GLOBAL CYBERSECURITY ALLIANCE

Automation Cybersecurity Requirements in Public Policy: Key Points

1. US President Biden issued Executive Order 14028 on May 12, 2021 addressing securing automation in critical infrastructure; and the ISA Global Cybersecurity Alliance (ISAGCA) submitted a formal response.
2. ISAGCA member companies, industry organizations, and their constituents represent **over $1.5 trillion in annual revenues**, coming from industries such as critical infrastructure, oil & gas, pharmaceuticals, automotive, automation suppliers, IT suppliers, and providers of cybersecurity products and services. Membership includes 50+ companies and continues to grow every week.
3. 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. ISA/IEC 62443 is the de facto standard.**
4. Post 9/11, ISA members recognized the need to secure automation that controls equipment and operations comprising US critical infrastructure. In 2002, ISA's ANSI-accredited standards department stood-up the ISA99 committee to develop the ISA/IEC 62443 series of standards for automation and control systems and, has since published a **comprehensive family of 15 standards and technical reports purpose-built to address securing automation and control systems.**
5. Over 1,000 engineering professionals and cybersecurity experts contributed to the ISA/IEC 62443 standards, **codifying thousands of years of engineering and cybersecurity subject matter expertise into a coherent series of standards.**
6. A founding principle of the ISA/IEC 62443 standards is the concept of **shared responsibility necessary for securing automation.** The standards define requirements for key stakeholder groups who are responsible for control system cybersecurity. **Stakeholder groups include Asset Owners (end-users), Automation Product Suppliers, Integrators** who build and maintain control system solutions and their components, and **Service Suppliers** who support the operation of control systems.
7. Because IACS are physical-cyber systems, **the impact of a cyberattack could be severe.** The consequences of a cyberattack on an IACS include endangerment of public or employee safety or health, damage to the environment, damage to the equipment under control, and other significant consequences.
8. **ISA/IEC 62443 standards align with the requirements in IEC 61511 for Safety Instrumented Systems (SIS)** and include performing a security risk assessment to identify the security vulnerabilities of the SIS and address the design of the SIS to ensure it provides the necessary resilience against the identified security risks.
9. The **NIST CSF references the ISA/IEC 62443 standards** to provide implementation requirements for conformance to the NIST CSF for automation and control systems.
10. **ISO 27001/2 are complementary to ISA/IEC 62443** and industry groups have published guidance for implementing the two standards as companion specifications for securing the entire spectrum of IT and OT technology in complex organizations.
11. The ISA/IEC 62443 standards and technical reports have been **successfully applied to a wide variety of industry sectors,** including process industries such as chemicals and oil & gas, building automation, electric power generation and distribution, medical devices, and transportation.
12. ISAGCA is working with state and federal legislators, regulators, and other standards bodies to **ensure that the ISA/IEC 62443 standards are included as the reference standards for establishing IACS cybersecurity metrics** in automation that affects our everyday lives.
13. **It is critically important for legislators and regulators to recognize the urgent need for response to this threat.**
14. **A standard definition of the security capabilities for system components is necessary;** it will provide a common language for product suppliers and all other control system stakeholders. **A fully developed ISA/IEC 62443 ecosystem enables facilities/ operations across many different industries to achieve IACS cybersecurity.** ISA/IEC 62443 provides guidance for all stakeholders in the entire automation lifecycle including suppliers, integrators/service providers, asset owners, regulators, and insurers.
15. **The ISA/IEC 62443 standards do not create 'winners and losers';** it is a security standard that is company and product agnostic, like seat belts in all motor vehicles. Everyone wins by having common cybersecurity requirements that protect the critical infrastructure of the nation.