NIST Special Publication 800-53
Revision 1

Recommended Security Controls for Federal Information Systems

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner
George Rogers

I N F O R M A T I O N S E C U R I T Y

SECOND PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

July 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

APPENDIX I

INDUSTRIAL CONTROL SYSTEMS

INTERIM GUIDANCE ON THE APPLICATION OF SECURITY CONTROLS

Industrial control systems[1] are information systems that differ significantly from traditional administrative, mission support, and scientific data processing information systems. Industrial control systems have many unique characteristics—including a need for real-time response and extremely high availability, predictability, and reliability. These types of specialized systems are pervasive throughout the critical infrastructure, often being required to meet several and often conflicting safety, operational, performance, reliability, and security requirements such as: (i) minimizing risk to the health and safety of human beings; (ii) preventing serious damage to the environment; (iii) preventing serious production stoppages or slowdowns that result in negative impact to the nation's economy and ability to carry out critical functions; (iv) protecting the critical infrastructure from cyber attacks and common human error; and (v) safeguarding against the compromise of proprietary information.[2]

Until recently, industrial control systems had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. In many cases, industrial control systems are using the same commercially available hardware and software components as are used in the organization's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation for these systems from the outside world and introduces many of the same vulnerabilities that exist in current networked information systems. The result is a greater need to secure industrial control systems.

FIPS 200, in combination with NIST Special Publication 800-53, requires that federal agencies implement minimum security controls for their organizational information systems based on the FIPS 199 security categorization of those systems. This includes implementing the minimum baselines described in Special Publication 800-53 in industrial control systems that are operated by or on behalf of federal agencies. This appendix discusses the problems that agencies may encounter in applying the security controls in Special Publication 800-53 to industrial control systems and provides some observations and recommendations on how to meet the intent of the requirements until NIST develops additional guidance specific to those types of systems. The specific guidance for industrial control systems may include modifications of the current security controls and control enhancements and/or interpretations of selected security controls for the specialized environments in which the controls are applied.

[1] An industrial control system is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. Industrial control systems are typically found in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries as well as in air and rail transportation control systems.

[2] See Executive Order 13231 on Critical Infrastructure Protection, October 16, 2001.

Because today's industrial control systems are a combination of legacy systems, often with a planned life span of between twenty to thirty years, and/or are a hybrid of legacy systems augmented with today's commercially available hardware and software that are interconnected to other organizational information systems, it is often difficult or impossible to apply some of the security controls contained in Special Publication 800-53. Recognizing this problem, NIST has initiated a high-priority project in cooperation with the public and private sector industrial control system community, to develop specific guidance on the application of the security controls in Special Publication 800-53 to industrial control systems. Since the project is still ongoing, the resulting guidance could not be included in the current release of Special Publication 800-53. However, on the basis of the project results to date, NIST makes the following observations and recommendations for organizations that own and operate industrial control systems:

- Section 3.3 of Special Publication 800-53, *Tailoring the Initial Baseline*, allows the organization to modify or adjust the recommended security control baselines when certain conditions exist that require that flexibility. Based on the discussion above, NIST recommends that industrial control system owners take advantage of the ability to tailor the initial baselines when it is not possible or feasible to implement specific security controls contained in the baselines. However, all tailoring activity should, as its primary goal, focus on meeting the intent of the original security controls whenever possible or feasible. Additionally, the organization must address the residual risks present after the tailoring is completed.
- In some cases, it may be infeasible, impractical, or unsafe to implement a specific security control within an industrial control system. For example, AC-11, *Session Lock*, is required for all moderate-impact and high-impact information systems. For industrial control systems with requirements for real-time response and extremely high availability, predictability, and reliability, session lock may not make sense (e.g., locking an operator's session in an electric power distribution system or an air traffic control system). However, the purpose of the session lock control is to prevent unauthorized access to an information system when the user or operator leaves the terminal or workstation unattended for a period of time. In this case, in order to meet the intent of the session lock security control, an organization could utilize the compensating control concept described in Section 3.3. With appropriate rationale and justification as described in the compensating control section, an organization can choose to compensate for not using session locks by incorporating other safeguards and countermeasures (e.g., increasing physical security, ensuring physical isolation of the terminal or workstation, increasing personnel security, and/or adding surveillance equipment to ensure that only authorized or trusted personnel are permitted in the vicinity of the terminal or workstation).
- Until NIST completes the industrial control system project and publishes specific guidance for industrial control systems, organizations should adjust their ongoing activities aimed at determining compliance with FIPS 200 and Special Publication 800-53 to allow for the types of flexibility that are discussed above. However, it is also reasonable to require industrial control system owners to develop a multiyear plan to demonstrate how the system owner plans to transition the industrial control system to a state that is fully compliant with FIPS 200 and Special Publication 800-53, particularly for systems that are planned to be in operation for several more years.