CISA Issues Preliminary Cross-Sector Cybersecurity Goals and Objectives for Critical Infrastructure Control Systems

Sep 28, 2021

Reading Time : **4 min**

By: Scott Daniel Johnson

As we noted here, the National Security Memorandum established “a voluntary initiative intended to drive collaboration between the Federal Government and the critical infrastructure community to improve cybersecurity of control systems.” It also directed DHS to “lead the development of preliminary cross-sector control system cybersecurity performance goals as well as sector-specific performance goals.” The preliminary goals were due September 22, 2021, and final cross-sector and sector-specific goals are due in July 2022. Secretary of Homeland Security Alejandro N. Mayorkas and Secretary of Commerce Gina Raimondo described the goals and objectives as “part of a long overdue, whole-of-government effort to meet the scale and severity of the cybersecurity threats facing our country.” And while they are not mandatory or legally enforceable in their current form, Secretaries Mayorkas and Raimondo also noted that it is “vital that critical infrastructure owners and operators immediately take steps to strengthen their cybersecurity posture toward these high-level goals.”

The preliminary goals span nine categories, and each includes “specific objectives that support the deployment and operation of secure control systems that are further organized into baseline and enhanced objectives.” The “baseline” objectives “represent recommended practices for all control system operators” while the “enhanced” objectives “include practices for critical infrastructure supporting national defense; critical lifeline sectors (i.e. energy, communications, transportation, and water); or where failure of control systems could have impacts to safety.” The nine categories—the order of which CISA notes “is not intended to imply a prioritization or specific progression of operations”—are:

1. Risk Management and Cybersecurity Governance. This includes identifying and documenting cybersecurity risks to control systems using established recommended practices and providing dedicated resources to address cybersecurity risk and resiliency.

2. Architecture and Design. This includes integrating cybersecurity and resilience into system architecture and design in accordance with established recommended practices "for segmentation, zoning, and isolating critical systems" and regularly reviewing and updating them to include lessons learned from operating experience.

3. Configuration and Change Management. This includes documenting and controlling "hardware and software inventory, system settings, configurations, and network traffic flows throughout control system hardware and software lifecycles."

4. Physical Security. This includes limiting physical access to "systems, facilities, equipment, and other infrastructure assets, including new or replacement resources in transit, . . . to authorized users" and securing against "risks associated with the physical environment."

5. System and Data Integrity, Availability and Confidentiality. This includes protecting "the control system and its data against corruption, compromise, or loss."

6. Continuous Monitoring and Vulnerability Management. This includes implementation of "continuous monitoring of control systems cybersecurity threats and vulnerabilities."

7. Training and Awareness. This includes training personnel "to have the fundamental knowledge and skills necessary to recognize control system cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices."

8. Incident Response and Recovery. This includes implementation and testing of "control system response and recovery plans with clearly defined roles and responsibilities."

9. Supply Chain Risk Management. This includes identification of risks "associated with control system hardware, software, and managed services" and establishment of policies and procedures "to prevent the exploitation of systems through effective supply chain risk management."

CISA also provides "Sample Evidence of Implementation" for each set of goals and objectives "to demonstrate what successful implementation . . . might entail for an organization." In other words, “[s]uccessfully implementing all baseline objectives would equate to successful implementation of a goal.” In addition, CISA states that “while all of the goals . . . are foundational activities for effective risk management, they represent high-level cybersecurity best practices.” But “[i]mplementation of the [preliminary] goals and objectives . . . is not an exhaustive guide to all facets of an effective cybersecurity program.” Rather, CISA and NIST developed and refined the preliminary goals “with as much interagency and industry input as practical for the initial timeline using existing coordinating bodies. DHS expects to conduct much more extensive stakeholder engagement as the goals are finalized” by July 2022.

Our sense is that the extent to which incorporating such goals and objectives into a cybersecurity program would be challenging or costly will depend heavily on the characteristics of existing programs (if any) and what specific actions would be relevant and feasible for each affected entity. Indeed, there likely will be much variability from entity to entity. However, two main features of the preliminary goals and objectives stick out. First, they are clear, concise and straightforward. While implementation likely would vary across sectors and entities, they are at least well organized and easy to understand. And second, CISA provided “Sample Evidence of Implementation” notes for each goal and objective, which likely would prove highly useful in measuring and, as needed, demonstrating progress and performance going forward. With regard to next steps, it would be prudent for affected control system owners and operators in relevant critical infrastructure sectors to review the preliminary goals and objectives in detail and begin to think about any necessary adjustments to their cybersecurity programs and practices that might be necessary to meet them. Beginning this work well in advance of the final cross-sector and sector-specific goals next year could pay significant dividends over time.

Categories

Transmission

Smart Grid/Energy Storage

Lobbying & Public Policy

Renewable Energy

Climate Change

Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.