CSIA RFI Responses, January 15, 2019

Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

ISACA Response to Request for Information on Update to the 2016 Federal Cybersecurity Research and Development (R&D) Strategic Plan

Document Citation: 83 FR 56378
Document Number: 2018-24668
Agency/Docket Number: 180821780-8780-01

ISACA, on behalf of its nearly 60,000 information and cyber security professionals in the United States and its global community of nearly 140,000 professionals, is grateful for the opportunity to respond to the National Science Foundation's National Coordination Office for Networking and Information Technology Research and Development (NITRD) request for information in advance of the 2019 update of the Federal cybersecurity R&D strategic plan.

This request for information is both timely and welcome. While strategic efforts within the Federal government's cybersecurity R&D efforts have been exemplary thus far, there are several elements that ISACA believes deserve additional attention and potential action as NITRD considers the Federal government's cybersecurity R&D strategic plan in 2019. ISACA believes that, while all these questions will provide valuable feedback to NITRD, our organization can best provide insights and information on questions 1, 3, and 4:

1. What innovative, transformational technologies have the potential to greatly enhance the security, reliability, resiliency, and trustworthiness of the digital infrastructure, and to protect consumer privacy?

The five emerging technologies focused on in the 2016 plan (cyber-physical systems and the Internet of Things, cloud computing, high-performance computing, autonomous systems, and mobile devices) remain technologies to watch. Additional innovative and transformative technologies that bear consideration include blockchain, biometrics, artificial intelligence and machine learning, as well as quantum computing and encryption.

Blockchain has the potential to change—and enhance—the methods through which transactions occur securely. However, it would be a mistake not to note that blockchain, from a security perspective, still requires maturity; banking institutions, for example, still maintain significant concerns regarding the cryptographic algorithms securing blockchains and other distributed ledger technologies.

Like blockchain, biometrics must also mature from a security perspective. There are still significant issues to be worked out regarding security, trust, and data storage. Successful use of biometrics could be a boon to the overall reliability, resiliency, and trustworthiness of the digital infrastructure. However, it would be appropriate to consider the lessons learned from India's Aadhaar initiative, the largest biometric identification project in the world thus far; there have been concerns regarding the creation of such a massive database as a potential target for bad actors, as well as concerns regarding misuse or abuse by those in power. Biometrics, however, provide a level security above and beyond current methods; biometrics can't be lost or stolen (unlike

tokens) and can't be forgotten (unlike passwords). When the security and trust questions surrounding biometrics can be answered, it could become an exceptional protector of consumer privacy.

Artificial intelligence and machine learning (AI/ML) have the potential to reshape automated response within information and cyber security efforts, thereby strengthening and enhancing the overall resilience of our digital infrastructure and providing increased privacy protection for consumers. Though more distant in the future, quantum computing and encryption (QC/E) have the potential for even greater impact than AI/ML. For AI/ML and QC/E, however, it is critical that their potential as assets to improve security, reliability and resiliency are optimized first; ISACA believes this to be critical to the Federal government's efforts to protect the privacy of its' citizenry's data going forward.

In the "autonomous systems" section of the 2016 plan, the convergence of technologies was only glancingly discussed. ISACA believes that the 2019 updates provide an opportunity to examine technology convergence more closely. In our organization's considered opinion, emerging discrete technologies will provide increased opportunities for enhancing overall security and privacy efforts, but the synergies derived from the combinations of multiple converging technologies will provide even greater opportunities for improving overall cybersecurity. Though such synergies may be yet unrealized, they nevertheless warrant discussion and consideration going forward; the best time to prepare to meet new challenges is always prior to their arrival.

3. What areas of research or topics of the 2016 Strategic Plan should continue to be a priority for federally funded research and require continued Federal R&D investments?

The Internet of things (IoT), cloud computing, autonomous systems, and mobile devices should all continue to be technologies that cybersecurity research and development focus on.

IoT technology is being deployed across many major industries and security is a major component for IoT success.

Cloud computing has grown exponentially since 2016 and will continue to grow as corporations develop hybrid cloud solutions that host their mission critical systems.

Autonomous system technology continues to develop and will be applied across many sectors in the years to come. Security of autonomous systems is essential to public safety and should be a continued focus for research and development.

Mobile devices continue to grow as the endpoint of choice for users. Securing mobile devices will always be critical to enterprise success and should be a continued focus of research and development.

Risk management across the entire cybersecurity spectrum should always be a major focus for the Federal Cybersecurity Research and Development Strategic Plan.

4. What challenges or objectives not included in the 2016 Strategic Plan should be strategic priorities for federally funded R&D in cybersecurity? Discuss what new capabilities would be desired, what objectives should guide such research, and why those capabilities and objectives should be strategic priorities.

The 2016 Cybersecurity Research and Development Strategic Plan appropriately emphasizes the importance of application developers building new systems with needed security controls. However, the plan does not offer specifics about what should be done during the systems development lifecycle to ensure that new systems are built securely. The plan should emphasize initiatives such as the Open Web Application Security Program (OWASP) and the National Institute of Standards and Technology (NIST) Special Publications 160 – Systems Security Engineering, an Integrated Approach to Building Trustworthy Resilient Systems. The OWASP and NIST programs offer specific approaches to secure systems development that can be leveraged in the NSF research and development.

Thank you again for this opportunity for ISACA to respond to the National Science Foundation's National Coordination Office for Networking and Information Technology Research and Development (NITRD) request for information in advance of the 2019 update of the Federal cybersecurity R&D strategic plan. ISACA looks forward to continuing to work with the Foundation and the Federal government on cybersecurity issues and concerns in the years ahead.