The ISAGCA, International Society of Automation Global Cybersecurity Alliance wish to thank the NIST for the opportunity to file these comments in response to the Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security, related to the May 12, 2021, EO 14028.

The ISAGCA is a collaborative forum hosted by the International Society of Automation (ISA), a 40,000-member global professional automation engineering society. ISAGCA's mission is to advance cybersecurity readiness through awareness, education, standards, and knowledge sharing. Membership is open to any organization concerned about cybersecurity—end users, automation providers, system integrators, consultants, government agencies, and more

**ISAGCA member companies, industry organizations, and their constituents represent over $1.5 Trillion in annual revenues, coming from industries such as Oil & Gas, Pharma, Automotive, Automation suppliers, IT suppliers, and cybersecurity products and services.**

ISAGCA Member companies and thought leaders have a long history of adopting a standards-based approach for securing automation products and operating sites based on the ISA/IEC 62443 series of international cybersecurity standards. **The scope of ISA/IEC 62443 standards applies to critical software in all phases of the automation solution lifecycle.**

Product suppliers have been developing automation products using ISA/IEC 62443 security lifecycle practices in their development processes since 2010. Companies are having their development **processes and products independently audited/certified** to be conformant with ISA/IEC 62443 via accredited certification bodies in the US and around the globe. **Company examples include ABB, Aveva, Azbil, Bayshore Networks, Carrier Corporation, CISCO, Eaton, Emerson Automation Solutions, Emerson Power & Water Solutions, GE Power Conversion, Hima, Hitachi, Honeywell, Johnson Controls, Nexus Controls, Rockwell Automation, Schneider Electric, Siemens, Toshiba, Yokogawa, Valmet, Wartsila, and many others.**

End users (asset owner/operators) are establishing cybersecurity programs at operating sites based upon ISA/IEC 62443, including their critical software.

The internationally recognized ISA/IEC 62443 standards have been adopted in the USA and throughout the globe. This is important since most product suppliers (includes critical software) have global customers. Further, many end-user companies operate internationally. ISA/IEC 62443 provides a common vocabulary for managing cybersecurity capabilities. A globally accepted set of standards reduces barriers to trade where country-specific product certifications are mutually recognized. It also provides end-users the basis for establishing companywide cybersecurity practices useful in all geographies.

ISA and its members have been an ardent supporter of the NIST CSF and contributed to its development of NIST CSF in 2014 and the ISA/IEC 62443 standard. The NIST CSF includes several key standards as informative references as a basis for implementing the NIST CSF requirements. ISA/IEC 62443 are featured prominently

for operational technology and automation. See attached Table A which shows where the ISA/IEC 62443 standards align with the NIST CSF requirements.

ISAGCA members request that NIST, in their Executive Order deliverables, consider the attached input to the Executive Order. Respectfully submitted by Andre Ristaino on behalf of the ISAGCA members. Feel free to reach out to me with any questions or to schedule a briefing on these recommendations.

Contact Info: Andre Ristaino, ISA Managing Director, Global Alliances, Consortia, Conformity Assessment
aristaino@isa.org Phone: 919-323-7660 67 T.W. Alexander Drive RTP, NC 27709

ISAGCA asks that you consider these additions to the Executive Order:

1. Reference these standards when defining "Critical Software": EO Section 4(g).
    a. ISA/IEC 62443-3-3-SR.5.2RE(2)/RE(3); ISA/IEC 62443-4-2-CR.2.10/CR.7.1) to define commands and essential functions including parameters and associated data that must be properly protected either by built-in technical capabilities (ISA/IEC 62443-4-2), integrated system capabilities (ISA/IEC 62443-3-3) and/or procedural/organizational capabilities(ISA/IEC 62443-4-1; ISA/IEC 62443-2-4 and ISA/IEC 62443-2-1).
    b. ISA/IEC 62443-2-4 standard defines best practices for OT Service Providers with a set of security capabilities that an organization needs to have while designing a secure automation solution. That includes the associated, hardware, software, and data.
    c. ISA/IEC 62443-2-4-SP.03.01BR provides Rationale to ISA/IEC 62443-3-2 including capability to translate a business, production and ultimately safety risk into technical and procedural capabilities that a system needs to encompass to become feasible
    d. ISA/IEC 62443-2-4-SP.03.09BR/10BR) including its safeguarding requirements needed to perform the risk translation includes the capacity to identify and manage security vulnerabilities and associated threats for all the associated components of the automation solution and its authorized data storage points, data flows and control actions by design
2. Reference ISA/IEC 62443 4-1 Product Security Development Life-Cycle Requirements as a standard to secure software development lifecycle for Operational Technologies. EO Section 4(e) which describes component or system development lifecycle requirements related to cyber security for those components or systems intended for use in an OT environment and provides guidance on how to meet the requirements described for each element. When a Product Supplier is using an ISA/IEC 62443-4-1 compliant process, enables a Service Provider to follow the ISA/IEC 62443-2-4 compliant practices to integrate, configure, validate, commission, and maintain an intended security posture by design.
3. Reference ISA/IEC 62443 4-2 Technical Security Requirements for Automation Components as a standard to secure software development lifecycle for Operational Technologies components. EO Section 4(e)
4. Reference ISA/IEC 62443 3-3 System Security Requirements and Security Levels as a standard to define security measures that shall be applied to the federal government's use of critical software. E.O. Section 4(I)
5. Reference ISA/IEC 62443 4-1 Product Security Development Life-Cycle Requirements (Section 9) to define the minimum requirements for testing software source code. See EO Sections 4(e)(iv, v) and 4(r).
6. Reference ISA/IEC 62443-4-1-SM-9 Security Requirements for externally provided components requires software development organizations to have a process to identify and manage security risks of all externally provided components used within the product. An SBOM implementation can be utilized as a method satisfy this requirement. The rationale of that requirement provides the guidance for compliance, referring to the Defense in Depth strategy, identifying all components as well as their security context, rigor applied to the component implementation, verification/validation, notifications, etc.

Many independent conformity assessment programs are already in place in the USA and around the globe which provide assurances that suppliers are utilizing the ISA/IEC 62443 requirements in their software design, development, deployment, and maintenance practices.

Table A – Map of ISA 62443 to NIST CSF

| Function Identifier | Function | Category Identifier | Category | IEC 62443 |
|---|---|---|---|---|
| ID | Identify | ID.AM | Asset Management | :2-4 – SP.06.02/SP.01.x |
| | | ID.BE | Business Environment | :2-4 –SP.01.x |
| | | ID.GV | Governance | :2-4 –SP.01.x<br>:2-1 -ORG-02 |
| | | ID.RA | Risk Assessment | :2-4-SP.02.01 |
| | | ID.RM | Risk Management Strategy | :2-1/2-4/3-3/4-1 |
| | | ID.SC | Supply Chain Risk Management | IEC 62443-2-4 |
| PR | Protect | PR.AC | Identity Management and Access Control | :3-3 –SR02.04/ SR.02.07/SR.03.08x<br>:2-4 -SP.08.x |
| | | PR.AT | Awareness and Training | :2-4 –SP.01.x |
| | | PR.DS | Data Security | :2-1 –DATA01-04 /CRYPT-01-03<br>:2-4 – SP.05.09x/ SP.03.10x<br>:3-3 – SR.03.01RE(1) /SR.04.03 |
| | | PR.IP | Information Protection Processes and Procedures | :2-1:ORG-02 /NET-12<br>:2-4: SP.03.08x<br>:3-3- SR 7.6 |
| | | PR.MA | Maintenance | :2-4 (complete)<br>:3-3 -SR.04.02 |
| | | PR.PT | Protective Technology | :2-4-SP.08.x<br>:3-3-SR01.01 – SR.02.07 |
| DE | Detect | DE.AE | Anomalies and Events | :2-4-SP.08.x |
| | | DE.CM | Security Continuous Monitoring | :3-3-SR02.08-SR02.12 /SR03.09/SR.06.01/SR.06.02<br>:2-4- SP.08x |
| | | DE.DP | Detection Processes | :2-4-SP.07.x/SP.06.x |
| RS | Respond | RS.RP | Response Planning | :2-4-SP.02.x/SP.12.x<br>:2-1-ORG-08/10/02 |
| | | RS.CO | Communications | :2-4-SP.02.x/SP.12.x<br>:2-1-ORG-x |
| | | RS.AN | Analysis | :2-4-SP.02.x/SP.12.x<br>:2-1-ORG-x |
| | | RS.MI | Mitigation | :2-4-SP.02.x/SP.12.x<br>:2-1-ORG-x |
| | | RS.IM | Improvements | :2-4-SP.02.x/SP.12.x<br>:2-1-ORG-x |
| RC | Recover | RC.RP | Recovery Planning | :2-4-SP.12.x<br>:2-1-ORG-x |
| | | RC.IM | Improvements | :2-4-SP.12.x<br>:2-1-ORG-x |
| | | RC.CO | Communications | :2-4-SP.12.x<br>:2-1-ORG-x |