrics (using formal and stochastic modeling methods) (p.12)

In conclusion, SIAM applauds the efforts of the federal agencies supporting cybersecurity R&D to combat cyber attacks and address the growing challenges in the field as well as NITRD's efforts to incorporate community feedback in shaping future cyber R&D initiatives. Basic research plays a key role in fostering the innovations and breakthroughs necessary to protect our nation's networks and infrastructure. Applied mathematics and computational sciences should continue to receive strong emphasis in developing the nation's future cybersecurity R&D portfolio.

January 11, 2012

Cyber Security and Information Assurance Research and Development Senior Steering Group (SSG), Federal Networking and Information Technology Research and Development (NITRD) Program

Via Email - cybersecurity@nitrd.gov

Re: Request for Comments (RFC)--Federal Cybersecurity Research and Development Strategic Plan, 77 FR 70483

To Whom It May Concern:

BSA | The Software Alliance appreciates this opportunity to provide comments concerning the report that the Cyber Security and Information Assurance Research and Development Senior Steering Group (SSG) of the Federal Networking and Information Technology Research and Development (NITRD) Program is working on relating to the 2011 Federal Cybersecurity Research and Development Strategic Plan. BSA | The Software Alliance is the leading advocate for the global software industry before governments and in the international marketplace. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life.

Support for a National Cybersecurity Research & Development Plan

BSA has long promoted the development of a national cybersecurity research and development (R&D) plan to harness innovation to improve cybersecurity. Our networks and electronic data are continually under attacks perpetrated by well-organized criminal elements and other entities that threaten our economic and national security. As these attacks are increasingly technologically sophisticated, we need to ensure that our technological defenses are as advanced, if not more.

A robust R&D plan is necessary to ensure cybersecurity, online confidence, and trust. BSA supports a global cybersecurity framework that not only promotes R&D but also addresses such critical policy areas such as consumer privacy, data breach, federal agencies'

Robert W. Holleyman, II
President and CEO

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

cybersecurity, software assurance, cybercrime, and critical infrastructure. Only by addressing these areas collectively can we ensure that businesses and users can use information tools and technology with confidence and trust.

We commend the SSG and NITRD for working to develop and implement the Federal Cybersecurity Research and Development Strategic Plan. With the development of this Plan, the SSG is addressing strategic cyberspace vulnerabilities through technological innovation, which is both a key tool in our efforts to secure cyberspace and a driver for fueling economic growth. The plan's forward looking approach of addressing underlying cybersecurity deficiencies, channeling expertise from a wide range of disciplines and sectors, and utilizing principles that stay current despite the fast-paced changing nature of technology is exactly the type of leadership that is needed from the government.

BSA has long maintained that a successful cybersecurity R&D plan must be created jointly by government and industry, identify national-level priorities, and include a strategy to reach these objectives. Such a plan must focus government resources on "game-changing" long-term and basic research and allow for any solutions developed through R&D to be transferred to and adopted quickly by the marketplace, both of which the current plan address to a limited extent. Only by working together at all stages of the R&D process can the government and private sector successfully meet the challenges of cybersecurity. We look forward to continuing to work with the SSG to strengthen our public-private partnership efforts.

The Role of the Private Sector in a National Cybersecurity Research & Development Plan

While BSA appreciates the efforts of the SSG in developing national-level cybersecurity R&D objectives, we believe that the overall process and implementation undertaken by the government to achieve these objectives should be strengthened. R&D provides a great understanding of weaknesses in systems and networks, as well as how to protect and make those systems resilient. While the strategic plan notes a role for the private sector, it may not necessarily take into account the extent of the industry's R&D efforts that often drive market solutions and meet the demand of both government and consumers. Page two of the plan, for example, states that "Government investment in basic research is essential because industry does not have the economic interest or return-on-investment time horizon to make such investments or conduct such research." It is true that the government plays an important role in cybersecurity R&D but, at the same time, the private sector has and will continue to make a significant investment in R&D to develop innovative solutions. The private sector's economic interests are very much tied to assuring that products, systems, and networks are secure and trustworthy for consumer, business, and government use.

As the entities that design, build, own, and operate the majority of software, systems, and networks, the private sector's role in helping set the federal R&D agenda from the onset and throughout its lifecycle can help assure that government spending and efforts in this area are not duplicative or contradictory to commercial efforts. In these economic times, helping the government focus its resources on R&D is critical. In particular, the government can play a key role in addressing measurable security gaps not currently being tackled by the private sector and commercially available technological solutions. Recently, the National Academies Press issued a report on "Continuing Innovation in Information Technology," which noted the complex ecosystem by which innovation takes place. As noted in the report:

> *The government role has coevolved with the development of IT industries: its programs and investments have focused on capabilities not ready for commercialization and on the new needs that emerged as commercial capabilities grew, both of which are moving targets.*

As this past experience on public-private partnership on innovation demonstrates, there is a close connection between successful innovation and the flow of people and ideas between stakeholders in industry, government, and academia.

As the SSG continues to roll out specific programs and projects in the cybersecurity R&D arena, BSA urges it to consider more fully tapping into and harnessing the capabilities of the private sector. Gathering input from the private sector and other stakeholders through this process is a good step, but more can be done to effectively develop a national cybersecurity R&D plan that recognizes the complex nature of current cybersecurity efforts among all stakeholders. We welcome the opportunity to work with the SSG to develop and implement a robust, collaborative, and established public-private partnership whose objectives reflect the broad needs of the nation, For all sections of the plan, including the evaluation of the four themes – Designed-In Security, Tailored Trustworthy Security, Moving Targets, and Cyber Economic Incentives – a more robust information-sharing and integrated approach, not only across agencies and academia, but with the private sector is critical to successfully tackling difficult technical, policy, and legal issues. Likewise, the private sector can help the federal government develop additional themes that reflect innovative changes and address the operational challenges we are seeing in our global businesses in a more systematic and meaningful manner.

Creating such a partnership will not only allow for the development of national level priorities, but also a strategy to reach these objectives, and focus government resources on "game-changing" long-term and basic research. This would be in furtherance of the NITRD's efforts to not only meet priorities of specific agencies, but the broad cybersecurity needs of the nation. BSA looks forward to continuing to work with the SSG in developing a

more integrated and collaborative approach to assuring that federal government and private sector cybersecurity R&D efforts are complementary.

Themes of the National Cybersecurity Research & Development Plan

The plans lays out the four themes designed to guide federal cybersecurity R&D priorities: Designed-In Security, Tailored Trustworthy Spaces, Moving Target, and Cyber Economic Incentives. The last three themes are not new to federal R&D efforts but are outgrowths of the National Cyber Leap Year activities of 2009, which brought together government, academia, and the private sector to look at game-changing concepts in cybersecurity. Continuing R&D efforts in those identified areas, including on the tracks laid out in the report, make sense so long as there is an accounting of private sector efforts, as discussed above. BSA supports efforts to meet cybersecurity R&D gaps in these areas.

The "Designed-in Security" theme is new and focuses on "designing and producing software systems that are resistant to attacks by dramatically reducing the number of exploitable flaws." This is an area in which BSA and its member companies have invested significant resources in recent years. There is no question that security has become a requirement for software companies as market forces, the need to protect critical infrastructures, and the need to build and preserve widespread trust in computing have become core components of cybersecurity efforts. Government agencies, businesses, and consumers are looking for ways to implement less burdensome and more cost-effective security management systems that rely less and less on patches and fixes to existing software systems.

The result of these demands is that the software industry has invested more in R&D and in the development of stringent software processes that focus on security. Doing so minimizes vulnerabilities on the front-end of the software development lifecycles. These developments allow companies to build better and more secure software that can meet variable metrics and accountability standards in both enterprise and consumer settings.

There is little question that more R&D is needed in this fledging space. More so than in other areas, however, there must be a close alliance between the private sector and the government in cybersecurity R&D efforts. Government and industry must work together to ensure that government procures secure software and hardware in a manner that takes into consideration the ever-evolving nature of IT developmental processes and how supply chain related requirements can affect these efforts. We would urge the SSG to develop a systematic approach to such a collaboration that does not unnecessarily burden or harm the innovative efforts happening in the private sector.

Robert W. Holleyman, II
President and CEO

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

In the request for comments, the SSG asks if there are other research areas and themes that should be included in the strategic plan. There are three areas in which we would encourage federal government R&D efforts be considered. The first involves the government's partnership with the private sector to counter software piracy, which cuts into innovation and job creation, lowers government tax revenues, and compromises the security of information technology systems worldwide, putting businesses, governments, and consumers at risk. While industry has and should continue to have the lead in developing technologies to address online content piracy in a voluntary manner, the government should consider R&D efforts that evaluate and ensure that legal offerings for digital content services are facilitated. Government's research on the best legal and policy solutions for addressing online content piracy should meet two objectives that support existing industry efforts:

1. To effectively deter illicit downloading, uploading, making available and use of content and,

2. To ensure existing technologies function as designed, that innovation and the development of new technologies and services are not obstructed, and that users' enjoyment of software, computers and the Internet is not diminished.

Specifically, an evaluation of how the prevalence of software piracy adversely affects national cybersecurity interests is merited. There is a lack of research in this area and the government is well-positioned to evaluate the technical, legal, and policy causes and implications of this issue. From the spread of malware to the integrity of the supply chain for critical systems, there is a need for additional R&D.

The second area that the SSG should consider exploring to future cybersecurity R&D efforts is how international efforts, especially relating to innovative technologies and advance innovation, impact the development of the U.S. cybersecurity efforts. In particular, R&D efforts documenting how international technical requirements, especially in growing emerging economies, affect American companies, create trade barriers, encourage the adoption of discriminatory public procurement practices, and affect the security of American products and services would assist the U.S. in understanding the growing global nature of interconnected and interdependent technologies.

Research in this area would be in furtherance of the *International Strategy for Cybersecurity* released last year, which called for the U.S. to work internationally to promote an open, interoperable, secure and reliable information and communications infrastructure. According to the Government Accountability Office, there were at least 19 global organizations in 2010 that significantly influenced the security and governance of cyberspace. Those groups ranged from non-decision-making information sharing forums to

treaty-based, decision-making governmental bodies. In the past year, additional groups, as well as individual countries, have started evaluating international standards and requirements in the cybersecurity space. The increasing number of global entities promulgating and implementing cybersecurity requirements and standards impacts the U.S. efforts on the cybersecurity and innovation front. An evaluation of how these activities influence the security and government of cyberspace, including a catalog of R&D efforts in the already developed theme areas, would be useful.

The third area in which BSA would encourage the government to focus R&D efforts involves the development of effective and useful metrics for measuring cyber-attacks. The development of metrics will allow the U.S. to quantify the scale and scope of cyber-attacks, a task that has been daunting to date. The development of effective metrics will allow for the improved identification of system vulnerabilities, weaknesses, and strengths, demonstrate effective security trends, and promote the reduction of cyber risks. Quite simply, metrics will allow for both industry and government to better understand the extent and nature of cyber-attacks and where to invest with regards to cybersecurity efforts.

If these areas are of interest, BSA would welcome the opportunity to come in and discuss in more detail how these potential themes can be developed into specific R&D themes.

Technology Transfer to the Marketplace/ Transition to Practice

BSA commends the plan's recognition of the need to accelerate transition of the "fruits of research into practice if federal cybersecurity R&D investments are to have significant, long-lasting impact" (Page 14). We agree that requiring research program to have transition plans developed at the front end of the R&D process so as to map the appropriate paths from research to commercialization can assure that R&D is fully utilized. We encourage the SSG in its report to assess how to better leverage public-private partnerships to facilitate the transition to the marketplace of technologies developed with federal cyber security R&D funding.

As it evaluates cross-cutting activities such as technology discovery, test and evaluation, and transition, adoption, and commercialization as part of is Accelerating Transition to Practice activities, we encourage the SSG to also evaluate what barriers exist to successful technology transfer. For example, BSA encourages the SSG to evaluate whether the status of the intellectual property generated by federally-funded cyber security R&D needs to be clarified. The strategic plan stated that "government-funded R&D programs should consider how to best reward government program managers and principal investigators for making measurable progress" in accelerating technology transfer (page 16). The SSG may want to evaluate whether a more systematic approach to a reward system is needed,

including possibly considering licensing conditions for innovation developed by specific agencies.

In addition, the role that education and workforce plays in the effective transfer of innovation is an area that the SSG may want to highlight. The plan references in its Maximizing Research Impact section the role that the National Initiative for Cybersecurity Education (NICE) plays in enhancing the United States' cybersecurity posture by accelerating the availability of educational and training resources. BSA supports this emphasis on cybersecurity education but believes it can be expanded to assist in advancing the government's technology transfer efforts. Effective transfer of innovation into existing or new commercial systems, as we have seen in the private sector, often depends on the flow of people, whether senior executives or graduate students. BSA believes that NICE's work to broaden the pool of individuals preparing to enter the cybersecurity workforce, including expanding access to computer science in K-12 and the strength and capacity of computer science and cybersecurity education in higher education, can help transition to practice efforts.

Conclusion

BSA thanks the SSG for the opportunity to offer input into its report on the 2011 Federal Cybersecurity R&D Plan. We look forward to working with the SSG in the future. Please do not hesitate to contact Tim Molino, Director, Government Relations, at policy@bsa.org with any questions or concerns.

Sincerely,

Robert Holleyman

Robert W. Holleyman, II
President and CEO

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org