Position Paper for Executive Order #14028

Shoshana L. Wodzisz, CSSLP
Rockwell Automation
slwodzisz@ra.rockwell.com
+1 330-730-5670
May 26, 2021

This position paper is in response to the following item requested by NIST:

2. *Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government.* This list of standards shall include criteria and required information for attestation of conformity by developers and suppliers. See EO Section 4(e)(i, ii, ix, and x).

Rockwell Automation is pleased to see President Biden issue EO 14028 which will improve cybersecurity capabilities of the US Government including better sharing of incident and vulnerability data. It is our hope that this executive order will be used as a model for industry to follow to protect the critical infrastructure of the nation.

Rockwell Automation recommends and endorses the IEC 62443 global cybersecurity industrial control system standard. We recommend the federal government rely on this standard for software and components used in OT environments. Following the requirements and best practices in this standard can protect control systems that are used to operate facilities such as government buildings and plants.

The IEC 62443-4-1 portion of the standard defines the practices and requirements for a Security Development Lifecycle (SDL) for components used in OT systems. The requirements span the full product lifecycle from initial concept development to end of life disposal. Included in the standard are the requirements that a component supplier perform due diligence on their supply chain. Certifications are for specific maturity levels, and can apply to a specific site, product team, or the entire company:

- Maturity Level 1: No SDL is documented.
- Maturity Level 2: Processes for using the SDL are documented but are not necessarily repeatable across the company or across product teams.
- Maturity Level 3: Processes for using the SDL are documented, repeatable, and consistently followed across the company or across product teams.
- Maturity Level 4: Processes for using the SDL are documented, repeatable, consistently followed, measured, and steadily improved.

In addition, the IEC 62443 4-1 standard imposes requirements on the software supply chain. Therefore, major control system vendors have already been working on influencing the software supply chain, through contractual requirements, risk assessments, auditing processes, and educational processes for raising the security posture of their vendors.

The IEC 62443 standard has increasingly gained acceptance and adoption as the only global standard specific to cybersecurity for industrial control systems and associated software. All major control system vendors have obtained certifications to this standard from independent certifying bodies.

In addition to the use of this standard, we want the federal government to not just encourage but actively incentivize the private sector – especially critical infrastructure – to adopt the IEC 62443 standard. The IEC 62443 standard complements the NIST Cybersecurity Framework (CSF) and the ISO 27001 standards that are commonly used to protect business systems. It represents many years of work and refinement over the years as it was implemented by major vendors. It is a proven success, and there is no reason to replace it. On the contrary, it should be used as a model for development of a comprehensive software supply chain standard / certification for software outside of the industrial control systems domain.

Rockwell Automation is a founding member of the ISA Global Cybersecurity Alliance (ISAGCA). The ISAGCA is supporting and promoting the use of the IEC 62443 standard globally. As part of that organization, Rockwell Automation is involved in work with US State, US Government, and governments across the globe to promote the adoption and use of this standard.