Tomas Vagoun
NCO/NITRD

December 17, 2018

Thank you for keeping the federal cybersecurity R&D strategic plan current and relevant by seeking input from the public, industry, and subject matter experts.

Taproot Security is a private firm advising clients and policymakers on vital cybersecurity matters. I have worked in the past helping NSF and DHS evaluate cybersecurity grant applications from academia, and I collaborated with White House cybersecurity advisor Howard Schmidt during the Obama administration. I also help private sector firms with cybersecurity research, inventions, and patents.

I appreciate this opportunity to respond to your RFI questions:

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?

Artificial Intelligence (esp. Machine Learning) has broad potential to improve detective controls by identifying more anomalies automatically while reporting fewer manually, thereby increasing true positives and reducing false positives. Natural language processing (NLP) combined with intel sharing schemas (e.g., STIIX/TAXI) can facilitate dissemination and monitoring of security incidents, thereby promoting sharing among private and public sector entities.

2. What progress has been made against the goals of the 2016 Federal Cybersecurity R&D Strategic Plan? Are there mature private-sector solutions that address the deficiencies raised in the 2016 Strategic Plan? What areas of research or topics of the 2016 Strategic Plan no longer need to be prioritized for federally funded basic research?

None of the 2016 goals has been satisfactorily met and all remain important. In particular, security operations (fusion centers, SOCs, ISACs, etc.) continue to over rely on manual procedures and methods that could be automated / smartened in order to better scale up against the rising daily volume of asymmetric threats. Tools to enable more reliable attack attribution are also still lacking.

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?

Transition to practice remains the biggest reason why the R&D community has not met the 2016 strategic goals and objectives. The R&D community (esp. academia) is primarily incented to publish papers and obtain grants, not necessarily to make practical solutions operational or even to understand the needs of the operational community. Federal agencies (e.g., NSF) can play a role in bridging this gap by aligning R&D goals to operational needs and by including explicit transition to practice outcome requirements in grants and RFPs.

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.

A greater emphasis on Internet of Things (IoT), Artificial Intelligence (AI), public cloud security, supply chain risk, and nation state adversaries than was needed in 2016 is now necessary given today's threat landscape. Some of these were discussed as Emerging Technologies in the 2016 strategy, but today they are mainstream and no longer emergent.

5. What changes to cybersecurity education and workforce development, at all levels of education, should be considered to prepare students, faculty, and the workforce in the next decade for emerging cybersecurity challenges, such as the implications of artificial intelligence, quantum computing, and the Internet of Things on cybersecurity?

Basic cybersecurity hygiene should be taught to everyone starting from an early age. As for addressing chronic shortages in US cybersecurity workforce, high schools and universities need help creating programs that attract/recruit a diverse population of students and teach them the right skills. Federal agencies (e.g., Dept of Education) can play a helpful role incenting school administrations and teaching faculties how to construct a successful program.

6. What other research and development strategies, plans, or activities, domestic or in other countries, should inform the U.S. Federal cybersecurity R&D strategic plan?

NIST of course has done important work with its cybersecurity framework (CSF) and other cyber standards that should inform the R&D strategy. DHS has built useful partnerships in the past with academia (e.g., I3P) for steering federal grant dollars. US standards bodies that work intensively on cybersecurity (ASC X9, IETF, W3C, etc.) should be invited to provide input, as should industry security associations (ISSA, ISC2) and sector specific think tanks (e.g., BITS).

Thank you for this opportunity to share our perspective on cybersecurity R&D priorities.

Sincerely,

Michael McCormick
President, Taproot Security
www.taprootsecurity.com
mike@taprootsecurity.com