November 1, 2016

Cybersecurity Research and Development Recommendations for the 45th President of the United States

Provided by ICF Cybersecurity and Resilience and the CyberSci 2016 Cybersecurity Research and Development Symposium

Contents

Introduction

This document conveys summary recommendations to the 45th President of the United States concerning cybersecurity research and development (R&D). The recommendations are the result of presentations given and panel discussions that took place during the CyberSci 2016 Cybersecurity Research and Development Symposium, October 27, 2016, at ICF. Samuel S. Visner, ICF Senior Vice President for Cybersecurity and Resilience, and Professor, Cybersecurity Policy, Operations, and Technology, Georgetown University, chaired the event. A more fully elaborated set of recommendations will be published as part of the symposium's proceedings. The symposium's agenda is provided as an appendix to this document.

The symposium comprised these panels:

- Cybersecurity and Privacy
- The Future of Cyber Operations and Technologies
- Beyond the Government: Mobilizing Industry and Academia

Technical presentations were organized in these tracks:

- Cybersecurity in the Service of National Security
- Securing the Emerging National Smart Infrastructure
- Cybersecurity and the Social Network

Technical track presentations were selected through anonymous peer review. Presentations ranged from improving cybersecurity analysis and protecting cyber systems from electromagnetic pulse to developing cybersecurity R&D funding strategies.

The following recommendations are the opinions of ICF and not necessarily those of individual CyberSci 2016 panelists and presenters. They reflect whole-of-nation cybersecurity R&D concerns rather than specific R&D efforts or cybersecurity technologies.

General Observations

The cybersecurity R&D establishment of the United States covers a broad range of disciplines with deep and substantial resources invested in many areas vital to the nation's protection. Important work is underway to characterize the behavior of complex networks, including those that serve the nation's critical infrastructures, which are managed increasingly by information technology (IT). These "smart" infrastructures reflect the continuing interconnection of "traditional" enterprise IT systems and the Internet of Things—the system of interrelated Internet Protocol-enabled devices from which we can extract important data and through which we manage these infrastructures.

Impressive research also is under way to detect anomalous behavior in such complex networks as well as to detect, block, and mitigate advanced cyber threats—including threats without known signatures. Researchers are probing the vulnerability of our cyber systems—including critical infrastructures—to electromagnetic pulse. Other researchers are examining the links between threats to cybersecurity and the use of social networking tools.

The range of organizations involved in cybersecurity research is impressive. Cybersecurity R&D is being conducted by the U.S. Department of Defense (DoD)—including the Army Research Laboratory, Navy Research Laboratory, Air Force Research Laboratory, Defense Advanced Research Projects Agency, and the Cybersecurity Information Analysis Center of the Defense Technical Information Center—the U.S. Department of Energy's (DOE) National Laboratories, federally funded R&D centers (e.g., the Software Engineering Institute and MITRE), National Institute of Standards and Technology, various universities, and numerous private sector companies specializing in cybersecurity products and technology. Published in February 2016, the *Federal Government Cybersecurity Research and Development Strategic Plan* "establish[ed] the direction for the Federal R&D enterprise in cybersecurity science and technology (S&T) to preserve and expand the Internet's wide-ranging benefits …"[1] The plan challenges the federal government to lay out cybersecurity R&D priorities for the government's own resources.

At the same time, national cybersecurity R&D efforts remain unfocused. A national cybersecurity R&D community has yet to be defined. National cybersecurity challenges beyond those discussed at a high level in the aforementioned strategic plan should be identified. Also needing definition is a concept of operations to coordinate nationally the efforts of organizations engaged in cybersecurity R&D activity. At the highest level of abstraction, cybersecurity R&D goals have not been coupled tangibly to expressions of the national interest or to the nation's security, defense, and homeland security strategies. This year's CyberSci symposium reflected cross-sector acceptance of cyber threats as pervasive and permanent, making the establishment of foundational support from the White House more important than ever.

Recommendation 1: Connect Cybersecurity R&D to National Technology Development.

Cybersecurity technology and practice are not keeping pace with advances in the IT infrastructures we must safeguard. Advances in information technology are relentless, providing our nation with global competitive advantage. Creating faster, more agile cybersecurity technology synchronized with advances in IT is vital.

[1] National Science and Technology Council, *Federal Cybersecurity Research and Development Strategic Plan*, accessed October 20, 2016, at https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf.

The advance of technology in general throughout our nation's infrastructure is one of the hallmarks of national progress. Information technology is being called upon increasingly to manage transportation, energy, communication, manufacturing, and other infrastructures. Increased use and complexity are likely also to amplify vulnerabilities. However, the advance of technologies used throughout the nation has not been accompanied, necessarily, by commensurate advances in the cybersecurity technologies employed to protect our infrastructures. A tighter coupling of the technology development overall with the nation's approach to cybersecurity R&D would result in national infrastructures that are more secure and resilient.

The connection between such R&D efforts is possible. DOE's National Laboratories are participating collectively in a grid modernization consortium. According to the department, "By coupling headquarters collaboration with the strengths of the labs—in areas including their tremendous computational abilities, knowledge of cybersecurity systems [emphasis added], integration of renewable and energy efficient technologies, and command of sensing and control technologies—the Consortium will tackle the challenges associated with achieving a modern grid that will make a clean energy future possible."[2] The consortium is serving as the vehicle to synchronize the development of the "smart grid" with the cybersecurity technologies necessary to protect it. This approach exemplifies what should be done nationally for every infrastructure sector and for every aspect of the national economy on which we depend for our national, homeland, and economic security.[3]

Recommendation 2: Define a National Cybersecurity R&D Community.

The cybersecurity challenges facing the United States are vast and complex. Addressing them will require a whole-of-nation approach to the development and application of requisite cybersecurity capabilities. The next President should define carefully the national cybersecurity R&D community to ensure that all needed resources are applied and that efforts can be coordinated and effective.

Although an impressive range of enterprise is engaged in cybersecurity research, coordination of efforts awaits definition of the national cybersecurity R&D community. Defining a community that echoes the approach taken in post-WWII years to define R&D communities for nuclear energy and aerospace technology would improve collaboration, enable the synchronization of efforts to address specific cybersecurity R&D challenges, and illuminate progress against those challenges.

[2] U.S. Department of Energy, energy.gov, Launch of the Grid Modernization Laboratory Consortium, accessed October 20, 2016, from http://energy.gov/articles/launch-grid-modernization-laboratory-consortium.

[3] Congressman Ruben Gallego expressed his support for reaching across sectors as the new approach needed to address the cyber threats that are growing rapidly in tandem with technological advances.

Such a community would be well served by national-level leadership, possibly at the level of the White House and potentially informed by a National Cybersecurity Advisory Committee to the President. The formal creation of a cybersecurity R&D community supported by such an advisory committee would elevate the importance of cybersecurity in general and also could improve recruitment of some of the nation's best minds to the various cybersecurity R&D disciplines.[4]

Recommendation 3: Define National Cybersecurity R&D Challenges.
Choosing cybersecurity R&D challenges that deserve priority attention by the national cybersecurity R&D community is more important than ever, given the challenges that exist to our critical infrastructures, intellectual property, and personal information. The effective allocation and coordination of vital R&D resources will depend on astute choices by the next President.

Creation of a national cybersecurity R&D community can be followed swiftly by definition of national cybersecurity R&D challenges for the community to address. Initial challenges can be derived from the *Federal Government Cybersecurity Research and Development Strategic Plan*[5] but should go beyond the plan to identify challenges associated with smart infrastructures—the IT-mediated management of infrastructures (e.g., energy and transportation) —and the needs of cybersecurity operators within DOD and the Intelligence Community. National-level cybersecurity challenges also should include securing our financial system, because crypto-currencies and global trading are increasingly important realities. Other challenges should be defined and prioritized, including those necessary to secure medical devices and medical information, protect vital intellectual property, and defend our critical infrastructures from the well-orchestrated computer network attacks of nation-state adversaries.[6]

Recommendation 4: Enable Cybersecurity R&D Information Sharing.
Development of an effective national cybersecurity R&D community will pose the significant challenge of sharing important information quickly and securely. Although an existing Presidential Executive Order calls for stronger information sharing, efforts to build a national cybersecurity R&D information-sharing architecture should be formalized and accelerated.

[4] In the CyberSci panel discussion Beyond Government: *Mobilizing Industry and Academia*, Dr. Alexander Kott of the Army Research Laboratory pointed out that our nation's higher education and private industry help define what makes us truly great but that we do not take sufficient advantage of these resources. Dr. David Honey of the Office of the Director of National Intelligence noted that as the work of industry, government, and academia move to the cloud, we are gaining new opportunities for collaboration.

[5] National Science and Technology Council, op. cit.

[6] A theme that echoed from CyberSci was the importance of understanding our adversaries' values and behavioral norms as a research and development priority, alongside more traditional technology-oriented priorities.

The development of a national cybersecurity R&D community and the definition of national cybersecurity R&D goals should be enabled with strong information-sharing mechanisms.[7] The Presidential Executive Order of February 12, 2015, calls for improved private-sector information sharing.[8] The order defines information-sharing and advisory organizations (ISAOs) at a high level. Such ISAOs can promote swift, efficient, and transparent information sharing for specific cybersecurity challenges (e.g., industrial control systems and smart infrastructures). ISAOs can complement existing, industry-specific information-sharing and analysis centers and can be the vehicle to improve nationwide information sharing and collaboration for cybersecurity R&D. An effort is under way at the Intelligence and National Security Alliance's Cyber Research and Development Sub-Council to define such a cybersecurity R&D ISAO.[9] The sub-council's work should enjoy the support of the White House in general, and of the Office of Science and Technology Policy in particular.

Recommendation 5: Understand and Address Through R&D the Cybersecurity Technology Challenges Posed by Privacy.

Our Constitution's Fourth Amendment represents a cornerstone of our freedoms. R&D for the creation of new cybersecurity technologies should serve to enhance our protections rather than treat national cybersecurity and privacy as conflicting imperatives.

National concerns endure about the privacy of information used to safeguard the nation. The United States, with approximately 5% of the world's population, will continue to host and provide transit for a disproportionate amount of all Internet and telephony traffic. Our Intelligence Community will need to conduct intelligence operations, including computer network exploitation, in an environment where foreign target communications transit the nation, targets of interest may communicate with U.S. persons, and national security and law enforcement concerns will overlap. Cybersecurity R&D activities should reflect cognition of these challenges, looking for ways to adhere to the protections afforded by the Fourth Amendment to the U.S. Constitution and ensuring that the search for vital intelligence does not become fixed surveillance of U.S. persons so protected. This challenge remains difficult. A January 2015 report from the National Academies notes that "no software-based technique can fully replace the bulk collection

[7] Congressman Gallego noted that "cyber" is not owned by anyone, though it is used by everyone. Although discussions continue about where cyber "belongs," technology speeds along without the benefit of the best information available by those in our country who need it. Dr. Kott noted that we should not miss opportunities to share with and learn from our country's allies and partners.

[8] The White House, "FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing," February 12, 2015, accessed October 20, 2016, from https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform.

[9] Intelligence and National Security Alliance's Cyber Research and Development Sub-Council, accessed October 20, 2016 from http://www.insaonline.org/i/c/cyber/c/index.aspx.

of signals intelligence, but methods can be developed to more effectively conduct targeted collection and to control the usage of collected data."[10] The development of these methods must respect the protections afforded by the Fourth Amendment and should be regarded as a cybersecurity R&D requirement of special importance.[11]

Conclusion

The CyberSci 2016 Symposium made clear the need to mobilize academia and the private sector more strongly in support of cybersecurity research and development. It also brought into sharp focus the need to build cybersecurity technologies and capabilities that do not offend our national values or impinge on our legal protections. The creation of a national cybersecurity R&D community and the definition of appropriate national cybersecurity R&D challenges—coupled with an understanding of the role cybersecurity R&D should play in support of national technology development—would signify important steps toward addressing a national imperative. The next administration has the opportunity to play a pivotal role in the way our country addresses the serious challenges posed by cybersecurity. We hope these recommendations will well serve the 45th President of the United States in doing so.

About ICF

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with more than 5,000 professionals focused on making big things possible for our clients. We are business analysts, policy specialists, technologists, researchers, digital strategists, social scientists and creatives. Since 1969, government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success. Come engage with us at **icf.com**.

[10] National Academies of Sciences, Engineering, and Medicine, National Research Council, "New Report Says No Technological Replacement Exists for Bulk Data Collection; Software Can Enhance Targeted Collection and Automate Control of Data Usage to Protect Privacy," accessed January 15, 2015 from http://www8.nationalacademies.org/onpinews/newsitem.aspx?recordid=19414.

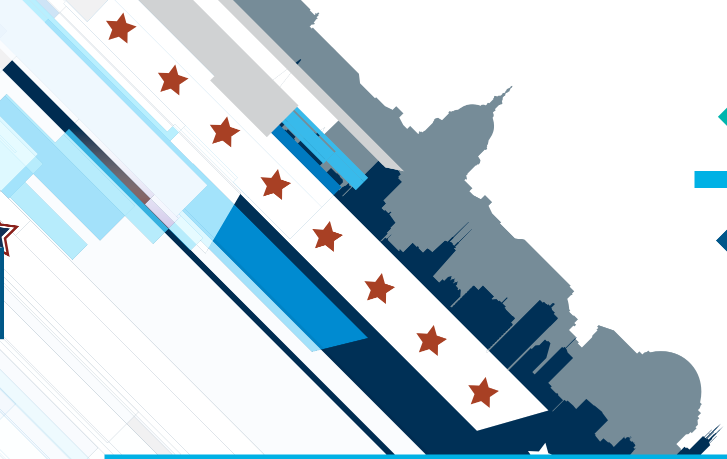
[11] CyberSci's Cybersecurity and Privacy panel of experts analyzed this multifaceted issue, which is complicated by the amount of data becoming available and the value of that data for governmental and commercial decision-making. The panel stressed our country's growing cybersecurity exposure resulting from the proliferation of unsecure software through the Internet of Things and discussed encryption, consumer education, and segmentation as possible components of an approach to improving cybersecurity while preserving privacy.

For more information, contact:

Samuel S. Visner
samuel.visner@icf.com +1.703.225.5860

facebook.com/ThisIsICF/
twitter.com/ICF
youtube.com/icfinternational
plus.google.com/+icfinternational
linkedin.com/company/icf-international
instagram.com/thisisicf/

CyberSci symposium 2016



ICF

Thursday, October 27
ICF Conference Center, Fairfax, VA

Agenda

8:00 a.m.–8:45 a.m.	**Registration/Breakfast**
8:45 a.m.–9:00 a.m.	**Opening Remarks** **Sudhakar Kesavan,** ICF Chairman and Chief Executive Officer
9:00 a.m.–9:30 a.m.	**Keynote Address: The Internet of Battle Things** **Dr. Alexander Kott,** Network Science Division Chief, U.S. Army Research Laboratory
9:30 a.m.–10:30 a.m.	**Panel: Cybersecurity and Privacy** **Panelists:** **Mark Weatherford,** former Department of Homeland Security Deputy Under Secretary for Cybersecurity **The Honorable Patricia Hoffman,** Assistant Secretary of Energy for Electricity Delivery and Energy Reliability **Dr. Peter Eckersley,** Chief Computer Scientist, Electronic Frontier Foundation **Moderator: Samuel S. Visner,** ICF Senior Vice President/General Manager for Cybersecurity and Resilience This panel will highlight the R&D challenges associated with enhancing and sustaining cybersecurity in support of national policy objectives while respecting privacy and civil liberty concerns. Discussions will include civil liberties protection and the Fourth Amendment of the U.S. Constitution, encryption as it relates to civil liberties and national security, and the evolution of U.S. policy regarding the cybersecurity and privacy of the global information commons.
10:35 a.m.–10:45 a.m.	**Networking Break**
10:45 a.m.–11:45 a.m.	**Panel: The Future of Cyber Operations and Technologies** **Panelists:** **Lieutenant Colonel Paul Rozumski,** U.S. Air Force **Christian Thomasson,** U.S. Air Force **First Lieutenant Francis V Adkins,** U.S. Air Force **First Lieutenant Val Red,** U.S. Air Force **Moderator: Captain Daniel Stambovsky,** U.S. Air Force Based on the recently released book entitled *Evolution of Cyber Technologies and Operations to 2035*, this panel will explore the future of cyber technologies and cyber operations which will influence advances in social media, cybersecurity, cyber physical systems, ethics, law, media, economics, infrastructure, military operations, and other elements of societal interaction in the upcoming decades.
11:45 a.m.–12:15 p.m.	**Keynote Address** **Congressman Ruben Gallego,** Arizona (D) House of Representatives, member of the House Armed Services Committee
12:15 p.m.–1:00 p.m.	**Networking Lunch**

1:00 p.m.–1:30 p.m.

Keynote Address: Russia, Putin, Hacks, Elections… Where to go from here?

General Michael Hayden, retired four-star general, former Director of the CIA and National Security Agency

	CONFERENCE ROOM A	CONFERENCE ROOM B	AUDITORIUM
1:40 p.m.–2:10 p.m.	**Recent Developments in Linkography Based Cybersecurity** **Dr. Robert Mitchell,** Sandia National Laboratories *Track: Securing the Emerging National Smart Infrastructure*	**Value-of-Information (VoI) Sensitive Cyber Sensor** **Steven Hutchinson,** ICF **Jason Ellis,** ICF *Track: Cybersecurity in the Service of National Security*	**Cybersecurity Risks in the Industrial Internet of Things** **Dan Sullivan,** Raytheon **Dr. Ed Colbert,** U.S. Army Research Laboratory *Track: Securing the Emerging National Smart Infrastructure*
2:15 p.m.–2:45 p.m.	**The Use of Entropy in Lossy Network Traffic Compression for Network Intrusion Detection Applications** **Sidney "Chuck" Smith,** U.S. Army Research Laboratory *Track: Cybersecurity in the Service of National Security*	**Securing Cyber-Physical Systems** **Dr. Dhananjay Phatak,** University of Maryland, Baltimore County *Track: Securing the Emerging National Smart Infrastructure*	**Cyber and Intelligence Research and Development Funding Strategy** **Dr. Edmund Mitchell,** CSIOS Corporation *Track: Cybersecurity in the Service of National Security*

2:45 p.m.–3:00 p.m. **Networking Break**

	CONFERENCE ROOM A	CONFERENCE ROOM B	AUDITORIUM
3:00 p.m.–3:30 p.m.	**Ransomware Over the Past 5 Years: Overview and Best Practices** **Timothy Obenshain,** ICF *Track: Cybersecurity in the Service of National Security*	**Social Networking Tools May Accidentally Increase Insider Threat: The Unintended Psycho-Social Effects on False Positive Indicators of Insider Threat** **Dr. Jennifer Cowley,** CERT/Software Engineering Institute/Carnegie Mellon University *Track: Cybersecurity and the Social Network*	**A Data-Stream Classification System for the Investigation of Terrorist Threats** **Era Vuksani,** Massachusetts Institute of Technology Lincoln Laboratory *Track: Cybersecurity in the Service of National Security*
3:35 p.m.–4:05 p.m.	**Collateral Effect Potential Metric for Computer Exploits** **Giorgio Bertoli,** Aberdeen Proving Ground, Maryland *Track: Cybersecurity in the Service of National Security*	**Protecting the US Infrastructure from Attacks via EED** **Tim Cash and John Link,** The Lever Group *Track: Cybersecurity in the Service of National Security*	**Modeling, Simulation, and Analysis of a Social Media Propaganda Network: The Case of ISIS/ISIL/Daesh** **Joseph Shaheen,** NATO STRATCOM COE and George Mason University *Track: Cybersecurity and the Social Network*

4:10 p.m.–5:10 p.m.

Panel: Beyond the Government: Mobilizing Industry and Academia

Panelists:

Dr. David Honey, Director, Science and Technology, and Assistant Deputy Director of National Intelligence for Science and Technology
Dr. Misty Blowers, ICF Vice President, Cybersecurity Research Programs
Dr. Alexander Kott, Network Science Division Chief, U.S. Army Research Laboratory
Dr. Douglas Maughan, Director of the Cyber Security Division, Homeland Security Advanced Research Projects Agency, Department of Homeland Security

Moderator: John Paczkowski, ICF Senior Vice President

This panel will examine ways to build a national cybersecurity research and development community, establish cybersecurity research and development priorities, and mobilize resources throughout the private sector and academia in support of national cybersecurity needs and policy requirements.

5:10 p.m.–5:45 p.m.

Presentation and Closing Remarks: The Cybersecurity Storm Front—Forces Shaping the Cybersecurity Landscape

Samuel S. Visner, ICF Senior Vice President/General Manager for Cybersecurity and Resilience

5:45 p.m.–7:00 p.m. **Networking Reception**