March 14, 2023

COMMENTS IN RESPONSE TO JOINT NITRD/NSF REQUEST FOR INFORMATION ON THE 2023 FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN[1]

ACM, the Association for Computing Machinery, is the world's largest and longest established association of computing professionals, representing approximately 50,000 individuals in the United States and more than 100,000 worldwide. ACM is a non-profit, non-lobbying and non-political organization whose U.S. Technology Policy Committee ("USTPC") is charged with providing policy and law makers throughout government with timely, substantive, and apolitical input on computing technology, and the legal and social issues to which it gives rise. Consistent with that charge, USTPC is pleased to submit these comments in response to the recent *Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan* issued jointly by the Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO) and the National Science Foundation (NSF).[2]

General Recommendations

With regard to the overall structure of the proposed strategy, USTPC recommends eliminating "Deter" as a separate category of Defensive Element. We do so because "Deter" seems dissimilar to its present companion elements: "Protect," "Detect," and "Respond." Specifically, we note that deterrence can be achieved in many ways: through protective measures that are strong enough to make successful attacks prohibitively expensive, through certainty of attribution and (possibly political or military) response, or through reducing the likelihood of gain from a particular attack by dispersing or encrypting resources. All of these means (with the possible exception of political or military responses) easily fit into the other elements listed. Including "Deter" as a separate defensive category thus seems inaccurate.

---

[1] The principal author of these comments for USTPC was Security Subcommittee Co-Chair Carl Landwehr with significant contribution from USTPC members Arnon Rosenthal and Gene Spafford.

[2] 88 FR 7999 (February 7, 2023), Document Number 2023-02578 [https://www.federalregister.gov/documents/2023/02/07/2023-02578/request-for-information-on-the-2023-federal-cybersecurity-research-and-development-strategic-plan] as modified at 88 FR 10552 (February 21, 2023) by Document Number 2023-03557 [https://www.federalregister.gov/documents/2023/02/21/2023-03557/request-for-information-on-the-2023-federal-cybersecurity-research-and-development-strategic-plan].

Question-Specific Responses

1. What new innovations have the potential to greatly enhance the security, reliability, resiliency, trustworthiness, and privacy protections of the digital ecosystem (including but not limited to data, computing, networks, cyber-physical systems, and participating entities such as people and organizations)?

USTPC believes that all of the following have the potential identified in this question:

- Innovations in the tools and techniques for rigorously defining design requirements for software, hardware, and data – and for assuring that those requirements are correctly implemented – have significant potential for enhancing the security and trustworthiness of critical components of the digital ecosystem;

- Developments in the organization and mechanization of assurance arguments for complex systems hold promise for improving safety, resiliency, and security of those systems;

- Advances in machine learning, and more generally in artificial intelligence, have the potential to improve systems in many ways. At the same time, however, they may enhance attacker capabilities and make systems less predictable if used inappropriately;

- Innovations in secure hardware and firmware, particularly in the security properties of chip architectures, may enable creation of systems that are more resistant to attack. Techniques for making systems more agile may help them adapt quickly, *i.e.*, increase resiliency; and

- Homomorphic encryption is becoming practical in limited domains. In the next decade advances in this area could lead to significant improvements in both privacy and security.

2. Are there mature solutions in the marketplace that address the deficiencies raised in the 2019 Strategic Plan? What areas of research or topics of the 2019 Strategic Plan no longer need to be prioritized for federally funded basic and applied research?

- No. Although the marketplace for defensive measures and resilient systems continues to expand, no specific areas highlighted in the 2019 plan are yet sufficiently mature and stable to discourage research funding.

3. What areas of research or topics of the 2019 Strategic Plan should continue to be a priority for federally funded research and require continued Federal R&D investments?

- The 2019 strategy lists six priority areas: artificial intelligence, quantum information science, trustworthy distributed digital infrastructure, privacy, secure hardware and software, and education and workforce development. All these areas continue to merit research investment; and

- Since the 2019 strategy was issued, the effects of artificial intelligence, machine learning, and large language models on critical systems and applications have become even more prominent. Research managers should give priority to research into the dependability and security of systems that both incorporate, and also might be attacked using, these same technologies.

4. What objectives not included in the 2019 Strategic Plan should be strategic priorities for federally funded R&D in cybersecurity? Discuss the challenges, desired capabilities and outcomes, and objectives that should guide research to achieve the desired capabilities, and why those capabilities and outcomes should be strategic priorities for federally funded R&D.

- The recently issued National Cybersecurity Strategy appropriately focuses on long term improvements in critical infrastructures by incentivizing developers to produce systems with fewer built-in vulnerabilities.
    - Research priority should be given to technologies and development processes that will assist developers in producing such systems; and
    - Open-source software has been a pillar of system development for decades and the emergence of AI-assisted programming opens an even wider path for non-proprietary, non-classically engineered software development. Research on tools and techniques that will enable rigorous assessment of non-classically engineered software to minimize vulnerabilities and protect against malicious alteration upon its deployment should be prioritized.
- The strategy does not, however, adequately consider data.
    - The security, privacy, and provenance of data held in repositories such as data lakes, data warehouses, data lake houses, and in operational systems need further research. Conventional digital signatures are not routinely used for data authentication or provenance. A new generation of data managers (*e.g.*, log-based delta tables) may be more amenable to their use. Further, research may be needed to make applications sensitive to the characteristics of the data they process, for example to check whether input data was compromised or of low quality; and
    - Techniques for providing resiliency when a data source has been found to be compromised deserve investigation. Conventional practice connects applications to sources chosen in advance, known at build time (*e.g.*, authoritative sources), and chosen for large datasets. Research is needed into techniques that provide resiliency without imposing these constraints.

5. What other scientific, technological, economic, legal, or societal changes and developments occurring now or in the foreseeable future have the potential to significantly disrupt our abilities to secure the digital ecosystem and make it resilient? Discuss what federally funded R&D could improve the understanding of such developments and improve the capabilities needed to mitigate against such disruptions.

- Legislation in the US or elsewhere that restricts the use of strong cryptography could significantly undercut our ability to secure the digital ecosystem and make it resilient. Whether the motivation is to defeat terrorism or reduce child exploitation, restrictions on strong cryptography or requirements for "back doors" will weaken the use of encryption overall and potentially create a tool for state repression and a target for criminals. We need more research on how to hold criminal elements accountable without limiting the civil liberties of the law-abiding population; and

- More comprehensive privacy laws could impact our approaches to securing the digital ecosystem. Regulations such as the EU's GDPR embrace Fair Information Practice Principles and give individuals greater control over their personal information. US persons are showing greater concern over privacy of their information, particularly as they see unconstrained use (and abuse) of information by commercial interests. Thus, there is the possibility of increased interest in privacy laws and regulations in the US and internationally. Research into how to better support privacy of data and behavior should be encouraged. We need to better understand how to improve security and privacy simultaneously so that increases in one do not detract from the other, as has sometimes been the case historically.

6. What further advancements 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?

- *Intentionally blank*

7. 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?

- *Intentionally blank*