Federal Register Notice: 88 FR 7999, https://www.federalregister.gov/documents/2023/02/21/2023-03557/request-for-information-on-the-2023-federal-cybersecurity-research-and-development-strategic-plan, March 3rd, 2023.

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan: Responses

Pursuant to the Cybersecurity Enhancement Act of 2014, Federal agencies must update the Federal cybersecurity research and development (R&D) strategic plan every four years. The NITRD NCO seeks public input for the 2023 update of the Federal cybersecurity R&D strategic plan. The updated plan will be used to guide and coordinate federally funded research in cybersecurity, including cybersecurity education and workforce development, and the development of consensus-based standards and best practices in cybersecurity.

This document contains the 10 responses received from interested parties.

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government or any entity within the U.S. Government. The U.S. Government bears no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Contents

Association for Computing Machinery (ACM) 1

Brian Barnier 6

Computing Research Association (CRA)'s Computing Community Consortium (CCC) 11

Danielle Jablanski 28

David Clark, Kc Claffy 32

International Society of Automation (ISA) 34

Jennifer O'Connor 35

MITRE 37

The American Psychological Association Services, Inc. (APA) 61

The App Association (ACT) 66

Federal Register Notice 88 FR 7999, Federal Register : Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

Association for Computing Machinery (ACM)

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

acm U.S. Technology Policy Committee

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*

Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

Brian Barnier

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Comments on 2023 Federal Cybersecurity R&D Strategic Plan
https://www.federalregister.gov/documents/2023/02/07/2023-02578/request-for-information-on-the-2023-federal-cybersecurity-research-and-development-strategic-plan?mod=djemCybersecruityPro&tpl=cy
Prior plan: https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf
cybersecurity@nitrd.gov

Hello,

Providing answers to your questions.

First, a bit of context…

- Most all breaches are self-inflicted, as revealed by systems and root cause analysis common to other disciplines and widely in federal government (not the flavor typically used in cybersecurity).
- Breaches are not primarily a technical problem.
- Instead, it is that cyber pros are setup to fail by structurally flawed (technical term) math and methods.
    - In addition, these structurally flawed math and methods cause burnout and stress among cyber pros as seen in surveys.
    - The human/people-centric element so common in other occupations (factory workers, pilots, nurses, truck drivers, industrial plant operations, military, sports, music performance) gets little attention in cybersecurity.
    - In cybersecurity, math and methods lag many decades behind what is used elsewhere in federal government and the private sector. For example, methods common in WWII or before are largely unknown in cybersecurity.
- Back to systems and root cause analysis. Breaches are caused by a flawed assumption about the nature of the system in which cybersecurity lives. This flawed assumption about the system cascades to methods, measurements and analytics, technology and comes together to crush cyber pros (this is easily illustrated with Mr. Ishikawa's famed Fishbone Diagram).

With this in mind, answers to the listed questions…

1. What new innovations have the potential to greatly enhance the security…

> This is not primarily a tech issue.
>
> > It is a problem of how many decades cyber security lags behind other disciplines (including in federal government).
> >
> > Imagine an airplane cockpit that is as lacking in interoperability as cybersecurity.
> >
> > Consider how widely critical thinking, systems thinking and industrial-strength design thinking have been used in the federal government alone.
> >
> > > The best NIST document 800-160 takes a systems approach but receives not enough focus.

Zero Trust, despite being in President Biden's Executive Order on cyber security is widely misunderstood. This is authentic Zero Trust https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

2. Are there mature solutions in the marketplace that address the deficiencies raised in the 2019 Strategic Plan?

This is not primarily a tech issue.

The reason for breaches is the structurally flawed math and methods that setup cyber pros to fail. Thus, more research is needed using systems and root cause analysis, drawing on work such as W. Edwards Deming's for WWII logistics, Medical Team Training at the Veterans' Health System that significantly reduced deaths, NTSB, CSB and many more.

Shift away from threats to what to protect. End users should be able to click all day on malicious links with no problems. Are passengers on an airplane expected to fly the plane or load bags? No. Are spectators at sporting events expected to play the sport? No. Protecting people from danger is the objective of authentic Zero Trust (above).

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?

Artificial intelligence – only in the context of decision science. So much money is wasted flowing to "data science" programs that lack an understanding of the limitations of AI.

Quantum – beyond cybersecurity, this is a national priority.

Trustworthy Distributed Digital Infrastructure – only in the context of authentic Zero Trust Strategy (ZT is not an architecture) – in the context of the CISA document above.

Secure Hardware and Software – only in the context of NIST 800-160 (the best NIST document) and authentic Zero Trust.

But the benefits of these tech programs are limited without…

Education and Workforce Development – only in the context of what has been proven and practical in other occupations for decades.

- What is currently done in cyber lags other disciplines by decades – or longer. Those should be halted as ineffective and inefficient.
- Instead, empower people with critical thinking, systems thinking and industrial-strength design thinking needed to solve the real problems. Feel free to contact me for a selection of thinking programs in federal agencies.

Yet it is the "Critical Dependencies" that need to become the focus…

- Human Aspect – it is a meme! Look at the Charlie Chaplin Modern Times (1936) "factory scene" on youtube.com with about 80 million views, or Lucy in the Chocolate Factory

(1952). These are laugh lines in my conference presentations. This is what cyber pros feel. Methods used (outside of cybersecurity) for decades in federal agencies and the private sector set up cyber pros for success.

- Risk Management – the methods currently cited from NIST are structurally flawed. Why? Because they are mostly based on bookkeeping (audit) and insurance (loss after the bad thing). They are not systems math. Systems math is needed.
- Scientific Foundations –
    - "…models of complex and dynamic systems at multiple scales…" is by far the most important.
        - Today the typical assumption for math and method is that the system in which cyber lives is like bookkeeping (largely due to a federal government error in the 1970s compounded by accountants in the 2000s) – assuming a linear, stable and highly-rules based process where most adversaries have employee badges.
        - This is not the reality of the complex, dynamic, often chaotic and highly adversarial system that is the reality of the system in which cybersecurity lives.
    - "Frameworks" used in cybersecurity are <u>not</u> "frameworks" as used in other disciplines. Thus, delete the term "framework."
        - Formally, a "framework" provides a comprehensive understanding of a phenomenon/system (varies by discipline). This means that anything that can change the outcome of a system is included in the system and thus part of a framework.
        - Consider the incompleteness of cybersecurity "frameworks" in the context of other disciplines…
            - If cyber "frameworks" were used for building codes, the buildings would fall.
            - If cyber were used for aviation, planes would fall from the sky.
            - Consider NASA or national lab frameworks used to model our planet Earth, weather or rainforests. Many more examples.
    - All else in this section needs to be revised per these two points.

4. What objectives not included in the 2019 Strategic Plan should be strategic priorities for federally funded R&D in cybersecurity?

> Critical thinking, systems thinking and industrial-strength design thinking that have been so successful for both government and private sector for centuries. For a reference, see Harold Evans, They Made America: Two Centuries of Innovation from the Steam Engine to the Search Engine.

5. What other scientific, technological, economic, legal, or societal changes and developments occurring now or in the foreseeable future…

- Please see above. The problem is not primarily about tech or public policy that will change.

- The real problem in cybersecurity is the deeply flawed assumption about the nature of the system in which cyber lives, cascading to math and methods lagging other disciplines by decades. Thus, cyber has great difficulty coping with any type of change. This cascades into flawed measurement and analytics, flawed tech, poor work-life balance for cyber pros, stress and burnout, cascading to more self-inflicted breaches.

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…

- Need to break down the current silos that exclude so much knowledge from cybersecurity education. Deming's System of Profound Knowledge and critical thinking, systems thinking and industrial-strength design thinking that go back centuries (millennia to Plato and Aristotle).
- A balance of both 1) substantive systems knowledge and 2) individual, team and organizational change knowledge (common in Industrial Operations Engineering Departments and B-Schools, but not in cybersecurity). This includes coaching that is so common in sports and music performance, and Deming, but not in cybersecurity.
- The reference to "Internet of Things" is instructive as this brings together industrial control systems (medical, aviation and more) and cyber security.
    - Yet today a structural flaw is that bookkeeping checks are conflated with automated controls. The first dates to ancient Egyptian grain accounting and second to ancient animal traps.
        - While tire pressure can be "checked" like a bookkeeping tally the accurate pressure comes from a systems understanding https://www.nist.gov/news-events/news/2016/11/national-aviation-history-month-nist-tests-airplane-wheels.
        - This conflation stems from an error in the 1970s in U.S. federal government that viewed computers as largely for accounting, thus applying bookkeeping checks to them. It was a structural flaw to spread these to info/IT/cyber security. Why? Because the nature of the two distinct systems are extremely different.
        - When the systems math is calculated, most "controls" in NIST SP 800-53 are ineffective, another set are a waste of money, and some are both efficient and effective.
    - IOT people know this, thus are dismissive of the errors of cyber pros. But IOT people are too hasty and don't understand the value of what they are rejecting because cyber pros lack knowledge and context to communicate better. Thus, breaches result.

Very respectfully submitted,

Brian Barnier
Co-founder, Think.Design.Cyber and CyberTheory Institute.
ISACA Conyers and Wasserman awards recipient, OCEG Fellow
[redacted]

Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

Computing Research Association (CRA)'s Computing Community Consortium

(CCC)

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

CCC
Computing Community Consortium
Catalyst

Computing Community Consortium's Response to RFI on the 2023 Federal Cybersecurity Research and Development Strategic Plan

March 3, 2023

Written by: *Nadya Bliss (Arizona State University), Elizabeth Bradley (University of Colorado-Boulder), Randal Burns (Johns Hopkins University), Thomas M. Conte (Georgia Institute of Technology), David Danks (University of California San Diego), Nathan Evans (Arizona State University), Kevin Fu (Northeastern University), Haley Griffin (Computing Community Consortium), William D. Gropp (University of Illinois Urbana-Champaign), David Jensen (University of Massachusetts Amherst), Chandra Krintz (University of California-Santa Barbara), Brian LaMacchia (Farcaster Consulting Group), Daniel Lopresti (Lehigh University), Madhav Marathe, (University of Virginia), Melanie Moses (University of New Mexico), Ann W. Schwartz (Computing Community Consortium), Ufuk Topcu (University of Texas-Austin), and Pamela Wisniewski (Vanderbilt University)*

This response is from the Computing Research Association (CRA)'s Computing Community Consortium (CCC). CRA is an association of nearly 250 North American computing research organizations, both academic and industrial, and partners from the professional societies. The mission of the CCC is to bring together the computing research community to enable the pursuit of innovative, high-impact computing research that aligns with pressing national and global challenges.

The Appendix to this response contains both the reference to the CCC Response to NITRD "RFI on Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan" (2019) and the relevant white papers and visioning activities since the last response.

This response includes answers to questions 1, 3, 4, 5, 6 and 7. Detailed responses are below, but we highlight a few key points here:

- **Socio-technical resilience and human aspects of cyber security:** While the 2019 Federal Strategy did include multiple references to the importance of the Human Aspects of cybersecurity, it did not elevate that topic to a "Priority Area". While it is, of course, a "Critical Dependency" as it is referred to in the previous strategy, it is also important to invest in R&D in this area. Research in this area could potentially include development of multi-scale multi-theory models to understand interdependent socio-technical infrastructure systems. This can lead to identification of new vulnerabilities, making systems more resilient, early warning systems, and understanding inter-dependencies. A big challenge is the availability of data and including this in the federal cybersecurity strategy can initiate new ways data can be shared safely.
- **Resilience and security by design:** The 2019 Federal Strategy has significant focus on cyber defense. A key theme of the comments below is to incorporate security up front, by design and not as an afterthought. That, together with socio-technical resilience as described above, is likely to lead to more secure systems.
- **Artificial intelligence:** Recently, there has been increased adoption of Large Language Models (LLMs) and generative AI models in general. These potentially present a significant cybersecurity risk, particularly in their ability to generate disinformation effectively and efficiently, and at an overwhelming scale. More broadly, the ability to discern between authentic, accurate, auto-generated, and maliciously generated information via artificial intelligence (regardless of modality - text, images, video, etc.) presents significant challenges to cybersecurity and needs to be prioritized in the updated research strategy. While the technology companies are increasingly investing in dis- and misinformation related work, this work needs to be continually complemented by academic research and education initiatives.
- **Pandemic and computing:** The COVID-19 pandemic led to rapid adoption of remote working environments which continue to persist because both employees and employers find them attractive. Computing capabilities enable significant connectivity and productivity, but also have the potential to lead to a broader attack surface.
- **Climate and computing:** Rapidly accelerating effects of climate change require new research in resiliency and security of computing infrastructure, particularly in context of the accelerating rate of extreme weather events. There are many opportunities for highly impactful computing research in hardware, software, and algorithms that could support both security and efficiency in a co-optimized fashion.

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)?

Computing researchers in the public and private sectors are rapidly innovating to improve digital systems, and there are many instances of great successes that have resulted from these efforts:

Artificial Intelligence/Large Language Models

Continued advances in machine learning have made artificial intelligence a powerful tool in detecting cyber attacks, particularly advanced persistent threats (APTs) that are long lasting, adaptive, and have a small attack signature. Large language models and graphical neural networks can detect anomalies in configurations, programs, scripts, and network traffic. Learned models can be used to characterize normal activity and, as a consequence, detect malicious and faulty data and programs beyond the capabilities of human analysts, rule-based systems, and classical statistical methods. Finally, LLMs and other AI technologies can be deployed to redirect and distract human attackers by providing believable decoy activity, documents, etc; for example the IARPA (Intelligence Advanced Research Projects Activity) program cited below[1]. LLMs and other AI technologies could substantially enhance this approach to cyber-defense.

It is worthwhile to point out that while AI has the potential to enhance cybersecurity, it can also be deployed as a threat accelerator. For example, large language models could be leveraged as either instruments of disinformation or efficiently probing socio-technical systems for weaknesses at scale.

Human-centered privacy frameworks

Examples include Privacy as Contextual Integrity[2], Privacy by Design[3], and Safety by Design[4]. These frameworks take more nuanced/contextualized approaches to designing digital systems in a proactive way that acknowledges that humans are often the biggest threat to security, reliability, resiliency, trustworthiness, and privacy protections.

[1] https://www.iarpa.gov/research-programs/rescind

[2]https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/#:~:text=Contextual%20integrity%20ties%20adequate%20protection,norms%20of%20distribution%20within%20it.

[3] https://link.springer.com/chapter/10.1007/978-3-030-82786-1_2

[4] https://www.datocms-assets.com/22233/1652864615-child-safety-by-design-report-final-1.pdf

Post-deployment code repair

Research in automated and human assisted code repair on legacy codes has also presented opportunities to mitigate cybersecurity risk in deployed systems, thus allowing increased trustworthiness of infrastructure.

Privacy enhancing technologies

Advances in privacy enhancing technologies and their adoption from multi-party computation to homomorphic encryption to privacy preserving video analytics (as for example, in Homeland Security relevant scenarios[5]) has also been observed in the last few years.

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?

Re-framing: Human-Centered Design, Resilience and Empowerment

The areas of research in the 2019 Strategic Plan are largely missing a critical part of cybersecurity: humans. In this context, people are both part of the solution, the problem, and an entity that needs to be secured. It is critical that continued Federal R&D investments have a sociocultural / sociotechnical lens that accommodates the people using and impacted by digital systems.

Creating resilient systems requires creative solutions that consider the humans interacting within the system. One way the topics could be adjusted to better accommodate humans is to include “Human-centered Design” or “Using Human-centeredness to Design Complex Socio-Technical Systems” as a cross-cutting priority. Human-centeredness is necessary for AI (e.g., fairness, bias, explainability) and the other more technical approaches to be effective. Human behavior is often a weak point in cybersecurity systems, for example when authorized users fall prey to phishing and other attacks. The creation of resilient systems also needs to take into account economic realities and other implementation or adoption challenges. If funding is not

[5] https://pets4hse.org/index.html

available to widely implement a system that already exists, like underfunded public hospitals lacking the resources to protect patient records from cyber criminals, then that system is not an effective or resilient solution and further research is necessary.

Broadly, the 2019 Strategic Plan also has a stark focus on defensive elements (i.e., deter, protect, detect, respond), that could be improved by taking more resilience-based or empowering approaches that allow for struggle, failure, and recovery. And privacy is sometimes interpreted too narrowly in the document, while it should be spread throughout the ecosystem and lifetime of systems.

Quantum Information Science

Quantum information science remains a key priority area of investment because of its potential to break cryptosystems. The technology today is most advanced with superconducting quantum technology, but ion-trap and neutral atom technologies are advancing rapidly, though none of these are yet on the type of exponential growth scale that enabled advances in CMOS semiconductors. At the same time, there is a perception that quantum computing has over-promised and under-delivered. This could result in a “quantum winter” much like the “AI winter” that prevented the US from realizing today’s AI technologies years earlier. It is imperative to remain focused on and continue to invest in quantum information science in general and quantum technology for computing specifically through this potential period of skepticism.

One issue that remains understudied in quantum computing is the need for higher level ways to program these systems. Current approaches, even those that use high level programming languages, express computation at a low quantum circuit level. New algorithms and applications for quantum computing are reserved for the domain of theoretical mathematicians and physicists. An analogy is to VLSI technology before the design rule revolution brought by Carver Mead and Lynn Conway: VLSI circuits were designed by applied physicists solving complex electrical equations. Mead and Conway introduced a series of design rules enabling non-specialists to readily create complex VLSI circuits, and as a result, the applications of integrated circuits exploded. A similar renaissance is required in the quantum domain to enable advances and innovation by a larger number of individuals.

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.

Operational Technology Cybersecurity Research

One gap in the 2019 Strategic Plan is Operational Technology (OT) Cybersecurity Research. The key challenge is how to co-design OT hardware and software to remain highly available and integrity protected despite constantly shifting threats that require updates and patches to both software and hardware. The R&D gap is so great that the industry has created the term "legacy device" to describe OT systems that are not only insecure because of known vulnerabilities, but also impossible to secure because of the lack of a mechanism to patch security holes. A desired capability is to enable security updates for legacy OT systems as well as finding economic models that incentivize the replacement of legacy OT systems with systems that can quickly adapt to shifting threat models. A specific outcome could be hospitals no longer needing to turn away patients when ransomware breaks into an OT system. A more general outcome is higher consumer confidence that OT systems will continue to provide essential functions even when under attack. This requires a shift in thinking away from component-centric security modules to system-centric trustworthy systems. These R&D priorities are important not only for science and engineering, but also for society that depends on highly available emergency medicine, reliable power grids, safe transportation, and every day public infrastructure despite endemic cybersecurity threats to availability and integrity of OT systems and their sensors.

Human-centered design and evaluation

Human-centered design and evaluation of complex socio-technical systems should not be conflated with privacy. They should be two separate priorities with the privacy section focused primarily on information flows. The human-centered priority should be cross-cutting (maybe a social, behavioral, and economic sciences orientation) to show that our federal government acknowledges that all of the technical solutions have significant impact on humans.

For solutions to be practical, responsible, and feasible, human-centered design principles must be implemented across national priorities that invoke translational and implementation science. Simply put, sometimes high-tech solutions are not the answer. True translational and implementation science needs to be led by those in the field (e.g., non-profits, practitioners, end users), so that the technologies we build to solve these problems do not have unintended consequences and/or negative impacts[6].

Core challenges to designing complex and resilient socio-technical systems include:

- Formative assessments that identify key human problems that need to be addressed, rather than prescribing state-of-the-art technologies to solve these problems without first clearly understanding them.
- Further, summative assessments of how these technologies affect humans once they are deployed are also necessary.
- Team dynamics of interdisciplinary research. Interdisciplinary teams often develop stratification, with subject matter experts in social sciences or humanities often playing a secondary role to the technical team. New incentives to create a more equal balance or even place the technical solutions architects in the 'service role' with the human subject matter experts as the 'customer'.

While such cross-disciplinary approaches are less straightforward and harder to implement, they are what is necessary to affect real positive change. A possible way to do this is to have grant funding mechanisms that are phased in two parts - where the social/behavioral team first scopes the problem space and defines the requirements (agnostic of a particular technical solution). Then, this team could solicit phase 2 proposals from technical teams that they feel would meet these requirements. A third phase would be the implementation/translational science piece, where the solutions that are built are evaluated for feasibility and impact. This approach mirrors more closely what is done in industry, where the customer/subject matter expert (SME) drives the requirements and the development team acts to provide the solution. In academia and when creating grant-funding mechanisms, this hierarchy is often flipped, where the technical experts take lead.

Privacy

While privacy is mentioned in the 2019 Strategic Plan, it is defined too narrowly, with a focus on individual privacy. The Strategic Plan should seek to address privacy problems beyond the individual, including interpersonal privacy threats such as sextortion (e.g., unauthorized sharing of digital imagery of a person) or the distribution of child pornography (e.g., digital rights of youth[7]).

[6] https://arxiv.org/ftp/arxiv/papers/2112/2112.09544.pdf

[7] https://journals.sagepub.com/doi/abs/10.1177/1461444816686318

Another area that could benefit from federal R&D investment is at the intersection of privacy preserving/enhancing technologies and incentives and policies to adopt those technologies. The U.S. has historically been misaligned/behind on regulations and policies that have been designed to protect individual privacy (e.g., not being part of GDPR, COPPA regulations for children being out-of-date). While creating policy would be outside the scope of federally funded research, research on adoption and incentive pathways would not be.

These are two privacy challenges that do not seem to be addressed in the strategic plan. And, while several privacy frameworks already exist, regulations and policies that hold platforms accountable for implementing these frameworks in a consistent way are lagging behind. Research initiatives that support validating which frameworks are useful in what contexts and finding ways to translate theoretical frameworks into actionable design principles and practices have potential to have significant impact.

Security and trustworthiness of the AI ecosystem

While AI is also mentioned in the 2019 Strategic Plan, the gap has widened between how AI-enabled functionality is developed and deployed and what a *trustworthy* distributed digital infrastructure can support today and possibly ever. The vulnerabilities due to potential deployment of large models over a distributed infrastructure are unclear. The training and execution and interactions with these models expand the attack surfaces of the systems in which they are going to be integrated to unprecedented levels. Additionally, the innovation ecosystem has grown to favor empirical performance over principles and guidelines for trustworthiness that have been established over decades-long experience. Deferring the security concerns to late stages of development has never been sustainable, and the exponentially growing complexity and cost—in data, computing, and engineering—amplifies the importance of security in the early stages of development and even conception of technology. It is therefore critical to incentivize security in the entire AI ecosystem. Otherwise, it will be increasingly costly and possibly catastrophic to walk the thin line that separates AI being an opportunity for security from AI being a security vulnerability.

Cryptographic agility and the transition to quantum-resistant cryptography

Finally, while the 2019 Strategic Plan briefly mentions goals of drafting standards for quantum-resistant (a.k.a. post-quantum) cryptography and implementing them, it is silent on all the other components necessary to effect a wide-scale cryptographic algorithm transition to post-quantum cryptography. As we have seen over the last 18 years (since NSA announced “Suite B” and their goal of transitioning public-key cryptography from RSA to elliptic curve), cryptographic algorithm transitions are difficult, time-consuming, and take much longer than expected. Indeed, many sectors of industry have still not transitioned to elliptic curve cryptography and are now being told to start another transition. The 2023 Strategic Plan should include R&D goals concerning integrating quantum-resistant algorithms into every security protocol that utilizes cryptography and improving system architectures with cryptographic agility to make this PQC transition (and future cryptographic algorithm transitions) easier[8].

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.

LLMs (and other generative models) vulnerabilities to cyber attacks

Large language models (LLMs) that generate text and chatbots that provide credible interactivity will emerge as powerful tools for cyber attacks. Social engineering attacks that have to date been conducted by human adversaries will become scalable to large populations and will still be personalized to individual users. For example, artificial intelligence will be able to conduct spearfishing attacks against entire communities, starting with customized emails or messages personalized based on browsing histories. Followed by interactive messages that adapt content based on the target’s responses. Detecting AI generated content will become a fundamental part of the cybersecurity arms race. Academic research is needed at a national scale to build the methods that make AI-generated misinformation and attacks robustly detectable, and also into the environments, interfaces, and tools to secure users' online interactions.

[8] See, e.g., Chapter 4 and Findings 4.12 and 4.13 of National Academies of Sciences, Engineering, and Medicine. 2022. *Cryptography and the Intelligence Community: The Future of Encryption*. Washington, DC: The National Academies Press. https://doi.org/10.17226/26168.

Rapid shift to hybrid work environments

The pandemic upended the workplace, significantly accelerating the trend to more remote work. The ability to keep society working even during a complete lockdown was to some extent a success of earlier investments in the digital ecosystem. We must now look to building a new class of tools to support hybrid workplace environments. Challenges include the urban, rural divide in terms of broadband access, equity issues across income and work types, education and issues related to privacy and security. Of course, as connectivity and remote work increases, so does the attack surface. Increasingly, as hybrid work environments become the norm, there needs to be a corresponding focus on cybersecurity in context of those hybrid work environments.

Opportunities and challenges for online education and training

This applies at all age levels. The challenges are acute for younger children. But perhaps new opportunities at high school and beyond levels, by bringing in new learning tools (AI agents), new materials, new set of teachers, etc.

Tools to to secure and improve our global supply chain

This issue has multiple components but advances in the digital ecosystem can help track goods, give early warning capabilities in terms of impending disruptions, and make it easier to re-engineer the network to move production and delivery of goods and services.

Tools for identifying, tracking and controlling the spread of (mis), (dis) information

Disinformation and misinformation targeted at individuals can have major impacts on system-wide responses to threats and challenges, as evidenced by vaccine hesitancy during the COVID-19 pandemic. With the deployment of AI based on large language and other generative models, the impact of disinformation on health, national security, and other aspects of society could become even greater. Identification and mitigation of disinformation is necessary, and individuals and communities need access to information that is contextualized and timely in order to make effective decisions.

New advances to collect, process and share personal information

Example areas that need these advancements in a manner that respects privacy, anonymity, fairness, etc. are mobility data, electronic health records, transaction data, and data collected by various body sensors. The COVID-19 pandemic showed the potential use of digital technologies such as contact tracing. Some countries used it effectively, others did not. The use of the technology is quite clear but requires further research into challenges and the potential misuse by individuals and organizations.

Biothreats and infectious disease surveillance

As there are progressive improvements in synthetic biology, biothreats will arise and need to be swiftly detected. More broadly detecting a multi-sector disruption that can potentially be engineered is needed. Opportunities for collecting, sharing information for infectious disease surveillance and monitoring (that includes environmental surveillance), and the ability to use new devices for sequencing are warranted. It is pivotal that these practices are connected in the large digital ecosystem that is secure by design.

Impacts of climate change

The increasing frequency of extreme events has the potential to stress and even de-stabilize the US power grids and, in turn, affect the communications networks that underpin the modern digital ecosystem. The security of this critical infrastructure is affected both by legacy systems that do not have protections built in and adoption of new technologies without proper protections. Federal support is needed to foster advances in computing research, together with interdisciplinary collaborations, to create robust, resilient next-generation infrastructure for the future. We need strategies for modeling the systems-level effects of climate change on the infrastructure that underpins our digital ecosystem, as well as decision-support systems and advanced algorithms to predict, identify, and mitigate failures (particularly cascading failures) in the context of those changes. In addition to leveraging decision-support systems to identify potential tipping points or security flaws in critical digital infrastructure, decision-support and visualization systems can be leveraged to optimize design of new infrastructure. Research in these areas will need to balance some important tradeoffs, as resiliency often requires redundancy and thus potentially reduces efficiency.

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?

In cybersecurity education and workforce development, there is often an assumption that people simply need to be taught how to use the technologies, rather than considering that the technology may simply not be useful for the user. Cybersecurity education and workforce development efforts - like research - should take a human-centered design approach that puts community stakeholders in the driver's seat. Promoting a Community Informatics approach to technology design, development, and buy-in may help address this challenge.

Experiential education (hackathons, capture the flag competitions, ethical hacking) has seen significant adoption and needs to continue.

Cybersecurity education for non-experts who form the vast majority of people who use and/or are impacted by the use of computers- policy, healthcare, etc. would help drive funding and research as more people would see the need for cybersecurity across sectors.

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?

The R&D Goal related to quantum-resistant cryptography should remain but be updated in light of the progress in this area since 2019. In July, 2022, NIST announced[9] their first selections of quantum-resistant public-key encryption and digital signature algorithms for standardization, and NSA shortly followed with an update[10] to their Commercial National Security Algorithm suite (CNSA 2.0) incorporating some of the NIST selections. Further, in May 2022, President Biden issued National Security Memorandum NSM-10 ("Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,"[11]) directing various activities within Executive Branch agencies to prepare them for the transition to quantum-resistant cryptography.

[9] https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf
[10] https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
[11] https://irp.fas.org/offdocs/nsm/nsm-10.pdf

Also, in December 2022 the President signed P.L. 117-260, the “Quantum Computing Cybersecurity Preparedness Act”[12], which adds additional reporting requirements on civilian agencies. The R&D goals in the QIS section, specifically those related to quantum-resistant cryptography, should be revised to build on these recent government activities.

Both the National Defense Strategy[13] and the National Security Strategy[14] place significant emphasis on cybersecurity in topics ranging from norms of operating in cyberspace to resilience to cyber attacks. Coordination between non-defense and defense research and ensuring that advanced capabilities are transitioned into application and practice would be beneficial.

[12] https://www.congress.gov/bill/117th-congress/house-bill/7535
[13] https://www.defense.gov/National-Defense-Strategy/
[14] https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

APPENDIX

Here is the link to the CCC's Response to NITRD's "RFI on Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan."

The following is a list of recent CCC RFI responses that have discussed issues which intersect with the issues raised by the RFI.

- Computing Community Consortium's Response to RFI "Request for Information on Advancing Privacy-Enhancing Technologies"
- Response to RFI on Federal Priorities for Information Integrity Research and Development
- The Computing Community Consortium's Response to Request for Information on Evaluating and Improving the NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management
- Response to RFI on Public and Private Sector Uses of Biometric Technologies
- Computing Community Consortium (CCC) Response to Establishing Confidence in IoT Device Security: How do we get there?

The following is a list of CCC workshops since our 2019 response (associated community reports can be found at the link) that have discussed issues which intersect the issues raised by the RFI.

Artificial Intelligence

- Artificial Intelligence Roadmap Workshop 2 – Interaction
- Artificial Intelligence Roadmap Workshop 3 – Self Aware Learning
- Artificial Intelligence / Operations Research Workshop 1
- Artificial Intelligence / Operations Research Workshop 2

Post Quantum Cryptography

- Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility

Computing in Complex Human Systems

- Code 8.7: Using Computational Science and AI to End Modern Slavery
- CCC / Code 8.7 Workshop on Applying AI in the Fight Against Modern Slavery

Workforce/Economics

- Content Generation for Workforce Training
- Economics and Fairness

- The CCC Hybrid Workshop on Best Practices for Hybrid Workshops

Assured Autonomy

- Assured Autonomy Workshop #1
- Assured Autonomy Workshop #2
- Assured Autonomy #3

Health

- NAE/CCC Workshop on the Role of Robotics in Infectious Disease Crises
- Computational Support for Substance Use Disorder Prevention, Detection, Treatment, and Recovery

Climate

- Building Resilience to Climate Driven Extreme Events with Computing Innovations: A Convergence Accelerator Workshop

The following is a list of CCC whitepapers since our 2019 response (associated community reports can be found at the link) that have discussed issues which intersect the issues raised by the RFI.

Climate

- Computing Research for the Climate Crisis

Artificial Intelligence

- Imagine All the People: Citizen Science, Artificial Intelligence, and Computational Research
- Artificial Intelligence at the Edge
- Artificial Intelligence and Cooperation
- Interdisciplinary Approaches to Understanding Artificial Intelligence's Impact on Society
- The Rise of AI-Driven Simulators: Building a New Crystal Ball
- Next Wave Artificial Intelligence: Robust, Explainable, Adaptable, Ethical, and Accountable

Socio-Technical Computing

- An Agenda for Disinformation Research

- Modernizing Data Control: Making Personal Digital Data Mutually Beneficial for Citizens and Industry

Broad Computing

- A National Research Agenda for Intelligent Infrastructure: 2021 Update
- Pandemic Informatics: Preparation, Robustness and Resilience
- Infrastructure for Artificial Intelligence, Quantum and High Performance Computing
- Robotics Enabling the Workforce
- A Research Ecosystem for Secure Computing

Core Computer Science

- Post Quantum Cryptography: Readiness Challenges and the Approaching Storm
- Theoretical Computer Science: Foundations for an Algorithmic World
- Computing Research Challenges in Next Generation Wireless Networking

Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

Danielle Jablanski

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Response to the Cybersecurity and Infrastructure Security Agency Interagency Working Group request for public input on federal priorities in cybersecurity R&D.

Danielle Jablanski, OT Cybersecurity Strategist, Nozomi Networks, & Non-Resident Fellow, Digital Forensic Research Lab, Atlantic Council

The FY 2023 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap does not address the goals stated in the 2019 Federal Cybersecurity Research and Development Strategic Plan, related to Cyber-Physical Systems and Critical Infrastructure. The strategy points out "As CPS systems become more complex, **the interdependence of components increases the vulnerability to attacks and cascading failures**" but the 2023 plan's only mention of a project in line with this consideration is the Air Force Office of Scientific Research and Air Force Research Laboratory program on "Critical Infrastructure Resiliency and Prediction of Cascading Effects." While this endeavor is indeed worthy, it is too limited in scope in this implementation to achieve the stated strategic goals:

- Develop methodologies and standards to support seamless, end-to-end security across interconnected networks with multiple owners, trust domains, topologies, networking paradigms, and the full range of mobile devices and mobile network layers.
- Develop technologies to sustain autonomous management of security across the communication infrastructure in ways that balance strength of security services with performance requirements of availability, latency, processing, and storage capacity.
- Develop end-to-end security and key management capabilities that will allow highly secure, highly resourced nodes to interoperate with resource-limited edge and IoT devices.
- As CPS systems (e.g., cars, medical devices, and utilities) scale in the number of devices they connect and the volume of data they process, develop approaches to assure that they remain resilient to adverse cyber activities. **This includes developing accurate models of CPS environments to reduce vulnerabilities and mitigate the impacts of incidents and failures. Develop methods and technologies that will successfully integrate human decision-making with cybersecurity technologies and process control technologies. Advance formal methods to validate high-assurance, fault-tolerant, adaptive subsystems that can operate in contested and degraded conditions for long periods without human interaction.**

Goal 4 deserves much more attention given today's threat landscape and the most recent national cybersecurity strategy and its imperatives surrounding cyber-physical systems. It is increasingly difficult to contextualize critical infrastructure both operationally – based on specific products, services, resources, processes, and technologies – and functionally based on centralized vs. distributed risks, dependencies, and interdependencies. Attempts to date have led to a debate between asset-specific (things - technologies, systems, and equipment) vs. function-specific (actions – connect, distribute, manage, supply) cybersecurity prioritization.

Operational Technology and Industrial Control System Census Data

Threading the tapestry of risk across critical infrastructure requires a more granular and purposeful model than the current approach to classifying critical infrastructure can deliver. Without contextualizing the broad problem set that is critical infrastructure cybersecurity, we risk two poor outcomes. First, increasing the cost of compliance-based cybersecurity to the extent that small to medium sized businesses cannot afford to meet expensive and prescriptive cybersecurity regulations. Second, that the government finds itself responsible for providing managed cybersecurity services to designated concentrations of risk across multiple sectors – an imprudent, wildly expensive, and unsustainable outcome.

Critical infrastructure cybersecurity presents a massive needle in a haystack problem. Where IT sees many vulnerabilities likely to be exploited in similar ways across mainstream and ubiquitous systems, OT security is often a proprietary case-by-case distinction. The oversimplification of their differences leads to a contextual gap when translating roles and responsibilities into tasks and capabilities for government, and business continuity and disaster recovery for industry.

What's eating critical infrastructure isn't the talent gap, the convergence of information technology and operational technology, or even the lack of investment in cybersecurity products and solutions. It's the improbability of determining all possible outcomes from single points of dependence and failure that exist between and extend beyond business continuity, physical equipment, and secure data and communications.

Federal cybersecurity research and development has a blind spot when it comes to holistic and national understanding of operational technology and industrial control systems. R&D should begin to answer the many open questions related to the lack of available data for OT/ICS vendor technologies embedded across critical infrastructure sectors in the U.S., to better understand penetration rates as well as centralization risks and potential for cascading impacts.

There is a lack of understanding of the census of industrial assets and technologies in use across critical sectors today, their configuration contingencies for risk management, and holistic awareness of realistic cascading impacts and fallout analysis for entities with varying characteristics and demographics. We need to better understand the national inventory of operational critical components, how to defend them based on an effects-based, rather than a means-based approach to protecting critical infrastructure, and proactive measures to reduce the severity of supply chain attacks and impacts.

SRMAs Capacity Building and OT Detection and Response

Regardless of commonalities, no two attacks on OT/ICS systems are ever the exact same, making automated response and remediation difficult. Unfortunately, this reality means that every operation and facility must wait to see another organization victimized before there can be shared signatures, detections, and fully baked intelligence for threat hunting to ensue. In terms of the threat landscape, there is no way to standardize and correlate threat and vulnerability research produced from the competitive market leaders. Information sharing is lacking trust and verification, has been siloed into sector-specific, private sector, or government agency-specific mechanisms—creating single sources of information without much consensus. This is a major roadblock for efficacy across SRMAs and their situational awareness/strategic planning.

In a perfect world there would be a dedicated cybersecurity SME at the federal level for each critical infrastructure sector, either within each SRMA or at CISA as a main technical liaison. In lieu of this reality, cybersecurity research and development should capture the entire OT/ICS supply chain – security management of suppliers, ECM, development environment, products and services, upstream supply chain, operational OT, and downstream supply chain – aligned to the CISA CPGs as a baseline. As the SRMAs designate required tools and capabilities at the asset owner level, they should continue vendor-neutral evaluations of designated and required tools and capabilities. SRMAs also need to identify what level of cybersecurity and risk management asset owners can afford to own vs. what government can reasonably subsidize and augment. I don't believe this can be effectively done without addressing points above.

In OT, response prioritization is dependent on detection. You can't defend what you can't see, but you also can't do damage control if you don't know the impacts of potential incidents as well as prevention or avoidance measures. In industrial control systems, in particular for energy delivery, there is a significant need to define more relevant risk calculation metrics for detection that reduces the severity of potential incidents.

Even when targeting intermediary Windows and Linux systems between corporate and control networks, many OT incidents potentially have more similarities to events such as wildfire contagion rather than enterprise risk management. Metrics on reducing the severity of impacts should be a key component of integrated response capabilities in OT. Response should be driven by impact and consequence evaluations, providing assessment and environment-specific context for detection and remediation.

Detection and incident response have far-reaching consequences to critical and interdependent sectors. An attack on transportation may impact everything from fuel delivery to generation, to the manufacturing supply chain. In the operational technology (OT) space, detection and incident response looks very different today compared to IT. Innate concerns and potential process failures are the exact precursors that allow threat actors to execute attacks in OT environments.

Electricity delivery systems have long been held to reliability and performance standards, including power quality, system and customer outage duration. Similar context for recalculating risk and mitigating cyber events with or without operational disruption are less normalized with available cybersecurity solutions. OT cybersecurity solutions should include real-world impact analysis rather than focusing on CVSS scoring or context-latent risks – another area for exploration. This, coupled with the census research above, will allow for more thorough contingency planning to occur across critical infrastructure OT/ICS cybersecurity as a whole.

Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

David Clark

Kc Claffy

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Subject: RFI Response: Federal Cybersecurity R&D Strategic Plan
Date: 3 March 2023
From: kc claffy CAIDA, UCSD, David Clark, CSAIL MIT

We write in response to the above-cited request for information. Our response draws on our collective history of research in Internet measurement, Internet security, and the relation of technical innovation to the larger societal context in which the Internet is positioned today.

Focus on Internet security

We urge that the R&D Strategic Plan be explicit in giving priority to the security of the Internet itself. The introduction to the 2019 plan mentions security of the Internet several times, but the rest of the report mentions it only once (aside from the phrase Internet of Things) in Trustworthy Distributed Digital Infrastructure, and there in the subsection on 5G and Post-5G. That section talks about the "accelerated development and rollout of next-generation telecommunications and information infrastructure". The report thus elides an underappreciated fact: society must live with the current-generation Internet we have today. Improving the security of the current Internet may not seem innovative, but it is critical. We note that the 2019 report refers to "seamless, end-to-end security across interconnected networks with multiple owners, trust domains, …" We agree that this is the correct scope of the critical challenge, but urge that it not be equated to "next-generation".

We understand that the focus on the Strategic Plan is on research priorities, not preferred research outcomes. However, we believe that better security of the Internet will require a reconception of how to approach the problem. The challenge is often stated using phrases such as: "improve the global security of the Internet". But thus stated, the goal is intractable because at that scale, the Internet includes malicious actors inside the system. We must adjust, and think about how to secure regions of the Internet (what we call *zones of trust*), or classes of user behavior (design of applications that damp abusive activities) knowing that we cannot exclude malicious actors from the ecosystem.

The report would benefit from articulating the specific vulnerabilities at the Internet layer: Distributed Denial of Service attacks, abuse (often in the context of DDoS) of the source address in packets, malicious routing announcements, vulnerabilities and abuse of the DNS and the Certificate Authority system. By flagging the specific vulnerabilities, their implications become more tangible.

Improving the trustworthy character of the user experience.

The section on Distributed Digital Infrastructure uses the word "Trustworthy" rather than "Secure" in the heading. We encourage a continued focus on making the Internet experience trustworthy, and note that a ``secure system'' (in its formal sense—that it operates according to its specification even under attack) does not automatically produce a safe or trustworthy experience. Much abuse on the Internet today, ranging from phishing to disinformation, is exploiting the features of the Internet as they were designed to be used.

However, most subsections of that section (and R&D goals) focus on technical innovations more related to security, rather than making the user experience more trustworthy. We urge elaboration of the challenge stated in the introduction: "to elevate human-oriented issues to be among the priorities for cybersecurity R&D".

The report has a strong section on privacy, but privacy is not the only, or perhaps not the most important, aspect of making the online experience more trustworthy. We support the mention in the section of Critical Dependencies of social and behavioral studies, and developing psychological, sociological and economic models. We urge that the report not view security as a primarily technical problem.

Enabling academic research on Internet security

In the section on Implementing the Plan, (the subsection on Academia and Research Organization), the report states that "researchers should provide comparisons against open datasets". This passing mention of open datasets does not address the larger challenge here, which is much of the data that will enable academia to participate in security research (and Internet research more generally) is collected by private-sector firms and is considered proprietary. Governments need to address the challenge of getting data about the operation of the Internet into the hands of the research community. This is critical for workforce development as well as sustaining the role of academia in understanding and improving cybersecurity.

The issue of access to data will evolve as the government takes more interest in the character of the Internet, and possible roles for regulation. The government will also collect data to support *its* role. A starting assumption might be that industry-provided data is available only to the government, protected by data sharing agreements with industry. We urge that this not be the norm. The European Union, in a regulatory context (which we understand is different from the space within which NITRD operates) has clearly articulated that independent academic research must be sustained by access to relevant data.

In their proposed regulation for Digital Services[1] they discuss the importance of ensuring access to proprietary data by the academic research community. The report states:

> *Investigations by researchers on the evolution and severity of online systemic risks are particularly important for bridging information asymmetries and establishing a resilient system of risk mitigation, informing online platforms, Digital Services Coordinators, other competent authorities, the Commission and the public. This Regulation therefore provides a framework for compelling access to data from very large online platforms to vetted researchers.*

They clarify what they mean by "vetted researchers":

> *In order to be vetted, researchers shall be affiliated with academic institutions, be independent from commercial interests, have proven records of expertise in the fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request.*

This regulation emphasizes a structure that allows the academic community to work with proprietary data, sending an important signal that they intend to make their academic research establishment a recognized part of shaping the future of the Internet in the EU. The U.S. needs to take a similar proactive stance, and we encourage NITRD to advocate for this stance.

Deterrence

The 2019 report states that "Deterrence also requires successful attribution of cyber attacks to specific offenders to dissuade them from pursuing cyber attacks." We believe that raising the level of effort that attackers must expend need not depend on attribution, and given the global nature of the Internet, as you note, we would urge an emphasis on other dimensions of deterrence—in particular, new design principles for applications that raise the cost of abusive behavior. In our view, the emphasis on forensic analysis may be misguided, and if this sort of attribution is important, it will be of most relevance at the application layer. This point is important, in that it brings a focus on the correct layer of the ecosystem.

[1] European Commission", "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services," 2020. https://eur-lex.europa.eu/legal-content/.

Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

International Society of Automation (ISA)

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

International Society of Automation
Setting the Standard for Automation™

RFI Response: 2023 Federal Cybersecurity R&D Strategic Plan

National Science Foundation (NSF)
FRN 2023-02578 | 1 March 2023

The International Society of Automation (ISA) is pleased to submit these public comments to the National Science Foundation (NSF) for consideration as the agency develops its 2023 Federal Cybersecurity R&D Strategic Plan.

About ISA

ISA (www.isa.org) is a non-profit professional association founded in 1945 to create a better world through automation. ISA empowers the global automation community through standards and knowledge sharing, driving the advancement of individual careers and the overall profession. ISA develops widely used global standards; certifies professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its members and customers around the world.

ISA created the ISA Global Cybersecurity Alliance (www.isa.org/ISAGCA) to advance cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes. The Alliance brings end-user companies, automation and control systems providers, IT infrastructure providers, services providers, system integrators, and other cybersecurity stakeholder organizations together to proactively address growing threats.

ISA developed ISA/IEC 62443, the world's only consensus-based automation and control systems cybersecurity standards.

RFI 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)?*

The International Society of Automation has published a consensus set of international standards (ISA/IEC 62443) that establish detailed requirements for securing automation and control systems for cyber-physical systems – the operational technology that is the foundation of the vast critical infrastructure and manufacturing sectors on which we all depend.

These international standards address the shared responsibility among all stakeholders in the automation lifecycle including automation suppliers, maintenance and integration service providers and owner/operators.

Manufacturers (supplier organizations) are already adopting the ISA/IEC 62443 standards and receiving ISA/IEC 62443 conformance certifications from globally recognized certification programs like ISASecure®.

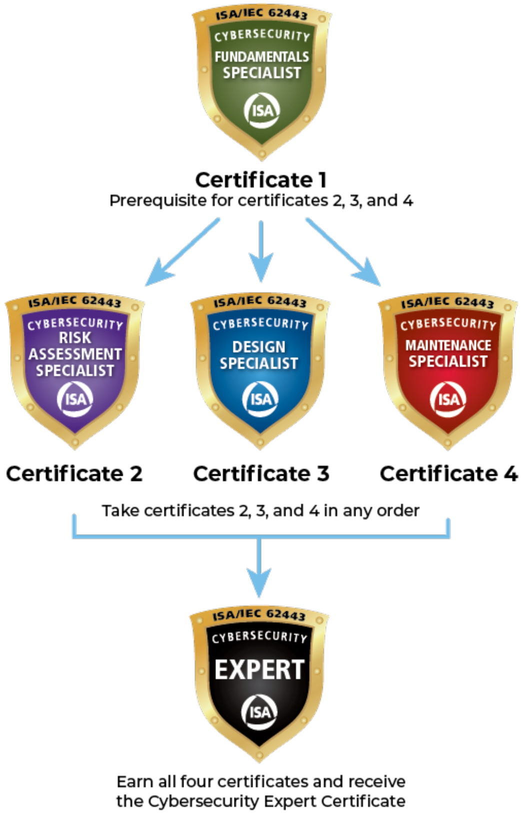
Owner/operators are developing a consensus operating site assessment specification under the ISASecure® program to secure and measure security of the automation systems at operating sites (similar to NERC-CIP in the regulated electric sector).

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?

Education and workforce development are areas of focus in the 2019 plan and will likely pervade into NSF's plans for the 2023 plan as well.

But it is important to note that there are a number of mature credentialing solutions that are already relied upon by employers and workers across many industry sectors, including cybersecurity training and credentials offered by ISA.

ISA industrial cybersecurity training courses and knowledge-based certificate recognition program are based on ISA/IEC 62443 and are a key component of government cybersecurity plans. This program covers the complete lifecycle of industrial automation and control system (IACS) assessment, design, implementation, operations, and maintenance.



The program is designed for professionals involved in IT and control system security roles that need to develop a command of industrial cybersecurity terminology, as well as a thorough understanding of the material embedded in the ISA/IEC 62443 series of standards. ISA cybersecurity training may also be incorporated at all levels of post-secondary education. The ISA/IEC 62443 cybersecurity certificates are awarded to those who successfully complete a designated training course and pass a 75-100 question multiple choice exam.

Pursuant to Office of Management and Budget (OMB) Circular A-119, *Federal Participation in the Development and use of Voluntary Consensus Standards and in Conformity Assessment Activities*, as well as the *National Technology Transfer and Advancement Act of 1995* (NTTAA), NSF is encouraged to consider whether existing private-sector-led training and credentialing programs that are built on voluntary consensus international standards would meet the agency's objectives and goals for workforce development and education efforts.

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?

One suggestion for a continued area of priority for the 2023 plan is identifying technology that can be embedded into cyber-physical systems to advance the ability of devices to intrinsically protect themselves from intentional cyber disruptions.

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?

The summary in the NSF request for information makes a highly perceptive statement: "The updated plan will be used to guide and coordinate federally funded research in cybersecurity, including cybersecurity education and workforce development, and the development of consensus-based standards and best practices in cybersecurity."

It is perceptive because the global manufacturing and industrial processing sectors have now coalesced around ISA/IEC 62443 as a series of consensus cybersecurity standards that is applicable to all industry sectors and critical infrastructure. The standards provide a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems, where compromise could result in any, or all, of the following:

- Threats to public and/or employee safety and health
- Threats to critical infrastructure including power grids and water processing
- Threats to national security
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Major economic losses
- Threats to the natural environment

The International Electrotechnical Commission (IEC) is one of three World Standards Cooperation members, a high-level, United Nations sanctioned collaboration that includes the International Organization for Standardization (ISO) and International Telecommunication Union (ITU). The global status and reach of the IEC has ensured that the ISA/IEC 62443 standards are now being applied in industrial and critical infrastructure applications across the modern manufacturing and industrial processing world.

The growing worldwide use of the standards is seen in two key developments since the 2019 NSF Cybersecurity Plan:

- A decision by the IEC to officially designate the IEC 62443 series of standards as having "horizontal" status, establishing primacy across the entirety of the vast range of IEC technical committees and subcommittees on matters pertaining to cybersecurity in industrial, critical infrastructure, and related applications.

- A decision by the United Nations Economic Commission for Europe to integrate the IEC 62443 standards into its Common Regulatory Framework on Cybersecurity, which serves as an official UN policy position statement for Europe.

The primary developer of the standards is not the IEC itself, but an engineering association with headquarters in the US, the International Society of Automation (ISA). Having direct responsibility for the standards is the ISA99 standards development committee, following procedures for openness and balance that are accredited by the American National Standards Institute (ANSI). The ISA99 committee brings together industrial cybersecurity experts from across the globe, representing in a range of industries and critical infrastructure applications.

The ongoing work of the ISA99 committee in developing and updating the consensus standards, which are known in the US as the ANSI/ISA 62443 series – and often referred to as the ISA/IEC 62443 Series – relies on experts who volunteer their time from production plant asset owners and operators, manufacturing systems and equipment suppliers, government and academic organizations, and more. NSF support of the standards development structure could be pivotal in accelerating the creation and updating of the ISA/IEC 62443 consensus standards and the related cybersecurity education and workforce development programs described above, particularly with respect to the ongoing need to reflect advances in cybersecurity technology and changes in the cyber threat landscape.

Conclusion

Thank you for this opportunity to highlight essential ongoing work in consensus cybersecurity standards and conformance programs, with related training and workforce development programs. NSF recognition and support of these programs would make a significant impact in advancing the security of our industrial and critical infrastructure.

Thank you for your consideration of these comments. Should you require any additional information, please contact Liz Neiman, ISA managing director of strategic engagement.
[redacted]

Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

Jennifer O’Connor

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

From: JENNIFER O'CONNOR [redacted]
Sent: Friday, March 3, 2023 1:46 PM
To: cybersecurity <cybersecurity@nitrd.gov>
Subject: Re: RFI Response: Federal Cybersecurity R&D Strategic Plan

Ironically, an article appeared in my feed this morning on an interesting privacy policy. If it was needed but inappropriate seems like there are cyber training gaps. Plus the US is far behind international privacy laws. Why put law enforcement in that position. Raise the bar fairly.

https://fcw.com/digital-government/2023/03/watchdog-secret-service-ice-failed-follow-federal-statutes-using-cell-phone-tracking-devices/383568/

On Thu, Mar 2, 2023 at 10:42 PM JENNIFER O'CONNOR [redacted] wrote:
Dear Mr. Vagoun,

Under item 1, there is an urgent need to train state and local law enforcement with regard to cyber and general privacy and security. The DC metro area is especially ripe for social engineering which when combined with dated cyber knowledge and skill sets means retirees and uninitiated are targets unaware of how easy it seems to be to gain control of a person’s private information. Personal experience has found that local law enforcement does not have the resources to look for patterns of emerging threats to individuals, families and companies because reporting and review is on an incident by incident basis with evidence based physical threat driving risk assessment and thus victim outcomes. Privacy violations are overwhelming and the current best source of info for retired non-cyber individuals is AARP magazine. It is the Wild West with regard to an individuals control of their data and what used to be difficult to do in terms of spoofing, etc can be Friday night chat for teenagers.

Open AI is going to make the problem worse rapidly as spoofing of legitimate official communications is automatible.

Best practices could immediately be updated and disseminated to level the proverbial playing field and aid citizens in forming ‘verified communities’ in real life as a check and balance on social media based identity. Further attention to the relationship of privacy loss, dignified help learning new cyber skills and mental health could actually make a difference in community building and turn the tide in identity and accompanying financial fraud.

Sincerely,
Jennifer O’Connor, PhD

Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

MITRE

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

MITRE's Response to the OSTP RFI Supporting the 2023 Federal Cybersecurity R&D Strategic Plan

March 3, 2023

For additional information about this response, please contact:

Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
[redacted]

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs); participate in and lead public-private partnerships across national security and civilian agency missions; and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resiliency. MITRE's 10,000-plus employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision making, technical findings, or policy recommendations.

MITRE has been at the forefront of cyber defense since the very beginning. MITRE draws from a wealth of deep technical expertise to create innovative solutions that address the ever-evolving challenges in cybersecurity.[1] We advocate a multi-faceted, interactive approach—which, in turn, broadens our impact through the power of collaboration. We know that working in partnership is crucial to national security, critical infrastructure, economic stability, and personal privacy. We serve as a trusted adviser across government (including both the national security community and federal agencies that serve citizens) and with other partners.

As part of our cybersecurity research in the public interest, MITRE has a 50-plus-year history of developing standards and tools used by the broad cybersecurity community. With frameworks like ATT&CK®,[2] Engage™,[3] D3FEND™,[4] and CALDERA™,[5] as well as a host of other cybersecurity tools, MITRE arms the worldwide community of cyber defenders. We give them vital information to thwart network intruders, build resiliency against future attacks, and develop assurance to overcome possible vulnerabilities.

Since 2014, MITRE has operated the country's only FFRDC dedicated to cybersecurity and the advancement of secure technologies, which supports the National Institute of Standards and Technology's (NIST's) National Cybersecurity Center of Excellence—a state-of-the-art collaborative hub where government, industry, and academia are building practical solutions to meet the real challenges businesses face each day. The National Cybersecurity FFRDC (NCF) is focused on the serious and growing risk cyber attacks pose to economic prosperity, public safety, and national security. The NCF brings multidisciplinary teams of cybersecurity architects,

[1] Cybersecurity. 2023. MITRE, https://www mitre.org/focus-areas/cybersecurity. Last accessed March 1, 2023.

[2] ATT&CK®. 2022. MITRE, https://attack mitre.org/. Last accessed March 1, 2023.

[3] Engage for Defenders. 2022. MITRE, https://engage mitre.org/defenders/. Last accessed March 1, 2023.

[4] D3FEND™. 2022. MITRE, https://d3fend mitre.org/. Last accessed March 1, 2023.

[5] CALDERA™-A Scalable, Automated Adversary Emulation Platform. 2021. MITRE, https://caldera mitre.org/. Last accessed March 1, 2023.

engineers, social scientists, and communications professionals together with NIST to design and build usable, real-world solutions.

A more detailed discussion of MITRE's cybersecurity history and impact is provided in Appendix A. Our recommendations in this response are based on insights gained through these extensive activities.

Introduction and Overarching Recommendations

The 2019 Federal Cybersecurity Research and Development Strategic Plan remains largely accurate and viable today despite technological advancements; COVID-19-driven changes in work, education, and communication paradigms; and new global conflicts and international competition that have taken place over the ensuing four years. This is a testament that the challenges in the prior Strategic Plan were both properly identified and difficult to overcome. That said, an updated 2023 Strategic Plan can also be significantly enhanced around the following areas.

Strategic Structure

The 2019 Strategic Plan did a good job of discussing areas of concern and then sharing supporting challenges and R&D goals for each. This is a critical aspect for most-impactful National Science and Technology Council (NSTC) activities. The 2019 Plan's organization for doing so, however, led to some confusion. Primary aspects within the strategy (Framing, Defensive Elements, Priority Areas, and Critical Dependencies) were largely treated independently, when in reality there is often great interdependencies among them that (1) research sponsors would need to properly prioritize and scope their efforts, and (2) researchers would need to consider to optimize the return on investment from their activities.

MITRE therefore recommends a more strategically comprehensive approach to developing and organizing the 2024 Strategic Plan. It may help to use a strategic planning framework that is consistent with the Government Performance and Results Act.

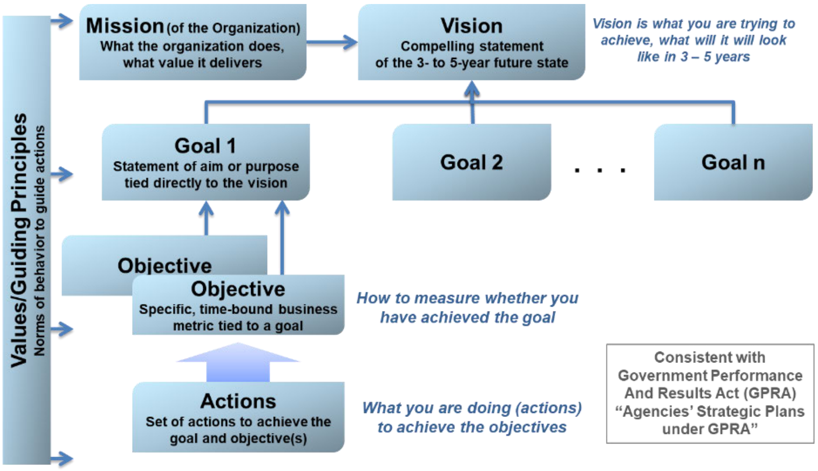

Values/Guiding Principles
Norms of behavior to guide actions
Mission (of the Organization)
What the organization does, what value it delivers
Vision
Compelling statement of the 3- to 5-year future state
Vision is what you are trying to achieve, what will it will look like in 3 – 5 years
Goal 1
Statement of aim or purpose tied directly to the vision
Goal 2
. . .
Goal n
Objective
Objective
Specific, time-bound business metric tied to a goal
How to measure whether you have achieved the goal
Actions
Set of actions to achieve the goal and objective(s)
What you are doing (actions) to achieve the objectives
Consistent with Government Performance And Results Act (GPRA) "Agencies' Strategic Plans under GPRA"

Figure 1. Strategic Planning Framework with Values/Guiding Principles

Such a structured planning framework provides:

- A set of values and principles that guides all subsequent activities
- A universal and compelling vision for the future state of cybersecurity
- A series of goals that collectively enables the vision to be met
- Subordinate research objectives and strategies for each goal that are specific and time-bound and that both help drive activities to successfully meet goals and provide the Executive Office of the President (EOP) the ability to measure progress

Collaboration

The 2019 document took the unfortunately common approach of being very predominantly internal government focused when public-private collaboration is required on this topic both to determine research priorities and to optimally drive capability advancement and adoption.[6,7] This has not been the case for a handful of most-successful prior NSTC activities,[8] and MITRE strongly recommends (1) pointedly folding in nongovernmental entities into the strategy development and implementation process and (2) taking actions to help ensure that research outcomes are maximally leveraged (e.g., also supporting standards development, transition to manufacturing, considering supply chain ramifications).

Similar NSTC strategies for technologies identified in the 2019 Priority Areas have also been developed and/or updated, thus requiring updated analyses. While doing so, MITRE recommends more explicit linkage between this Strategic Plan and those other strategies rather than the generalized discussion in the current document:

- What are the similarities and differences when investigating each issue through different lenses (e.g., cybersecurity vs. AI research)? How do both communities understand each other and collaborate?
- How would advancements in cybersecurity research impact these other strategies, and vice versa?

Linkages between this R&D Strategic Plan and the overarching National Security Strategy[9] should also be explicitly shown.

Supporting Small Entities

Cybersecurity is a nearly universal national concern, especially in the post-COVID remote connectivity environment, with incidents at one location creating cascading concerns at many others. Unfortunately, many (if not most) of the nation's cyber nodes are managed by small

[6] C. Ford, et al. A "Horizon Strategy" Framework for Science and Technology Policy for the U.S. Innovation Economy and America's Competitive Success. 2021. MITRE, https://www mitre.org/sites/default/files/2021-11/prs-21-1440-horizon-strategy-framework-science-technology-policy.pdf.

[7] Mid-Decade Challenges to National Competitiveness. 2022. Special Competitive Studies Project, https://www.scsp.ai/wp-content/uploads/2022/09/SCSP-Mid-Decade-Challenges-to-National-Competitiveness.pdf.

[8] D. Blackburn and M. Garris. A National Science and Technology Council for the 21st Century. 2021. MITRE, https://www mitre.org/sites/default/files/2021-09/pr-21-2388-national-science-technology-council.pdf.

[9] National Cybersecurity Strategy. 2023. The White House, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

entities or individuals who do not have the knowledge or resources to ensure their cybersecurity protection. Research into finding optimal ways to identify and then guide these entities into taking necessary actions is recommended. Such research into "raising the floor" of the nation's collective cybersecurity posture should not be forgotten.

Questions Posed in the RFI

2. What areas of research or topics of the 2019 Strategic Plan no longer need to be prioritized for federally funded basic and applied research?

None of the research topics included in the 2019 Strategic Plan have been "solved," and they all warrant consideration to continue being included in the updated research strategy. The topics would benefit from more strategic development and organization, as we discussed in the preceding section under "Strategic Structure."

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?

All topics within the 2019 Strategic Plan should continue, albeit with more specificity and targeted timelines. Doing so will both help drive activities and provide the EOP the ability to measure progress. Data-driven comments on several existing areas are included below to help develop this aspect of the strategy.

Use of Artificial Intelligence (AI) in Cyber Operations

Due to the growing number of threats to AI-enabled systems and the increasing use of AI in cybersecurity applications, the intersection of cyber and AI has become a critical area of research in recent years. From a national Cyber Science and Technology (S&T) Strategy point of view, several key research topics in the intersection of cyber and AI need further investment and investigation, including AI for cybersecurity, AI security, explainable AI, and privacy and data protection.

With the continued shortage of qualified cybersecurity professionals and the increasing volume and severity of attacks, there is a growing reliance on AI-driven cybersecurity defenses. A better understanding is needed of the implications of this increased reliance on AI for cybersecurity. For example, an AI defender must consider the system being defended and the mission it performs, and account for the uncertainties associated with sensing and action. It must also consider an attacker's capabilities to adapt their behavior based on what they observe about the system and the defender. In AI security, the unique opportunities presented by leveraging advancements in AI have led to an "AI arms race" between the U.S. and its adversaries.

AI-enabled systems have novel threat surfaces and unique vulnerabilities far beyond those of traditional cyber systems, as shown in the MITRE ATLAS™ framework,[10] which is modeled after and directly compatible with MITRE ATT&CK. These new AI threat surfaces are being

[10] MITRE ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems). 2023. MITRE, https://atlas mitre.org/. Last accessed February 27, 2023.

increasingly attacked and exploited[11] in operational systems across industry and government, and many organizations that operate AI-enabled systems are unaware of new threats[12] that cannot be fully understood or mitigated using current cybersecurity techniques. As recommended by the National Security Commission on Artificial Intelligence's Final Report,[13] organizations should stand up AI red teams to focus specifically on threats to systems incorporating AI capabilities.

With AI-enabled systems becoming more ubiquitous and complex, as in the recent adoption of ChatGPT, it is increasingly important to understand how those systems make decisions, the level of trust users have in those decisions, and measures of explainability of the systems. User adoption of AI systems will rely heavily on the trust users have in them. Concerns about privacy and data protection are paramount in the deployment of AI systems. AI systems rely on massive amounts of data, some of it private and sensitive, so developing methods to protect that data while still enabling the benefits of AI must remain a priority. The vulnerability of AI-enabled systems to open or insecure data sets requires additional scrutiny, particularly in recent developments of AI that rely heavily on semi- and self-supervised training methods. This concern is also true for many other autonomous systems, such as securing autonomous vehicles and the Vehicle-to-Infrastructure grid.

Smart Cities, IoT, and Critical Infrastructure

Several aspects of the Trusted Distributed Digital Infrastructure envisioned by the 2019 Federal Cybersecurity R&D Strategic Plan have yet to be realized and require further research investment.

The 2019 strategy speaks of pursuing design frameworks "that integrate safety, security, and privacy requirements, allowing system designers and developers to reason across all three domains concurrently." It continues to be the case that those three domains are often treated as disjoint concerns in smart city product development, particularly when it comes to the handling of data streams from smart city devices. Other cyber physical domains are beginning to address the security and safety aspects in a more unified way. However, this is not yet the case with privacy. Developers need better tools for linking privacy risks to smart city device and system design choices, as well as improved means to incorporate privacy-enhancing technologies (PETs) into these systems.

Many domains are newly incorporating Internet of Things (IoT) devices to enable new use cases. These may present specialized cybersecurity needs. As one example, IoT consumer and healthcare technologies within the connected digital health ecosystem—including device manufacturers, health delivery organizations, service providers, and government—have proliferated to accommodate individuals' desire to age with independence and to enable data collection/integration between patient/consumer and provider. This ecosystem is vulnerable to cyber attacks, with the growing older population as a susceptible target. Age-friendly user design related to cybersecurity is an overlooked but increasing risk. The healthcare to home trend requires improved cybersecurity, privacy, and usability of connected devices. Research is needed

[11] Case Studies. 2023. MITRE ATLAS, https://atlas mitre.org/studies/. Last accessed February 27, 2023.

[12] Market Guide for AI Trust, Risk and Security Management. 2023. Gartner, https://www.gartner.com/en/documents/4022879. Last accessed February 27, 2023.

[13] The Final Report. 2021. The National Security Commission on Artificial Intelligence, https://www nscai.gov/2021-final-report/. Last accessed February 27, 2023.

to incorporate assessment of cybersecurity vulnerabilities associated with age-related functional decline of users and to identify age-friendly security controls and mitigation.

Securing the hardware and software involved in smart city systems is another challenge area. Numerous solutions for security hardening and implementing trust and assurance have been developed over the course of many years of research. These advances, however, continue to find limited use in deployed systems. In our experience, the kinds of IoT and cyber physical systems involved in smart cities are the least likely to have incorporated such technology. In our work with device vendors, system integrators, and operators in this space, we have identified that many entities see the benefit of applying more advance security technologies to their products and systems but lack the resources or expertise to do so effectively. Research investment should be made on how to reduce the cost and complexity of applying and deploying existing hardware and software security techniques or, alternatively, developing easier-to-use methods with the goal of making them more accessible (economically and skills-wise) to developers and operators.

Cyber Resiliency

Notable progress has been made in cyber resiliency since the 2019 strategy. NIST guidance (Special Publication 800-160, Volume 2, Developing Cyber-Resilient Systems) was published in 2019 and revised in 2021. Cyber resiliency has been incorporated in federal and Department of Defense (DoD) systems planning and evaluation. Cyber resiliency is a unifying concept encompassing approaches such as segmentation, diversity, unpredictability, deception, and others. However, critical elements are still needed, such as a deep understanding of cost and effectiveness trade-offs, a robust range of available implemented resiliency mechanisms and resilient-by-default services, approaches to coordinate operation of resiliency across interconnected systems at scale, and development of use cases to support research in different domains. In addition, cyber resiliency designs are largely hand-crafted. More dynamic, automated capabilities are needed, both to adapt to changing situations and threats and to enable establishment and use of resiliency measures by staff with limited expertise.

The following are some important areas for research:

- Address at the Foundational Level. New laws such as the Bipartisan Infrastructure Law are making investments to improve sectors such as transportation in the critical concern areas of safety, climate, and workforce development. To achieve strategies that address these concerns, the sectors will be accelerating their adoption and integration of multiple technologies, with minimal focus on cybersecurity and/or privacy. Ensuring cybersecurity is addressed while keeping pace with such an acceleration of adoption is challenging. To mitigate this disparity, R&D efforts should focus on cyber resiliency strategies to ensure cybersecurity is addressed at the foundational level (e.g., strategies for moving to zero trust (ZT), cyber and privacy resiliency for smart cities). R&D efforts should also include developing methods for cyber resiliency at the systems integration level.
- Orchestrated Cyber Resiliency in Evolving Systems. Capabilities must be developed to coherently integrate and orchestrate cyber resiliency solutions (e.g., COTS, GOTS, emerging technology, innovative proactive defenses) into existing and emerging architectures, for scalability and to avoid creating gaps or new attack surfaces. As advanced cyber adversaries continue to evolve—and may be able to exploit

vulnerabilities installed in shared codebases or commonly used products—this orchestration needs to be ongoing; there is no "one and done" against the advanced persistent threat.

- Dynamic Mission Resilience at Scale. The challenge of ensuring secure and resilient operations exists at multiple scales and in a dynamic environment. Solutions exist for individual systems, services, and infrastructures, but often assume a static environment. Critical infrastructures and essential functions of large organizations depend not on an individual system but on systems of systems. An essential function's dependencies are themselves often dynamic, based on mission phases. The challenge is to orchestrate capabilities and practices dynamically across different constituent elements as they carry out mission functions. Next-generation capabilities will need to integrate mature resiliency capabilities (e.g., non-persistence, deception) with current commercial architectures (e.g., cloud services, zero trust architectures) and provide readily available, pre-packaged, threat-informed defensive courses of action to prevent cyber adversaries from achieving their goals. These capabilities will require sophisticated decision engines that manage and adapt resiliency mechanisms and that assist in orchestrating decisions made at different levels of enterprises and interconnected systems.
- Innovative Proactive Defenses. Cyber resiliency techniques and technologies that counter advanced adversaries need not be predicated on first detecting the adversary. New industry-provided technical capabilities (e.g., in ZT technologies and cloud services) provide opportunities for supporting proactive cyber resiliency, potentially in combination with enhanced ICAM (Identity, Credentialing, and Access Management), cryptographic obfuscation, and cross-domain filtering for high-trust segmentation. Attention should also be given to extending and adapting resiliency techniques to non-enterprise IT architectures (e.g., operational technology (OT), IoT, and industrial internet of things environments).
- Transforming Governance and Analytic Foundations for Cyber Resiliency. The transition to dynamic resiliency at scale involves shifts in governance, informed by threat-informed, risk-sensitive analysis methods. Guidance on effective and scalable implementation of advanced cybersecurity and cyber resiliency capabilities is needed to underlie definition, governance, and implementation of cybersecurity doctrine across enterprises involving on-premises, cloud, and multi-cloud IT environments. To enable and accelerate evolution from compliance-oriented toward threat-informed, risk-sensitive risk governance, and to maximize the usability of the guidelines and doctrine, tools (e.g., CREF Navigator™) and analytic methods for identifying cyber resiliency solutions and making risk management decisions must be refined and extended to apply to a broader range of system types and operational environments.
- Cyber Resiliency Analysis for Small and Medium-Sized Organizations. Small and medium-sized organizations depend on managed services (e.g., internet, cloud-based application services, backup/restore services) and pre-packaged application systems, often from niche providers. Methodologies are needed to enable small and medium-sized managed service providers and developers of commodity application systems to take advantage of cyber resiliency engineering and identify cyber resiliency capabilities to prioritize in their service offerings and applications. Such methodologies must be based on factors that have been found to be relevant in prior engineering and research efforts, and on repeatable, explicable, and extensible reasoning methods. Factors that can drive

the selection of cyber resiliency capabilities include prior investments and legacy technology (which can limit what can be implemented, but also offer functional capabilities for security, continuity of operations, and safety that can be leveraged for cyber resiliency), legal or regulatory requirements, architectural trends (e.g., ZT, convergence of IT and OT), physical constraints, and operational constraints (e.g., limited user expertise or attention). Research is needed into how to capture such factors, apply and adapt them to the setting of small and medium-sized organizations, and make the analysis extensible to different domains or sectors and operational environments.

- Resilient-by-Default Cloud Services. Default cloud configurations are set for quick deployment and are configured with only minimal Risk Management Framework or Federal Risk and Authorization Management Program (FedRAMP) security. Orchestration engines (e.g., Kubernetes, Terraform) help automate the infrastructure deployment, but they leave infrastructure configuration and application of mission-specific resilience and security to the client organization. Capabilities are needed to derive and efficiently combine cyber-resilient and optimal ZT-compliant software-defined networking/provisioning baselines for cloud environments, informed by operational need from criticality analyses.

Microelectronics Supply Chain

The U.S. economy, military, and commercial sector are highly dependent on advanced microelectronics (uE), but the globalization of the uE supply chain—from design through manufacturing—has introduced numerous threats to the security of these components in the form of hardware trojan horses (HTH), malicious modifications, and counterfeit parts. Counterfeit parts alone are estimated to cost semiconductor manufacturers more than $7.5 billion annually in lost revenue. Additionally, the threat of HTH or other malicious modifications has not only cost the DoD billions of dollars for protection but also precluded many DoD programs from using state-of-the-art microelectronics due to a lack of trusted sources.

Privacy

PETs represent one set of a series of tools that can be used to protect data and minimize legal, privacy, and ethical risks.[14] Modern PETs offer the potential to protect sensitive data while also helping government agencies achieve their mission goals. PETs should be considered in furtherance of recently issued Presidential Executive Orders and goals on Signals Intelligence data sharing, Securing and Protecting Access to Healthcare Services, Ensuring Responsible Development of Digital Assets, and collective efforts to use healthcare data to find a cure for cancer. Research regarding the different types of PETs and their effectiveness in different scenarios should be performed so that appropriate PETs are selected for adoption and implemented effectively. Also needed is further development of crypto-supported "zero-knowledge proofs for privacy" and "differential privacy."

Privacy threats are currently not well understood, and privacy threat modeling is not actively included in risk management processes within many organizations. It is important to effectively assess privacy threats and use privacy threat information as input for PETs selection and privacy

[14] Response of The MITRE Corporation to the OSTP RFI on Advancing Privacy-Enhancing Technologies. 2022. MITRE, https://www mitre.org/sites/default/files/2022-08/pr-21-01760-26-response-mitre-corporation-ostp-rfi-advancing-privacy-enhancing-technologies.pdf.

operations overall. Privacy risk models need to expand beyond consequences (which most of them focus on) to characterize threats and vulnerabilities as well. MITRE is currently developing a Privacy Attack Taxonomy named PANOPTIC that will provide a standard structure for mapping privacy attacks that can be used to model privacy threats and facilitate privacy risk management, including PETs selection. Security risk modeling typically focuses on confidentiality-based threats to information about individuals (e.g., data breaches). However, the Privacy Attack Taxonomy will enable identification of threats beyond those typically addressed in security risk modeling (e.g., threats related to consent; notice; and inappropriate use, sharing, or retention of information about individuals). This expansion in focus will also enable consideration of a broader set of PETs for potential implementation. Further research is needed in the area of privacy threat modeling and its implementations for privacy risk management.

AI ethics and privacy are critical considerations when developing and implementing artificial intelligence systems. As AI becomes increasingly integrated into daily life, it is essential to ensure that these systems are designed and used in ways that are ethical and transparent, and that respect people's privacy. Ethical considerations might include ensuring that AI algorithms do not discriminate against certain groups of people, protecting people's autonomy and dignity, and ensuring that AI systems are used for the common good. Privacy considerations might include protecting people's personal data, ensuring that data is collected and used only with individuals' consent, and ensuring that data is stored and transmitted securely. As AI continues to advance, research is needed to identify how best to address these critical ethical and privacy concerns to ensure that AI is used in a way that benefits society as a whole.

The IoT raises a host of privacy-related questions in need of more systematic exploration. These are difficult issues because they are cross-cutting. The architectural progression from lightweight sensors to sophisticated analytical systems complicates matters due to the significant shift in properties at almost every stage of the pipeline. The nature and implications of such shifts in terms of privacy have not been well analyzed, much less tackled. Emergent properties are likely at these points, including the social effects of implicitly infrastructural surveillance. Existing privacy risk models—even the more sophisticated ones—struggle to effectively capture these kinds of concerns. Privacy-enhancing technologies cannot be relied on to ride to the rescue as their use cases tend to be narrowly focused, lacking any calculus regarding composability. Approaches to data and AI ethics, meanwhile, tend to emphasize technical correctives and procedural remedies while side-stepping more fundamental questions regarding power asymmetries and the effects of distributed yet interacting decisions, among other issues. Holistically addressing privacy in IoT environments requires more formal and rigorous investigations into all of these topics, but from distinct vantage points.

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.

Defensive Capabilities for Under-Resourced Entities

Ransomware attacks on mission/business-critical operations have increased over the past four years, with many organizations unable to recover from them. While small and medium-sized businesses (SMBs) tend to believe they are too small to be targeted by ransomware (or other attacks), evidence does not support this belief. Furthermore, approximately one-third of SMBs in the U.S. reported they had to close following a ransomware attack. Those that did not shutter suffered significant loss of revenue.[15] This is a disturbing trend, especially given that small businesses generate 44 percent of U.S. economic activity.[16] Research that develops knowledge and tools to help these entities should be considered.

Establishing Partnerships with the Explicit Purpose of Enabling Assurance Evaluations of Large ML Models

Large machine learning (ML) models are increasingly applied to solve problems such as drug discovery[17] and protein folding,[18] with broad implications for humanity. However, the negative implications of generative models are not yet well understood. For example, models could be used for generating toxic molecules.[19] Similarly, large models that enable the generation of text[20,21] and source code[22,23] at scale could be used to generate adverse content to manipulate people or create malware, respectively.

Tools to Understand the Pedigree of Software and Greater Visibility of Its Supply Chain

Vulnerabilities in third-party software are the root cause of one of the most expensive cyber incidents on average, that organizations endure.[24] Research to understand and support software supply chain security should be considered including the need for capabilities such as software bills of materials (SBOMs) and how to adopt/implement their usage as well as methods and mechanisms an organization can use to determine whether appropriate choices were made for securing the software during the creation process. This includes information about the compilation and formulation options used in transforming the source components and parts into the resultant software.

[15] Ransomware: The True Cost to Business. 2022. Cybereason, https://www.cybereason.com/hubfs/Ransomeware_True_Cost_e-book_NewBrand.pdf.

[16] Small Businesses Generate 44 Percent Of U.S. Economic Activity. 2019. U.S. Small Business Administration, https://advocacy.sba.gov/2019/01/30/small-businesses-generate-44-percent-of-u-s-economic-activity/. Last accessed March 1, 2023.

[17] F. Urbina, et al. Dual Use of Artificial-Intelligence-Powered Drug Discovery. 2022. Nature Machine Intelligence, https://www nature.com/articles/s42256-022-00465-9. Last accessed February 27, 2023.

[18] J. Jumper, et al. High Accuracy Protein Structure Prediction Using Deep Learning. 2020. Fourteenth Critical Assessment of Techniques for Protein Structure Prediction (Abstract Book).

[19] F. Urbina, et al.

[20] N. Stiennon, et al. Learning to Summarize from Human Feedback. 2020. 34th Conference on Neural Information Processing Systems, https://proceedings neurips.cc/paper/2020/file/1f89885d556929e98d3ef9b86448f951-Paper.pdf.

[21] J. Devlin, et al. BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding. 2018. ArXiv, https://arxiv.org/pdf/1810.04805.pdf&usg=ALkJrhhzxlCL6yTht2BRmH9atgvKFxHsxQ.

[22] Y. Li. Competition-Level Code Generation with AlphaCode. 2022. Science, https://www.science.org/doi/10.1126/science.abq1158. Last accessed February 27, 2023.

[23] OpenAI Codex. 2021. OpenAI, https://openai.com/blog/openai-codex/. Last accessed February 27, 2023.

[24] Cost of a Data Breach 2022. 2022. IBM Security, https://www.ibm.com/reports/data-breach. Last accessed February 27, 2023.

Executive Order 14028 has motivated much progress toward requiring attestations from software suppliers regarding which of the items in NIST's SP800-218, Secure Software Development Framework, an organization applied when developing its software. However, there are no standards for how the software developers can be captured and conveyed in a manner that others can understand, machines can act on, be linked to the SBOM for the software, and that consumers of the software will have a reason to trust the information and its source.

There are promising approaches in the Linux Foundation's in-toto project as well as the Internet Engineering Task Force Supply Chain Integrity, Transparency and Trust working group. However, many open questions remain requiring critical thinking and evaluation of these proposals in order for the U.S. government and industry to rely on them for their future software and dynamic supply chains. Accelerating the convergence and maturity of these complementary efforts will address a massive capability gap that sorely needs to be addressed to achieve an overall articulated framework that can provide assurance of software and can convey the appropriate information tailored to the situation the software will be used in. An evidence-based approach that allows for self- and third-party verification in a highly automated manner would provide an evidence chain to demonstrate and measure trust of the pedigree and provenance of the software supply chain.

Increasing Hardware Assurance

The foundation of trust in computer systems is built on trust in hardware, and trust in hardware is in turn based on trust in hardware components that are of critical importance to the properties of the computer system. An important goal in advancing the assurance of computer systems is to constantly look for architectures that can be trusted based on fewer or simpler hardware or software components.

Also needed are hardware assurance primitives that are easy and cost-effective to integrate into industrial control systems, vehicles, and IoT devices. Poorly understood cost-benefit continues to be a barrier to adoption.

Cyber Deception and Adversary Engagement

Cyber deception, when used as an integral element of the defensive cyber framework, provides benefits across the goals of deter (diminish value of spoils), protect, and detect by providing high-quality indicators of compromise and techniques used to exploit and in current manifestations provide information to defenders to initiate response options. As AI/ML is increasingly used in attacking systems, deception can be utilized to counter and respond to increasing sophistication and speed of attacks. Needed capabilities include:

- Dynamic adaption of a deception environment to vary the perceived attack surface
- Providing deeper adversary attack opportunities while yielding no valuable data or exposure of protected systems
- Utilization of hyper-instrumentation from the deception environment to create widely available defensive signatures in real time to accelerate both detection to the locally defended system and distribution to standard defensive systems that may not deploy cyber deception
- Generation of response options to dynamically change the operational configuration of the defended system while maintaining the adversary's perception of the environment

- Real-time generation of defensive options that could be applied locally to thwart or render an attack ineffective
- AI-driven adversary behavior to classify and evaluate cyber deception techniques to advance testing and evaluation of deceptive capabilities
- Generation of defensive options that could be distributed to service providers to change the engagement or redirect an attack

Individually, each capability advances the objectives of the defensive framework pillars; combined, they provide the ability to change the defensive posture from one of passive response to active engagement to reduce the effectiveness of an attack.

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.

Preparing for the Post-Quantum Crypto Migration

Over the next 5–10 years, it will become increasingly important to move beyond today's factoring or discrete logarithm-based asymmetric cryptography toward alternative methods collectively known as "post-quantum cryptography." Migrations of cryptographic algorithms are notoriously slow and difficult. Among topics particularly relevant to post-quantum migration include protocol-oriented and standards-oriented study designed to anticipate and remove obstacles to adoption, as well as to minimize the impacts of increased resource demands from post-quantum algorithm use. Additional challenges include:

- Developing and improving post-quantum versions of alternative asymmetric crypto primitives such as identity-based encryption, attribute-based encryption, and so on
- Maturing post-quantum fully homomorphic encryption and developing a standard framework for expressing homomorphic transformations to enable applications

Embedded Security (Side-Channel, Fault Injection, etc.)

Embedded systems security is essential to the civilian, defense, and intelligence communities in their efforts to secure embedded systems. Embedded systems are the backbone of all modern infrastructure, sensing, navigation, communication, and weapons system capabilities. These capabilities have been applied to secure infrastructure and end-user equipment for a broad set of areas, including mobile, medical, transportation, and navigation. New R&D is necessary to better understand emerging threats and develop defensive technologies and tools to protect these systems and combat supply chain threats.

Zero Trust

ZT principles are being adopted broadly to reduce exposure and limit the ability for attacks to move freely within enterprises. Research is needed to advance the sophistication and effectiveness of architectures incorporating ZT principles, including:

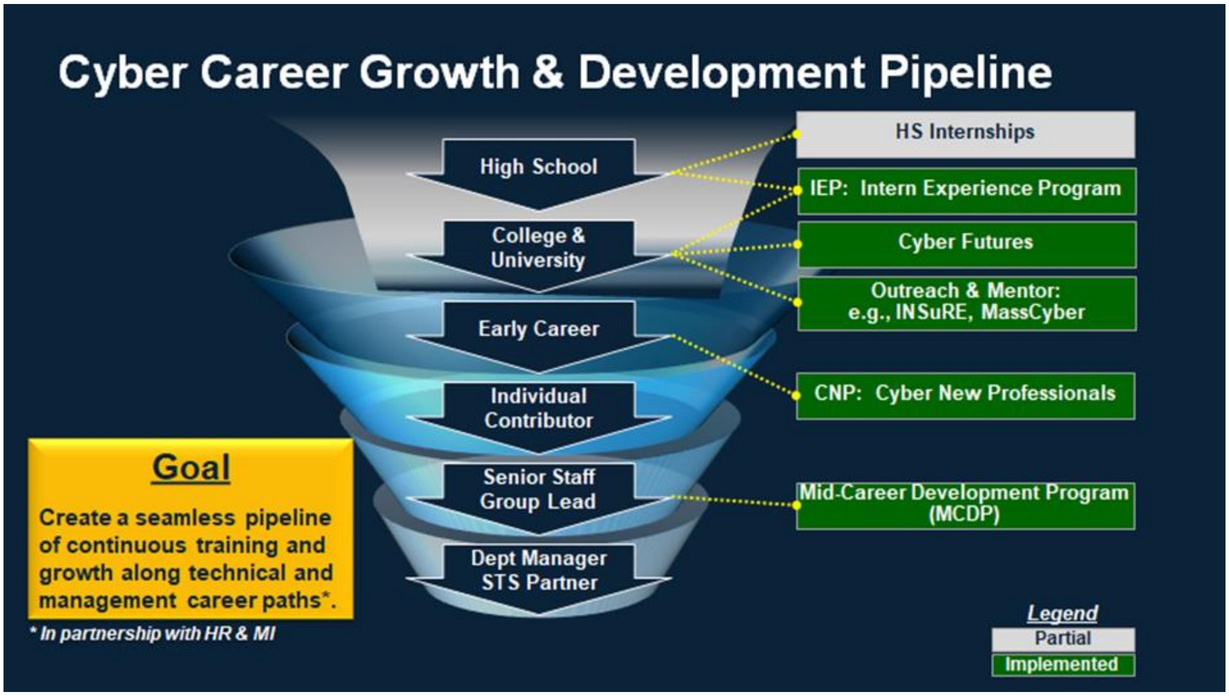
- Application of ML and AI to ZT capabilities such as automation, threat detection, vulnerability management, access decision, risk evaluation, and detection. Additional research will be required in this area to stay ahead of the expected use of AI, ML, and automation by adversaries.
- Approaches for interoperability between ZT Policy Enforcement Points (PEPs), orchestration platforms, services, and the like, which could include needed standards for information exchange between platforms and interpretation of telemetry.
- ZT approaches for architectures expanding beyond information technology to incorporate OT, 5G and other advanced networking capabilities, and Web 3.0/Metaverse.
- Dynamic policy enforcement and enhancing interoperability between ZT products and architectures, including the ability to communicate the point-in-time risk posture of subjects and resources between ZT components.
- Ways to fully incorporate access-relevant information and PEPs available from applications into end-to-end ZT risk evaluation and enforcement to enable more data-centric security.

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?

MITRE has previously responded to an Office of the National Cyber Director (ONCD) RFI that was wholly focused on this specific question.[25] Our overarching recommendation within that response was that maximizing growth within the cyber career path requires targeted and cohesive development throughout its pipeline while simultaneously recognizing that staff may onboard and leave at various stages. MITRE conceptually views this pipeline as depicted in Figure 2, which could easily be genericized for application at the national level and complement the suite of cyber workforce-related tools and approaches already offered by the Office of Personnel Management and other federal agencies.[26] It could also serve as a model for the private sector, though some adaptation will be required for smaller, less-technical organizations.

[25] MITRE's Response to the ONCD RFI on a National Cyber Workforce Strategy. 2022. MITRE, https://www mitre.org/sites/default/files/2022-11/pr-22-01891-09-mitres-response-oncd-rfi-national-cyber-workforce-strategy.pdf.

[26] For example, see Workforce Planning for the Cybersecurity Workforce. 2023. Office of Personnel Management, https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/. Last accessed March 2, 2023.



Cyber Career Growth & Development Pipeline

High School

College & University

Early Career

Individual Contributor

Senior Staff Group Lead

Dept Manager STS Partner

HS Internships

IEP: Intern Experience Program

Cyber Futures

Outreach & Mentor: e.g., INSuRE, MassCyber

CNP: Cyber New Professionals

Mid-Career Development Program (MCDP)

Goal

Create a seamless pipeline of continuous training and growth along technical and management career paths*.

** In partnership with HR & MI*

Legend

Partial

Implemented

Figure 2. Cyber Career Growth and Development Pipeline

We have developed learning programs at, and specific to, multiple stages within this pipeline, which are discussed in the response to the Office of the National Cyber Director RFI..

MITRE has also developed a Cyber Workforce Development Framework to help nations build a cyber workforce strategy. This framework is being applied on behalf of the U.S. State Department in several partner nations around the world, and by the Department of Homeland Security's Cyber Development, Education, and Training program in response to Solarium Commission recommendations.[27] Findings indicate that governments are usually best positioned to integrate the cyber ecosystem of industry, academia, cyber professionals, commercial training programs, and national security needs. They can convene leaders, develop standards, set long-range goals, incentivize progress and cooperation, and eliminate barriers. But government is not enough. The main finding of the framework survey is that public-private partnerships are key. Together, governments and private organizations can develop standards for training, job descriptions, and career pathways; develop policies that facilitate workforce development; and identify regional barriers for cyber career seekers. This framework can be used to collaboratively identify educational and workforce development needs for a wide range of entities:

- Nations transitioning to a digital economy or adjusting incentives and pipelines to increase investment in and access to cyber professionals
- City, state, or regional planning groups focused on increasing high-tech employment and an associated ecosystem
- Industry and academia seeking to grow a local talent pool

[27] Construction of the framework began with a broad survey of tech workforce development approaches across nations of various sizes and economies, development non-governmental organizations, and other subject matter experts. They identified commonalities, needs, and best practices in several categories and then synthesized the information into the framework, focused on key areas and approaches.

- Government agencies at all levels developing policy and/or legislation to incentivize cyber talent development and retention in key functional areas

Workforce Development through Gamification

Gamification of hands-on project-based learning activities is a proven technique for significantly improving learning outcomes and making complex subjects more accessible to a wider range of students. Since 2015, MITRE has been perfecting this technique as applied to its Embedded Capture-the-Flag (eCTF) event—a nationwide competition for high schools and colleges that provides an unmatched learning experience for embedded systems security (i.e., Secure Edge/IoT computing).

Embedded systems (like those found in smartphones, modern automobiles, and many military systems that are critical for national security) are significantly different from other computing systems. As such, these systems face unique security threats that require different skillsets than those needed for addressing traditional cybersecurity. MITRE noticed an educational gap in U.S. schools and universities in curricula for embedded systems security—and this gap largely still persists today.

To reduce this gap, MITRE developed the eCTF competition in 2015, and has successfully used it to raise awareness of this important field of study and to spur an interest among the nation's student population. The competition design was based on existing "capture-the-flag" competitions that have become popular for teaching traditional cybersecurity, but with three significant differences that make the eCTF unique:

1. A focus on embedded systems. Teams implement designs and conduct attacks on software running on real physical hardware.
2. Attack-and-defend. Teams design and implement their own solutions to the challenge and then develop attacks against the designs of other teams.
3. Extended time. The competition runs for three months over the spring semester from mid-January through mid-April to allow time for teams to design, implement, and attack.

Since the first year with only four universities, the competition has grown to 80 schools and over 500 students ranging in level from high school to Ph.D. Participant surveys indicate that the competition has greatly influenced students toward pursuing careers in embedded security and related fields.

The eCTF has also proved to be a powerful tool in diversity, equity, and inclusion. Through targeted outreach, the eCTF has been able to engage with three Historically Black Colleges and Universities and eight other Minority Serving Institutions, engaging communities historically underrepresented in embedded security and adjacent fields. After their inaugural participation in the eCTF, professors at Morgan State University published a paper about their success at leveraging the eCTF to attract minority students to their programs in secure embedded systems.[28]

[28] M. Kornegay, et al. Engaging Underrepresented Students in Cybersecurity Using Capture-the-Flag(CTF) Competitions (Experience). 2021. ASEE, https://peer.asee.org/engaging-underrepresented-students-in-cybersecurity-using-capture-the-flag-ctf-competitions-experience. Last accessed February 27, 2023.

Appendix A. Overview of MITRE's Cybersecurity Activities

Among MITRE's most renowned capabilities, cybersecurity is a core competency demonstrated by decades of seminal innovations and contributions to advancing the field. Throughout our 50-plus year history in cybersecurity, we have earned recognition for game-changing advances gained through collaborative processes and methods, starting with major contributions to the first government series, the Orange Book and Rainbow Series. Most innovations are widely adopted and used today, from the original designs of cross-domain architectures using MITRE's Bell LaPadula model to CVE®, the taxonmy used to characterize vulnerabilites, to more recent innovations such as ATT&CK® and CALDERA. We work across government, industry, and academic partners to develop, identify, and adopt new concepts and apply threat-informed engineering to build and defend resilient enviornments. In addition to MITRE's own innovations, we draw from other organizations' best-of-breed solutions and capabilites to bring them to our sponsors.

MITRE has broad and deep knowledge of secure and resilient architectures, cyber technologies, and cybersecurity operations that enable us to knowledgeably approach a comprehensive range of cyber-related challenges. In addition, MITRE has deep strength in the areas of cryptography, privacy, and cyber supply chain security, and continues to transform vulnerability management and threat intelligence.

MITRE works across the national security and civil sectors and industry to advance secure architectures and defensive cyber operations, develop innovative cybersecurity solutions, and analyze the cybersecurity implications of new and emerging technologies and applications.

MITRE leverages these diverse areas of cybersecurity expertise in a multidisciplinary perspective to assess emerging events such as SolarWinds, an attack that combined multiple direct and supply chain exploit strategies.

Innovation Highlights

MITRE balances classic cyber defense approaches and innovation with a strong emphasis on leveraging cyber threat intelligence to respond and adapt quickly to cyber attacks. To accomplish this, we form partnerships that promote sharing cyber threat information and effective tools. Our strategy thrives on a foundation of unrelenting innovation and operational experimentation. MITRE's cyber expertise includes wireless and wired network security, mobile device security, threat intelligence and hunting, cybersecurity assessments, Internet of Things security, medical device security, and adversary emulation, among other areas. Examples of MITRE's cyber security innovations are listed below.

Originator of ATT&CK® – Adopted by Industry and Government

MITRE is the creator and maintainer of the game-changing ATT&CK framework, which codifies the cyber attack tactics, techniques, and procedures known to be used by sophisticated adversaries. ATT&CK is populated by validated reports of adversary attack techniques contributed by a worldwide community of cybersecurity experts, creating synergy that favors the defender. ATT&CK quickly became the international nexus of public information about techniques revealed by adversary attacks and exploits. It has been used in many organizations as a basis to develop new detection capabilities and to analyze the coverage of their cybersecurity sensors and countermeasures. As an example, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) recently released a guide, titled Best Practices for Mapping to MITRE ATT&CK®, in an effort to encourage common language across organizations for threat identification and analysis. ATT&CK covers attack techniques against enterprise information technology, mobile technology, and industrial control systems, and its scope continues to broaden.

Originator of CVE®: The Taxonomy and Registry for Cybersecurity Vulnerabilities

MITRE originated CVE, the universally relied-upon Common Vulnerabilities and Exposures registry, and maintains it for CISA. Working with industry, MITRE tracks, validates, and publishes reported vulnerabilities. This MITRE innovation played an essential role in creating a cohesive cybersecurity community by enabling unambiguous communication among cybersecurity experts, vendors, and user organizations about what vulnerabilities exist, in what software they are found, and what cybersecurity mitigations can counter them. MITRE also created and maintains CWE^{TM}, the Common Weakness Enumeration, which catalogs the types of weaknesses in code that can lead to security vulnerabilities, with active input from the cybersecurity community. This allows recognition of weaknesses that are present in specific software components and creation of acquisition requirements specifying what must be eliminated. CWE publishes an annual list of the top 25 most dangerous software weaknesses as a way of drawing public attention to the most urgent issues to fix. CWE also recently, in partnership with Intel Corporation, expanded its scope to include hardware weaknesses.

Operator of NCF, the Nation's Only Cyber-Focused FFRDC

MITRE operates the nation's only cyber-focused FFRDC, the National Cybersecurity FFRDC (NCF), in support of the National Institute of Standards and Technology (NIST) Cybersecurity Center of Excellence (NCCoE). NCF's mission is to enable strong, practical, and resilient cybersecurity for all Americans. Sponsored by NCCoE, NCF advances the state of cybersecurity practice across industry, infrastructure owners/operators, commercial solution providers, government, and academia. With multiple laboratories to create exemplary integrated cyber solutions in topics ranging from Zero Trust Architecture to identity and access management, to medical devices, to commercial space systems, NCF develops practice guides and explores a range of pressing cybersecurity needs.

Leader in Cyber Resiliency

MITRE has been at the forefront of establishing the field of cyber resiliency for the past decade. MITRE built a community across government, industry, and academia, in part by creating seminal artifacts and by establishing annual workshops. The Cyber Resiliency Engineering Framework (CREF) developed by MITRE is the comprehensive technical framework providing guidance for implementation of cyber resiliency promulgated in NIST Special Publication (SP) 800-160 Vol. 2 (Rev 1): Developing Cyber-Resilient Systems. The CREF provides the keys to making systems across the government and more broadly in the private sector more resilient to cyber compromises and attacks, allowing them to continue accomplishing their missions without disruption in the face of sophisticated cyber attacks.

Recently, we held ResilienCyCon, which brought together experts from government, industry, and academia to discuss how cyber resiliency has been adopted in different domains and fostered synergy across the community. Industry, government, and academia leaders have adopted MITRE's Cyber Resiliency approach, as evidenced by speakers including the Google Cloud CISO; Amtrak CISO; Options Clearing Corporation Chief Security Officer; Ariam VP for Cybersecurity and Incident Response; Head of Cyber Resiliency at Standard Chartered Bank (in Poland); and senior government officials from OSD, Army, and NIST. Internationally, as part of the IEEE Conference on Cyber Security and Resilience (CSR), MITRE has partnered with PNNL for the past six years to co-lead the CSR Workshop on Cyber Resilience and Economics.

The CREF Navigator™, which makes the CREF more usable and accessible, is a major contribution in helping to bring its benefits to more organizations. CREF Navigator is a tool for effective visual browsing, distilling complex concepts and relationships into understandable tailored views to enable architectural and engineering discussions and analysis (see MITRE Launches Cyber Resiliency Engineering Framework Navigator). Ron Ross, NIST Fellow, regularly posts about the importance of the CREF and the CREF Navigator to enhance the resilience of the nation to cyber attacks.

Thought Leader in Health Cybersecurity

MITRE has provided cybersecurity support to the Food and Drug Administration's (FDA's) Center for Devices and Radiological Health since 2014. To help FDA understand the different stakeholder perspectives in coordinated vulnerability disclosure, MITRE conducted a stakeholder study. MITRE co-authored with FDA a journal article summarizing The Evolving State of Medical Device Cybersecurity in AAMI Biomedical Instrumentation & Technology.

MITRE developed the Playbook for Threat Modeling Medical Devices based on a series of threat modeling bootcamps sponsored by FDA and conducted by MITRE, the Medical Device Innovation Consortium, to encourage the adoption of threat modeling in the design and development of medical devices. Threat modeling is an element of FDA's new draft premarket guidance, and the playbook offers examples that medical device manufacturers can use to develop threat modeling training and aid in the adoption of threat modeling best practices.

MITRE is also working with hospitals to prepare for and respond to ransomware and other cyber attacks, since they are highly targeted. Hospitals develop and exercise emergency response plans for all kinds of emergencies, but we are helping them include cyber incidents, which typically involve longer downtimes and more widespread disruptions compared with other incidents. MITRE recently published the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook to capture some best practices. To help hospitals and others deal with ransomware threats, we created the Ransomware Resource Center (https://healthcyber.mitre.org) and tailored a lightweight assessment methodology Cyber Operations Rapid Assessment (CORA)for healthcare delivery systems (Threat-Informed Cybersecurity Operations for Healthcare Delivery Organizations).

MITRE has provided technical analysis to support FDA's regulatory role and has developed tools and documents to help medical device manufacturers implement FDA's guidance, which represents its current interpretation of the regulations. MITRE developed a rubric for applying the Common Vulnerability Scoring System to medical devices that considered the clinical context, which FDA qualified as a Medical Device Development Tool, and helps medical device manufacturers assess the exploitability of vulnerabilities.

Leader in Cyber Supply Chain Security and System of Trust

MITRE has been influential in developing approaches to improve the security of the software supply chain against being used to infiltrate cybersecurity attacks and malware into our systems. MITRE was one of the original contributors to the concept of a software bill of materials (SBOM) to capture and track the supply chains inherent in widely used software products that organizations use. SBOMs are now mandated in the May 2021 Cybersecurity Executive Order 14028, and MITRE is assisting early adopters in developing the first SBOMs. MITRE has also developed the System of Trust™ framework that defines attributes of suppliers, services, and products that should be scrutinized to assess supply chain risk, as well as mitigations that can be instituted to reduce risk.

Creator of CALDERA™ – Adversary Emulation to Automate Assessments

Seeing a need to provide tools that test by using the same TTPs adversaries use, MITRE developed CALDERA, a cybersecurity framework that empowers cyber practitioners to develop and use automated security assessments on a scalable, automated adversary emulation platform. The platform is used by red teamers to develop tests, as trainers for red teams and defenders, for testing defensive tools, and for assessing networks through "real" simulated (controlled) adversary attacks. The platform is being extended to support operational technology.

Originator of Engage™ – Advancing Tools for Adversary Engagement

MITRE has developed a collection of resources centered on MITRE Engage, a matrix designed to give decision makers and defenders the tools and common language they need to plan and analyze adversary engagement. Adversary engagement is an iterative, goal-driven process that leverages cyber denial and deception in unison to drive strategic planning. Unlike other defensive technologies, such as antivirus, adversary engagement technologies cannot be considered "fire and forget" solutions. Rather, an organization must think critically about what their defensive goals are and how denial, deception, and adversary engagement can be used to drive progress toward these goals.

Thought Leader in Defensive Cyber Operations

MITRE combines cutting-edge research with direct experience and threat intelligence from live environments to establish and evolve operations centers. We engineer solutions that work in real operations, identify where to invest scarce resources to optimize defense, and assess the ability to defend against real adversaries. Last year, MITRE published a book—11 Strategies of a World-Class Cybersecurity Operations Center—based on lessons learned across multiple government sponsors.

Creator of SAF – Automating Security Assessments and Baselines

The MITRE Security Automation Framework (SAF) is a set of tools designed to assist developers and security professionals in assessing systems against standards or custom baselines, apply automated mitigations, and ultimately harden systems. SAF provides open-source tools that help build security directly into software. This includes tools for developing security content based on specific security requirements as well as visualizing the security testing of any tool and trending over time. SAF is used at MITRE and in several software pipelines including the

Department of Defense, DHS, the Intelligence Community, and others. Several commercial companies have adopted SAF as well.

Additional Cyber Capability Highlights

MITRE operates special-purpose laboratories where we assess, engineer, and integrate technologies and processes to fill gaps and create affordable solutions to customer problems. Our laboratory capabilities include tools and techniques for evaluating and enhancing enterprise-class cyber defense products, applied mission resilience techniques, cyber-physical security technologies, cloud technologies, and cross-domain solutions.

Zero Trust and Cloud Architectures

MITRE is working across the federal government to evolve to Zero Trust Architecture principles and to secure sensitive data and applications in public and private clouds. We develop secure and resilient solutions to integrate cloud services with enterprise on-premises systems and business services. This includes taking an end-to-end perspective to ensure protection of data-at-rest, data-in-transit, data-in-use, and ransomware mitigation, and assessing appropriate security controls as commercial Cloud Service Providers (e.g., AWS, Azure) act as "scalers" to become 5G system and service providers. Expertise ranges from developing best practices in cloud security, design, migration, and operations to evaluating Cloud Service Providers, to implementing cyber analytic cloud environments.

MITRE has developed the CAVEAT (Cloud Adversarial Vectors, Exploits, and Threats) framework to capture cloud-specific adversary behaviors and potential exploits. CAVEAT will be evolved and maintained by the Cloud Security Alliance in collaboration with MITRE.

Cybersecurity Strategy, Policy, and Governance

MITRE has worked with many government organizations to develop and evolve their cybersecurity strategies and implementation roadmaps with focuses ranging from enterprise modernization to cybersecurity science and technology. In emerging nations, MITRE has worked with the State Department to develop national strategies to advance cybersecurity in their organizations, practices, workforces, and populations.

Cybersecurity Guidance

Historically, MITRE has been a key contributor to cybersecurity guidance since the earliest guidance created by the National Security Agency and NIST. MITRE has provided input to or co-authored guidance including NIST's special publications on security and privacy controls (NIST SP 800-53), system security engineering, and cyber resiliency (NIST SP 800-160 Vols. 1 and 2). In addition, MITRE has developed security profiles for applying controls to specific domains, assists organizations in implementing the guidance in their enterprises, and has supported government assessment of vendor products against guidance in programs such as FedRAMP and National Information Assurance Partnership. MITRE also performs technical analysis on implications of cyber technology-related decisions or policies for organizations developing guidance or regulations.

5G Cybersecurity

While 5G seeks to be more secure than prior mobile networks, its virtualization/cloud usage and service-oriented architecture still present a significant attack surface that must be carefully considered. MITRE has studied the cybersecurity aspects of 5G and has developed a threat-based framework for 5G security and resiliency, FiGHT^{TM} (Five-G Hierarchy of Threats). FiGHT covers 5G components, critical assets, threat vectors, and threat actors. It is intended to provide a comprehensive basis for understanding risks from known and emerging threats, in standards or in specific architectures, to be able to identify mitigations and reduce the attack surface. FiGHT, which has just been released publicly, enables the 5G ecosystem to build, configure, and deploy secure and resilient 5G systems for specific use cases and architectures, giving carriers, service providers, and enterprises the tools to quantify risks, share threat intelligence, and plan for cyber investments. MITRE is also engaged in analyzing and improving the cybersecurity of applications built on increasingly capable mobile communications and special-purpose devices, such as Internet of Things (IoT) and smart cities.

Other cyber technical capability areas include:

- **Cyber Assessments:** We tailor and apply a full range of vulnerability, architectural, and adversarial assessment methods to unique sponsor needs and technologies across the system life cycle.
- **Privacy:** We address sponsor privacy concerns systematically by developing privacy programs and strategies, ensuring compliance, and providing training. MITRE has written two books on privacy that are widely used across the federal government.
- **Mobile:** We develop technologies and approaches to securely integrate mobile devices and apps into enterprise and mission environments, based on threat assessments and adversary emulation.
- **Cyber Physical Security and Internet of Things:** We develop approaches to allow safe and secure use at scale of cyber-physical and Internet of Things systems that operate with varying degrees of autonomy and have physical consequences.
- **Cross-Domain Solutions:** We help sponsors securely access and transfer data across security domains through effective combinations of technology, architecture, and policy.
- **Identity and Access Management:** We develop scalable, interoperable COTS-based approaches to securely manage identities and perform authentication and access control throughout an enterprise.
- **Trust and Assurance:** We advance the state of the art through R&D in software assurance, embedded systems analysis, cryptographic protocols, and trusted computing.
- **Cyber Workforce:** We create and implement a range of innovative approaches to developing the cyber workforce, including an Intern Experience Program, Cyber New Professionals (for early career employees), neurodiversity, mid-career development, and others.
- **Cyber Threat Intelligence and Sharing:** We provide actionable knowledge of and insight into adversaries and their malicious behaviors in order to inform traditional and non-traditional cybersecurity defensive and offensive missions by providing better visibility, reducing harm, and enabling better security decision making via an iterative, repeatable process.

- **Cyber Data Analytics and Malware:** We apply state-of-the-art data analytics to cybersecurity problems, including threat detection and in-depth analysis.
- **Cyber Effects and Reverse Engineering:** We enable offensive cyber operations with software and hardware techniques and solutions. Our evaluations, rapid prototypes, and tools provide essential capabilities designed for real-world missions.
- **Cyber for Critical Infrastructure Protection:** We provide a range of cybersecurity capabilities for the detection, protection, and defense of critical infrastructure operational and information technologies.

MITRE has performed 650+ cyber assessments across 26+ agencies within the Federal Civilian Executive Branch, Department of Defense, and Intelligence Community, and has experience assessing systems that span on-premises, remote, cloud-based, and hybrid architectures; mobile and IoT; and specialty medical devices.

In addition to conducting cyber assessments across the federal government, MITRE has performed significant work with leading cybersecurity guidance and policy organizations including NIST, CISA, and the Office of the National Cybersecurity Director (ONCD) in the Executive Office of the President. This includes working with CISA on software supply chain planning guidance and assisting ONCD with 2024 cybersecurity budget guidance. We are also serving as a trusted adviser to the Office of Management and Budget's (OMB's) Chief Information Security Officer, providing input on recent policies, including zero trust and software supply chain risk management. Congress asked MITRE for input into the Federal Information Security Modernization Act (FISMA), and last year MITRE testified on changes needed to the Federal Information Technology Acquisition Reform Act scorecard, offering cybersecurity recommendations aligned with the administration's direction in its Cybersecurity Executive Order and Zero Trust Architecture guidance. Our recommendations helped inform the cybersecurity metrics OMB has recently issued on performance.gov and for FISMA reporting, which will be the foundation for future scorecard grades.

Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

The American Psychological Association Services, Inc. (APA)

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

AMERICAN
PSYCHOLOGICAL
ASSOCIATION
SERVICES, INC.

March 3, 2023

Tomas Vagoun
NCO/NITRD
2415 Eisenhower Avenue
Alexandria, Virginia
22314

RE: RFI Response: Federal Cybersecurity R&D Strategic Plan

Dear Mr. Vagoun,

The American Psychological Association Services, Inc. (APA) appreciates the opportunity to comment on the National Science Foundation (NSF) National Science and Technology Council and the Networking and Information Technology R&D (NITRD) request for information. This request represents a step in the right direction towards ensuring that stakeholders across a diverse array of disciplines are represented in future efforts to achieve cybersecurity research and development goals.

APA Services, Inc. is the companion organization of the American Psychological Association, which is the nation's largest scientific and professional nonprofit organization representing the discipline and profession of psychology, as well as over 146,000 members and affiliates who are clinicians, researchers, educators, consultants, and students in psychological science.

For decades, psychologist researchers have played a vital role in the understanding of policy implementation and broader organizational safety. As with other areas of science, psychologists bring a unique perspective to analyzing and recommending implementation cybersecurity strategies. This perspective provides meaningful assistance to those seeking to understand and push for the adoption of new policies. Psychological science has also played an important role in developing and deploying training programs that are essential to cybersecurity policy adoption and adherence.

We offer the following suggestions and resources to aid those looking to finalize a rule associated with this RFI; in doing so, we ask that the final rule keep in mind the value of psychological and organizational science.

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)?*

APA has an increasing focus on the psychological factors impacting the future of the workplace, including the role of psychology in ensuring the security, reliability, resilience, trustworthiness, and privacy present in workplaces.[1] New psychological science is being released on critical aspects of the future of work at a speed we have never previously witnessed. Further, while much of the recent popular societal dialogue surrounding Future of Work has focused on office workers (e.g., Zoom fatigue and remote work struggles), many psychologists have a maintained complementary broad focus that encompasses the entire workforce, often with special attention to DEI, at-risk populations, and the psychological importance of "decent work" and the way educational pathways fit the workplace. Through our network of experts and focus on the ever-growing scholarship in this area, we stand ready and willing to assist the NITRD in their efforts to create and distribute effective new policies.

2. *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?*

We were pleased to see psychology and psychological science represented in the 2019 Federal Cybersecurity Research and Development Strategy. Organizers of that strategy accurately note the role of psychology as a human factor to consider when developing and rolling out new policies. Psychological science has much to offer those seeking to understand and optimize their strategies for the roll out of new policies.

Successful implementation starts with a focus on a healthy workplace. There is a deep and rich literature of psychological science on enhancing and maintaining mental and emotional wellbeing in the workplace.[2] APA rolled out a call to action to employers across the nation to make employee psychological wellness a priority and recommends five strategies for success, including:

- Train your managers to promote health and well-being
- Increase employees' options for where, when, and how they work
- Reexamine health insurance policies with a focus on employee mental health
- Listen to what your employees need and use their feedback to evolve
- Take a critical look at equity, diversity, and inclusion policies

Additional information relating to fostering and growing a healthy workplace can be found in APA's 2022 Work and Well-being Survey.

Psychology also plays an important role in enhancing the effectiveness of cybersecurity strategies from a technical standpoint. Understanding the risk/reward structures motivating

[1] (2023). Apaservices.org. https://www.apaservices.org/advocacy/future-of-work

[2] See, e.g., the following APA books and journal special issues: The Psychologically Healthy Workplace, Total Worker Health, Interventions in Occupational Health Psychology, Preventing Interpersonal Stressors at Work, and Leadership and Health/Well-Being.

individual behavior, identifying patterns in the behavior of criminals, and deploying effective public awareness campaigns are just a few ways psychological science can be deployed in this fight.[3] Additional focus and integration on this scholarship is essential to effective cyber policies, especially at the federal level. We strongly encourage the NITRD to integrate this focus into future federal cybersecurity research and development strategies.

3. *What objectives not included in the 2019 Strategic Plan should be strategic priorities for federally funded R&D in cybersecurity?*

More focus must be placed on the role of psychology and the study of human behavior when updating the Federal Cybersecurity Research and Development Strategic Plan. The effectiveness of funding in the area of research and development relating to cybersecurity is increased when considering the role that human behavior plays.[4] Strategies and implementation policies ultimately fall short without adequate and effective adoption. An objective aimed at consulting with, and incorporating the recommendations of psychologists should be added to those projects funded through this program.

APA again thanks you for the opportunity to comment on this policy. If APA can be of any further assistance, please contact Corbin Evans, Senior Director of Congressional and Federal Relations, at [redacted]

[redacted]

Katherine B. McGuire, MS
Chief Advocacy Officer
American Psychological Association Services, Inc. x

[3] Wiederhold, B. K. (2014). The Role of Psychology in Enhancing Cybersecurity. Cyberpsychology, Behavior, and Social Networking, 17(3), 131–132. https://doi.org/10.1089/cyber.2014.1502; MIT. (2013) Cyber security and human psychology. http://cybersecurity.mit.edu/2013/11/cyber-security-and-human-psychology; Kirwan, G. & Power, A. (2012). The Psychology of Cyber Crime: Concepts and Principles. IGI Global. https://doi.org/10.4018/978-1-61350-350-8; Mumford, G. (2009, September 1). Preventing cyber-attacks. Monitor on Psychology, 40(8). https://www.apa.org/monitor/2009/09/cyber-attacks; (2023) ; Apa.org. https://www.apa.org/science/about/psa/2017/06/senses-privacy.pdf.

[4] American Psychological Association. (2017, June 1). Psychologist Jeff Hancock presents his cybersecurity research on Capitol Hill. Psychological Science Agenda. https://www.apa.org/science/about/psa/2017/06/cybersecurity-research; American Psychological Association. (2011, May 1). House hearing on cybersecurity references importance of social sciences. Science Policy Insider News. https://www.apa.org/about/gr/science/spin/2011/05/cybersecurity.

Federal Register Notice 88 FR 7999, Federal Register : Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

The App Association (ACT)

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

ACT The App Association

March 3, 2023

National Science Foundation
Networking and Information Technology Research and Development
National Coordination Office
2415 Eisenhower Ave
Alexandria, Virginia 22314

RE: ***Comments of ACT | The App Association Regarding the Networking and Information Technology Research and Development National Coordination Office's 2023 Updates to the Federal Cybersecurity Research and Development Strategic Plan***

ACT | The App Association, hereby, submits comments in response to the Networking and Information Technology Research and Development National Coordination Office's (NITRD NCO) request for input on its 2023 update to the federal cybersecurity research and development strategic plan to guide and coordinate federally funded research in cybersecurity education, workforce development, and the development of consensus-based standards and best practices in cybersecurity. The App Association appreciates the opportunity to share our thoughts to aid in the formulation of a national strategy that addresses cyber training, education, digital awareness, and the cyber workforce.[1]

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology.[2] Enhancing an app ecosystem worth more than $1.7 trillion and responsible for 5.9 million American jobs, our members' innovations will continue to grow and power the rise of the internet of things (IoT).[3] The app economy creates employment opportunities for people in all parts of the country with a variety of skill sets.

Our dynamic, internet-enabled world carries a growing threat of cyber-attacks and American workers and students must be prepared to engage in the digital economy in a safe and secure way. All sectors of the U.S. economy increasingly depend on a workforce equipped with computer science skills; therefore, the growing scarcity of workers with a computer science background is placing America's global leadership in peril and undermining our country's

[1] National Science Foundation, *Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan*, available at https://www.federalregister.gov/documents/2023/02/07/2023-02578/request-for-information-on-the-2023-federal-cybersecurity-research-and-development-strategic-plan

[2] *See* http://actonline.org/about.

[3] ACT | The App Association, *State of the U.S. App Economy: 2020 (Seventh Edition),* available at https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf

national security. Per a study by the Center for Strategic and International Studies, the United States needs between 10,000 and 30,000 cybersecurity specialists to effectively address cybersecurity issues; however, there are only about 1,000 security specialists in the United States with the set of skills necessary to operate effectively in cyberspace. The App Association strongly urges the U.S. government to take steps to provide our current and future workforce with the necessary skillset to succeed in the jobs that will drive our economic development and protect our national security.

The App Association urges for the updated federal cybersecurity research and development strategic plan to align with the following:

- ***Supporting U.S. Leadership in Artificial Intelligence:*** Artificial intelligence (AI) is an evolving constellation of technologies that enable computers to simulate elements of human thinking, such as learning and reasoning. An encompassing term, AI entails a range of approaches and technologies, such as machine learning (ML), where algorithms use data, learn from it, and apply their newly-learned lessons to make informed decisions, and deep learning, where an algorithm based on the way neurons and synapses in the brain change as they are exposed to new inputs allows for independent or assisted decision-making. Already, AI-driven algorithmic decision tools and predictive analytics have substantial direct and indirect effects in consumer and enterprise context and show no signs of slowing in the future.

  Across use cases and sectors, AI has incredible potential to improve consumers' lives through faster and better-informed decision-making, enabled by cutting-edge distributed cloud computing. Even now, consumers are encountering AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition, all forms of what we consider "narrow" AI. These narrow applications of AI already provide great societal benefit. As AI systems, powered by streams of data and advanced algorithms, continue to improve services and generate new business models, the fundamental transformation of economies across the globe will only accelerate.

  Nonetheless, AI also has the potential to raise a variety of unique considerations for policymakers. ACT | The App Association encourages approaches to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers, consistent with consensus policy principles we have developed based on the consensus of our small business innovator community (appended to this comment letter).

- ***Advance Privacy Enhancing Technologies:*** The App Association encourages for the prioritization of privacy enhancing technologies (PETs), in alignment with the efforts of the Office of Science and Technology Policy (OSTP). PETS are an important tool for unlocking the full potential of the data economy and can help ensure that innovation in emerging technologies runs concurrently with a respect for basic human rights, promotes equity in data processing activities, and increases trust in the digital economy writ large. Consumers who rely on our members' products and services expect that our members will keep their valuable data safe and secure. The small business developer community the App Association represents practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and as such, ensuring that the company's business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity. For this reason, we support the Administration's goal of ensuring the United States leads the world in responsible data practices and technologies, including PETs, which are critical to our economic prosperity and national security, and to maintaining the core values behind America's scientific leadership, including openness, transparency, honesty, equity, fair competition, objectivity, and democratic values.

- ***Supporting Strong Encryption:*** The app economy depends on technical data protection methods and strong encryption techniques to keep users safe from harms like identity theft. However, some, including within the U.S. government, insist that "backdoors" be built into encryption for the purposes of government access. These policies would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a security and privacy standpoint, the viability of app developers' products depends on the trust of end users. In alignment with leading policy and research from the National Institute of Standards and Technology, the App Association encourages the updated federal cybersecurity research and development strategic plan to prioritize advancing and supporting the use of advanced encryption techniques.

- ***Investing in (and Investigating) Quantum Computing:*** While advances in quantum computing offer the opportunity for incredible advances across a range of use cases, and should be prioritized and supported in the updated federal cybersecurity research and development strategic plan. At the same time, quantum computing presents the possibility of compromising encryption techniques widely relied upon across enterprise and consumer contexts.

- ***Developing the Cybersecurity Workforce:*** Generally, the App Association's community notes misalignment in and between the public and private sectors regarding workforce categories, specialty areas, work roles, and skill sets. And in the cybersecurity context, the workforce must contend with constantly evolving threats. We support U.S. government efforts to provide building blocks for the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams in the National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity,[4] and urge NITRD NCO to support and align itself with this key initiative.

  Currently, cybersecurity professionals have access to a wide variety of valuable education programs to keep them up to date on the latest cybersecurity trends and certifications. Unfortunately, these programs are often prohibitively expensive, creating a barrier for small businesses and their employees. The App Association believes market effects should define the success of certification programs, and strongly discourages the development of a cybersecurity workforce that endorses particular third-party certification programs. Cybersecurity professionals, particularly those in small businesses, should have the flexibility to utilize certifications to build their expertise in any, and all, areas of data security, and updates to the strategy should support this concept.

  Beyond the growing need for cybersecurity professionals, we urge the strategy reflect that while universities are increasingly offering degrees in computer science and related fields, it is not currently known how well-ingrained cybersecurity is into such computer science curriculum. While we believe the U.S. government should support the university-level development of a U.S. cybersecurity workforce curriculum across classes (as opposed to standalone classes), cybersecurity education programs within public and private sectors will vary in type and effectiveness. There is currently no standard, scalable training, education, or awareness program for the cybersecurity discipline; this has resulted in industry groups offering their own solutions to this challenge. While more needs to be done, we applaud and appreciate the U.S. government's prioritization of cybersecurity education through grants and public-private partnerships.

We have witnessed firsthand that cybersecurity professionals must be well-versed in a wide range of technologies and potential risk vectors, including industry-specific skills such as supervisory control and data acquisition (SCADA) in the energy industry, or blockchain in the financial industry. We urge the U.S. government to help employers invest in the education and training of their current cybersecurity workforce and to utilize innovative programs, such as apprenticeships, to build the future workforce.

As IoT, cloud-based services, and cognitive computing play an increasingly vital role in our world, the demand for skilled cybersecurity professionals will steadily rise. While artificial intelligence and cognitive computing will greatly assist cybersecurity professionals in predicting and responding to cyber-based attacks, these technologies have their own vulnerabilities that will need to be addressed by security and data professionals.

The App Association appreciates the opportunity to weigh in on the 2023 federal cybersecurity research and development strategic plan on cyber training, education, workforce development, and best practices. We commit to working with all stakeholders to achieve a competitive and robust cybersecurity workforce in the United States.

Sincerely,

[redacted]

Brian Scarpelli
Global Senior Policy Counsel

Leanna Wade
Regulatory Policy Associate

ACT | The App Association
1401 K St NW (Suite 501)
Washington, District of Columbia 20005