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®.

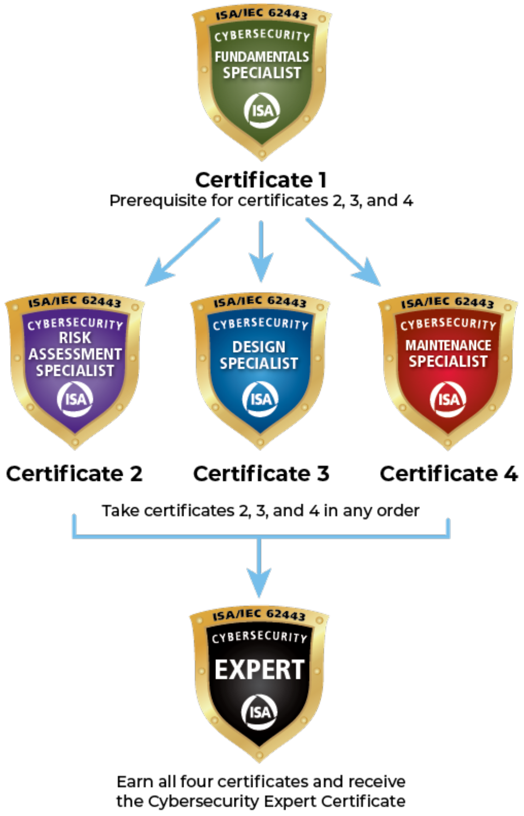
Owner/operators are developing a consensus operating site assessment specification under the ISASecure® program to secure and measure security of the automation systems at operating sites (similar to NERC-CIP in the regulated electric sector).

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]