May 26, 2021

VIA ELECTRONIC SUBMISSION AT: swsupplychain-eo@nist.gov

National Institute of Standards and Technology - NIST
100 Bureau Dr., Stop 1070
Gaithersburg, MD 20899-1070

RE: ABB position statement for NIST workshop on software supply chain security executive order

To whom it may concern:

ABB Inc., on behalf of ABB, Ltd. ("ABB") submits this position paper in response to the National Institute of Science and Technology's (NIST) request for papers in advance of its June 2nd workshop on Software Supply Chain Security.

ABB, a New York Stock Exchange listed corporation headquartered in Zurich, Switzerland, is one of the United States' and world's largest providers of electrical and industrial technology and control systems. Our products and solutions are used across the energy, utility, and critical infrastructure sectors. We produce many of those products in the U.S. at our 50 domestic manufacturing or assembly sites spread across 30 states. Safety, reliability, and security are central to our product development, manufacturing, and service offerings. This commitment includes ensuring that we reduce and mitigate cybersecurity risks and vulnerabilities throughout or product lifecycle and supply chain.

1. Criteria for designating "critical software." Functional criteria should include, but not be limited to, level of privilege or access required to function, integration, dependencies, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised.

ABB supplies hardware and software to many of the critical infrastructure sectors defined by CISA and takes a "defense in depth" approach to cybersecurity and mitigation. Software which is designated as "critical" must designed to meet cybersecurity best practices. There are a number of well accepted industry standards that set criteria for cybersecurity mitigation. IEC 62443 4-2 provides a comprehensive listing of functional security requirements which informs ABB software development of the expected capabilities. In the Electric Sector NERC-CIP established differentiating criteria such as operating voltage level or impact to the overall bulk electric system. A challenge to any regulation specifically targeting is "critical software" is defining what exactly qualifies as such software. There needs to be bright lines established as to what rises to the level of critical software and how it is isolated from non-critical software systems. Often times this line is specific to each critical sector, making a broad definition challenging. Further, many software and control system solutions serve non-critical sectors as well, further blurring the lines and expanding the impact of any regulation designed just for critical systems.

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.

ABB has organized our product development around the international standard IEC 62443 4-1 Secure Product Development Lifecycle. Compliance is assessed to 8 different Practices covering: Security Management, Security Requirements, Secure Design, Implementation, Validation Testing, Vulnerability Handling, Updates and Operational Guidelines. This standard is well suited to the operational technologies which are prevalent in critical infrastructure and ABB has been contributing its development along with other community stakeholders for over a decade. Guidelines outlining security measures that shall be applied to the federal government's use of critical software, including but not limited to, least privilege, network segmentation, and proper configuration.

ABB maintains detailed security configuration guidelines to help integrators and end users to ensure systems and components are configured with important security controls. Topics such as role-based access control, operating system hardening and firewall configuration as well as security policies must be available and implemented for any software used in critical applications. Additionally, ABB provides a reference architecture which advises integrators on proper network segmentation to help provide defense in depth.

3. Initial minimum requirements for testing software source code including defining types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing), their recommended uses, best practices, and setting realistic expectations for security benefits.

The product testing program at ABB is required for all software and hardware product and include fuzzing, flood, protocol manipulation and vulnerability scanning. During development security assessments, code analysis and threat models are evaluated. ABB is moving to get the testing program accredited to conform to IEC 62443 testing requirements.

4. Guidelines for software integrity chains and provenance.

ABB recommends that vendors establish a Public Key Infrastructure to distribute digital certificates to development locations where code is externally signed to ensure its integrity as wells as its authenticity. This a current best practice and recognized as state of the art. For software components not compatible with the use of digital certificates, a hash should be generated and published by the vendor so that end users can validate the component. This should be additionally enhanced via a Software Bill of Material so that authenticity can be determined for installed components at any time during operation.

Thank you for the opportunity to submit comments; we would be glad to discuss these questions further.

Regards,

Jim Lemanowicz
Global Cyber Security Product Manager
ABB Inc.