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

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.