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

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]