Federal Register Notice: 89 FR 78915, Federal Register :: Networking and Information Technology Research and Development Request for Information on Cyber-Physical Systems Resilience Research, September 26, 2024.

Request for Information on the National Cyber-Physical Systems Resilience Plan

Bethany Johns

Jacob Dowd

Monowar Hasan

Assefaw Gebremedhin

Protecting Digital Agriculture from Cyber Breaches

RFI Response: ***Networking and Information Technology Research and Development Request for Information on a National Plan for Cyber-Physical Systems Resilience***

Bethany Johns
Assistant Director, Federal Relations, Washington State University
[redacted]

Jacob Dowd
Director, Federal Relations, Washington State University
Email: [redacted]

Monowar Hasan
Assistant Professor, School of EECS, Washington State University
Email: [redacted]

Assefaw Gebremedhin
Associate Professor, School of EECS, Washington State University
Email: [redacted]

RFI Response Focus: The U.S. agriculture sector is being infused with various cyber components. However, the cyber-physical resilience of these digital assets from threats ranging from extreme weather, power grid outages, to cyberattacks is still an afterthought. There is a need for a critical analysis of the cybersecurity posture of precision agriculture applications and improving the preparation and protection of this sector against cyberattacks. Protecting the U.S. agriculture sector is critical and requires a concerted, cross-domain research, thoughtful synthesis of ideas and methods, and investment in workforce development.

1. Introduction

Increased reliance on digital technologies and networked distributed systems across various industrial sectors has made critical infrastructure cybersecurity one of the top priorities for national security. The U.S. food and agriculture sector continues to be identified as one of the 16 critical national infrastructures in the U.S., accounting for roughly one-fifth of the nation's economic activity [1], [2]. As this sector adopts advanced and innovative digital technologies -- such as connected sensors, embedded computers, smart tractors, drones and Artificial Intelligence (AI) - productivity has increased, nutritional value has improved, disease resistance, and resilience to climate change. While these technologies have enabled unprecedented gains in innovation and productivity, they expose modern agriculture to various cyber vulnerabilities impacting precision agriculture operations. Due to the high value of agricultural sectors to adversaries, limited or no cybersecurity defense, and lack of domain-specific security understanding of those systems, digital agricultural systems are increasingly becoming targets for cyber breaches. The food and agricultural sectors have faced a rising number of cyberattacks, with over 30 major incidents have been reported [6], Recent examples of major cyber incidents in the U.S. agricultural sector include ransomware attacks on JBS facilities [3], Russian hackers targeting an Iowa grain co-op [4], and a Minnesota grain handler [5]. leading to significant financial losses. Attacks originating from other critical sectors, such as the utility grid and industrial control systems, could also threaten the food supply chain due to close interdependence, as indicated by the U.S. Department of Energy [7]. Any cyberattack targeting agriculture and closely related critical infrastructure could jeopardize the nation's agricultural production, exports, food security, and ultimately, national security.

A critical limitation in our progress on security for cyber-physical systems is the lack of knowledge and training of professionals in the domains these systems are being deployed. For example, there is a growing need for individuals with knowledge in the agriculture, food, and life sciences domains to help build resilient cyber systems that can withstand threats to these domains. There is much within the food and agriculture knowledge domain that requires specialized threat intelligence to mitigate threats and ensure a resilient system. Cross-domain knowledge will become increasingly vital as cyber-physical systems intelligently interact with other systems across information and physical interfaces.

2. Research Needs

The following systematic research is needed for a thorough understanding on how resilience by design or resilience by intervention can prepare for recovery and adaptation in different threat scenarios.

Risk Assessment and Cyber Forensics Tool. Development of new software tools and cyber risk models for optimal cybersecurity investment, enabling ag asset owners to assess risks and implement cost-effective mitigations continuously. Resilience strategies will include redundant systems for critical operations, automated recovery protocols, and fallback mechanisms to maintain safety, such as livestock health, even during system compromises. A comprehensive set of "what-if" contingency scenarios need to be developed with optimal precomputed remedial actions to address potential operational impacts, safety concerns, and economic losses.

AI and Machine Learning-based Anomaly Detection and Mitigation. Incorporating AI and machine learning, deep learning, and reinforcement learning for automated detection and real-time mitigation of cyber anomalies. Federated learning will enable collaboration among distributed agents for system-wide intelligence while preserving privacy. How can such models continuously learn and adapt to evolving threats and optimize detection strategies based on domain-specific data? How do we integrate those models into Security Information and Event Management (SIEM) platforms for real-time cybersecurity solutions?

Zero-Trust Platform. To support attack prevention, mitigation, and cyber resilience, how do zero-trust principles (i.e., "never trust, always verify") and moving target defense algorithms adapt system parameters to reduce attack surface and prevent attacks dynamically? The food and ag sectors have a combination of Information Technology (IT) and Operation Technology (OT) systems, and the forensic analysis in OT presents additional challenges as they often do not capture system state (via system logs or network logs) coupled with legacy hardware and embedded software still being utilized in these systems. We need to develop cyber forensics tools for food and agriculture OT systems, focusing on recording state information and conducting deep log analysis. One challenge is identifying threat intelligence (attack types, sources, compromised subsystems, or credentials) so that a zero-trust model can be effective.

Blockchain-based Data Sharing Platform. Can distributed ledger technology support product traceability and secure data sharing, with robust algorithms ensuring data security and privacy? Malicious alterations to sensitive farm data can cause financial losses and harm to crops or

livestock. The challenge is to study whether traditional privacy techniques are sufficient for the evolving agricultural ecosystem.

Systems Integration. Further research is needed on integrating developed cybersecurity technology testbeds into real-world cyber secure and resilient system testbeds for the food and ag sector, namely, the animal agriculture testbed, food crops testbed, agricultural machinery testbed, and inter-dependent agriculture-water-energy testbed. Synergistic partnerships with various ag stakeholders and industry, government, national labs, and academic institutions are needed to build and release real-world datasets and use-case scenarios. The developed testbeds can then use the datasets and attack vectors to demonstrate their feasibility and efficacy concerning cybersecurity.

Agriculture Cybersecurity and Climate Change. Cybersecurity in agriculture directly impacts how effectively the sector can mitigate and adapt to the effects of climate change. Modern agricultural practices depend on data-driven technologies such as satellite-based weather forecasting, precision irrigation, and climate modeling. These technologies enable farmers to make informed decisions about crop management, water usage, and soil health, which are crucial for reducing agriculture's carbon footprint and conserving water in the face of climate variability. If cybersecurity vulnerabilities in these systems go unchecked, they could be exploited to disrupt data flows or corrupt decision-making models. For example, an attack that manipulates climate or weather data could lead to incorrect decisions about irrigation scheduling, pesticide application, or crop planting, ultimately undermining efforts to adapt to changing environmental conditions. Another challenge is isolating unintentional faults from cyberattacks so farmers/ag-tech vendors can proactively make informed decisions. Hence, there is a need for a new data-driven model and leverage advancement of AI technologies to understand the impact of climate change on agriculture decision-making. Therefore, protecting agricultural systems from cyber threats is integral to ensuring that the sector can continue to play a vital role in addressing climate change through sustainable and efficient practices.

3. Cross-Domain Exploration

Agriculture does not exist in isolation. It is deeply intertwined with other critical infrastructure sectors, such as the power grid, water management, and transportation systems. As a result, cybersecurity vulnerabilities in other domains can have cascading effects on agriculture, jeopardizing food security and economic stability. For instance, a cyberattack on the power grid or energy delivery system can directly impact agriculture by disrupting power to irrigation systems, sensors, and storage facilities. This can lead to crop loss, water waste, and reduced resiliency in agricultural operations, especially during extreme weather events. A failure in the power grid could

also affect the cold chain logistics critical for preserving food post-harvest, leading to significant food spoilage and supply chain disruptions. For instance, if hackers were to compromise the data networks used in energy distribution, they could manipulate electricity prices or availability in ways that severely impact the cost and reliability of energy needed for farming equipment, heating systems for livestock, or greenhouses.

Similarly, cybersecurity vulnerabilities in transportation systems could delay the delivery of essential supplies such as seeds, fertilizers, and machinery or prevent crops from reaching markets on time, affecting food availability and prices. **We stress that cybersecurity research in agriculture must consider how interrelated sectors like the power grid, water infrastructure, and logistics are interconnected.** This cross-domain research is essential for developing comprehensive security strategies that ensure agriculture can remain resilient despite cascading disruptions from other sectors.

4. Workforce Development and Interdisciplinary Research Environment

There is a critical need for a well-trained and diverse cybersecurity workforce in the US, across all sectors. Federal initiatives to cultivate the US cyber workforce, such as the Workforce Framework for Cybersecurity, National Centers of Academic Excellence in Cybersecurity, and the 8140 series of Department of Defense (DoD) Directives, have yielded much dividend. A recent addition to these initiatives is the establishment of the Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ (VICEROY). The mission of VICEROY is to "Establish academic cyber institutes at institutions of higher learning, to develop foundational expertise in critical cyber and spectrum operational skills for future military and civilian leaders of the Armed Forces and the DoD, including such leaders of the reserve components." Towards this goal, VICEROY funds undergraduate cybersecurity education at designated Virtual Institutes.

One such institute is the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) [8]. Established in 2021 in the first cycle of VICEROY, CySER is a consortium of four institutions in the Northwest led by Washington State University (WSU) with partner institutions Montana State University (MSU), University of Idaho (UI), and Central Washington University (CWU). CySER's focus is training a Reserve Officer Training Corps (ROTC) and national defense-oriented civilian workforce, combining cybersecurity technical competency with professional competencies of leadership, communication, teamwork, and lifelong learning. The CySER program has thus far had remarkable achievements, including catalyzing the launching of a new Bachelor of Science in Cybersecurity degree program at WSU and increasing collaboration in research and education across multiple institutions [9].

Federal investment in programs like VICEROY is needed in sectors outside of defense as well, including in agriculture. Institutions such as WSU, where a successful VICEROY program has existed and is well established, serve as valuable models for scaling up and branching out cybersecurity workforce training into other domains.

A matter closely tied to the education and training of cybersecurity workforce is the **establishment of reliable cyber ranges** that students and other trainees can easily access. Cyber ranges are interactive and simulated platforms that replicate networks, systems, tools, and applications. They provide a safe and legal environment for acquiring hands-on cyber skills, and they have a crucial role to play in cybersecurity education and training. They may consist of actual hardware and software or a combination of physical and virtual components. Types of cyber ranges commonly used include *simulation ranges*, *overlay ranges*, *emulation ranges*, and *hybrid ranges*. The type that would be most desirable for contexts in academic institutions such as WSU is a hybrid range, which would integrate features and capabilities from simulations, overlay ranges, and emulation, creating a hybrid environment that suits specific requirements.

5. Beyond Agriculture

Considering the diverse agriculture domain (plants, crops, livestock, seafood) and external climatic variabilities (weather, water), understanding cybersecurity issues and building techniques using digital twins to bolster security posture requires concerted, multiyear efforts.

Although the majority of this RFI response document focused on agricultural cybersecurity, accompanying research is needed to investigate how this agricultural domain knowledge can be transferred to understanding and protecting other critical sectors, such as power grids, transportation systems, biomanufacturing, public health, food supply chain, and wildfire management, using the digital twin technologies.

References

[1] "GIAC Cyber Security Discussion Paper." Accessed: Jun. 06, 2024. [Online]. Available: https://www.ams.usda.gov/about-ams/giac-may-2024-meeting/cybersecurity

[2] "Food and Agriculture Sector-Specific Plan - 2015." Accessed: Jun. 06, 2024. [Online]. Available: https://policycommons.net/artifacts/12474227/food-and-agriculture-sector-specific-plan/13370861/
[3] "JBS S.A. ransomware attack," Wikipedia. Accessed: Jun. 15, 2024. [Online]. Available: https://en.wikipedia.org/wiki/JBS_S.A._ransomware_attack
[4] "BlackMatter Hits Grain Cooperative With Ransomware Attack." Accessed: Jun. 15, 2024. [Online]. Available: https://www.itprotoday.com/attacks-breaches/blackmatter-hits-grain-cooperative-with-ransomware-attack
[5] "Minnesota grain handler targeted in ransomware attack." Accessed: Jun. 15, 2024. [Online]. Available: https://www.reuters.com/technology/minnesota-grain-handler-targeted-ransomware-attack-2021-09-23/
[6] A. Kulkarni, Y. Wang, M. Gopinath, D. Sobien, A. Rahman, and F. A. Batarseh, "A Review of Cybersecurity Incidents in the Food and Agriculture Sector," Mar. 12, 2024, *arXiv*: arXiv:2403.08036. Accessed: Jun. 06, 2024. [Online]. Available: http://arxiv.org/abs/2403.08036
[7] US Department of Energy, "Cybersecurity considerations for distributed energy resources on the US electric grid." [Online]. Available: https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf
[8] "VICEROY Northwest Institute for Cybersecurity Education and Research (CySER)." Accessed: Jun. 05, 2024. [Online]. Available: https://cyser.wsu.edu/
[9] "MCPA - Crabb - Cyber Education and Research — public.milcyber.org." [Online]. Available: https://public.milcyber.org/activities/magazine/articles/2024/crabb-cyber-education-and-research