ENGINEERING WHITEPAPER

Peraton

RISK MANAGEMENT FRAMEWORK SERVICES

Cybersecurity Risk Management Framework Services for Secure, Compliant Information Technology and Operational Technology Infrastructure for U.S. Government Facilities

Government systems and facilities are prime targets for cyber attacks. Everything from information technology to cyber physical control systems to building facilities require risk and threat management. Peraton Labs specializes in the validation, engineering, assessment, and authorization of classified and unclassified systems and enclaves in accordance with the NIST Risk Management Framework (RMF) and the Federal Information Security Management Act (FISMA) to help federal agencies obtain and retain their Authority to Operate their networks and systems.

THE CHALLENGE

Civilian and defense government systems and facilities are prime targets for cyber attacks. While IT networks and systems have been the traditional focus for cybersecurity, government facilities have many other electronic systems and networked equipment to support base operations, building management, and cyber physical technology that have in the past been exempt from cyber policy. The interconnected nature of these systems means a compromised system could affect other systems, spreading the effects of the attack. Peraton Labs specializes in the validation, engineering, assessment, and authorization of classified and unclassified systems and enclaves in accordance with the NIST Risk Management Framework (RMF) and the Federal Information Security Management Act (FISMA).

Many government programs and facilities have legacy infrastructures that no longer meets the current U.S. government standards for cybersecurity and monitoring. Support systems, notably operations technology for mechanical, fire protection, electrical distribution, and other base and building infrastructure must now be scrutinized to the same extent as IT networks and systems. Further, advances in control system technology introduces new attack surfaces. Base and building support facilities and automation systems have become more intelligent, more dependent upon processor-driven control, and reliant upon firmware patching and network access for facility monitoring, energy management, and integration into base micro-grid systems. Cyber attacks are not limited to desktop computers—many support facilities are controlled by processor-driven systems that need to be secured.

Known as Industrial Control Systems (ICS), these cyber physical systems present a much broader cyber attack surface than traditional infrastructure and must be protected for mission assurance. ICS is a collective term that describes different types of control systems and associated instrumentation. It includes the devices, systems, networks, and controls used to operate and/or automate industrial processes. For example, an ICS network can monitor many infrastructure systems, such as military base and airport runway lighting, hanger door controls, facility HAVAC, elevator, water, sewer control and, IoT networks.

Supervisory Control and Data Acquisition (SCADA) is a subset of ICS that focuses on the networks and user interfaces that facilitate industrial systems. SCADA systems collect data from remote locations and provide a centralized interface for monitoring and control. They provide a graphical user interface for operators to observe the status of a system, receive any alarms, and control the process. More SCADA systems are being introduced as government facilities are modernized.

Securing these systems requires specific skills - a combination of SCADA and control system engineering expertise and domain knowledge; deep familiarity with NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations); CISSP certifications; and experience in successfully bringing large-scale control systems through the certification process to Authorization-to-Operate (ATO) under the Risk Management Framework.

FISMA is a federal law that requires federal agencies and vendors to develop, document, and implement an information security and protection program. FISMA was enacted in 2002 to protect government information, operations, and assets. Some FISMA compliance requirements include:

- Maintaining an inventory of IT systems
- Categorizing data and systems according to risk level
- Assessing risk and maintaining a system security plan

Peraton Labs Risk Management Framework Solution

Decades of experience

Design & Charette support

Define RMF scope

Stakeholder relationships

Risk tolerance

Define cybersecurity architecture

RMF package preparation

Service value

The security authorization process required for Information Systems (IS) in the federal government requires an ATO for all infrastructure. The ATO is the decision that culminates from the security authorization process of a technology system in the US federal government, which is a unique industry process requiring specialized practices.

The U.S. Government has steadily increased its security requirements for ICS, building automation, life safety, and base control systems, bringing them under the Risk Management Framework process with DoD Unified Facilities Criteria (UFC) 4-010-06 and Unified Facilities Guide Specifications (UFGS) 25 05 11.

PERATON LABS SOLUTION

Our approach covers cybersecurity measures and controls for the control system applications, intelligent electronic devices and remote terminal units, communication networks, telemetry reporting and control, and automation logic to provide the appropriate Confidentiality, Integrity, and Availability (CIA) impact level (low, moderate, high) for each device and control system application. The RMF, as applicable to UFC 4-010-06, UFGS 25 05 11, and other applicable government cybersecurity requirements are incorporated into the cyber design and applicable engineering deliverables (drawings, outline specifications, data acquisition, cost estimate, etc.).

A successful facilities upgrade project now requires the discipline of cybersecurity to take a seat at the table with the architects, engineers, and trades to contribute to the facility design to minimize potential cyber risks, suggest alternatives and compensating solutions, and provide guidance to eliminate unnecessary features that may create additional cybersecurity burden and project cost. Peraton Labs provides RMF consulting services to support the end-to-end process for facility renovation, rebuilds, and upgrade projects.

Support Design and Charettes

Should the government wish to use a charette as a collaborative planning process to harnesses the talents of interested parties to create the project master plan, Peraton Labs will participate in on-site/remote facility investigation meetings and design charettes with the customer stakeholders to represent the project cybersecurity requirements, begin identifying the systems that will be subject to RMF, and ensure the project plan and budget appropriately reflect the needed activities, milestones, resources, and schedule to achieve ATO.

Peraton Labs will meet with the system owner and authorizing official to understand the Confidentiality, Integrity, and Availability (CIA) impact levels assigned to facility systems.

Define RMF Scope

Peraton Labs will define the RMF scope by identifying all control systems, facility assets, building automation, environmental support, and communications systems that require cybersecurity consideration and RMF review as addressed in design and charette meetings. This activity includes identifying all cybersecurity requirements by Common Control Identifiers (CCI).

Establish Stakeholder Relationships

Peraton Labs will establish relationships with the site security officers to understand security priorities, special, site-specific cybersecurity considerations, and cybersecurity CIA requirements for the project.

Identify System Risks

Peraton Labs will research and investigate the proposed systems, review the vendor documentation, and speak with the product vendors to understand the capabilities and limitation of their equipment. Based on the mission and function of the system(s), and the detailed review of specific equipment chosen to implement the architecture design, Peraton Labs will assess each system's risk level according to its Confidentiality, Integrity, and Availability impact (low, moderate, or high).

Define Cybersecurity Architecture

Peraton Labs will define and convey an overall cybersecurity strategy and architecture to be included in the system design. Peraton Labs will apply inherited security controls where appropriate to reduce project costs. Using the impact levels, Peraton Labs will identify and document the cybersecurity controls NIST SP 800-82 to be applied to each component. The determination of cybersecurity risk reduction must also consider any risks to system functionality due to application of the security controls.

Peraton Labs will prepare or support the creation of the system cybersecurity configurations and conduct control-based validation and vulnerability testing.

Prepare RMF Package

Peraton Labs will support the system security authorities in submission of the RMF package for government approval and ATO. Peraton Labs will prepare all the necessary artifacts for the components, document the Control Correlation Identifier list for each of the singular, actionable statements that comprise a security control, ensure cybersecurity design considerations are incorporated in all applicable deliverables.

Peraton Labs will review the RMF package with the residing ISSOs and related stakeholders, identify and direct any needed modifications to the RMF package, and provide support for submitting the RMF package for government approval and ATO.

Peraton Labs will modify the RMF package and develop appropriate Plan of Action and Milestones (POAM) to address Security Control Assessor and ATO review comments for resubmission, as required.

Decades of Experience

Peraton Labs has decades of experience with ICS, government cybersecurity and the RMF process in both unclassified and classified environments, including programs involving tactical weapon systems and radio signaling.

Our expertise in control systems and operational technology stems from over a decade of experience supporting critical infrastructure operators in the utility, energy, water, gas and industrial control sectors. Peraton has developed deep domain expertise to understand the engineering operation of controls systems, their unique risks and cyber limitations, and operational activities they need to support as real-time control systems. Securing control systems infrastructure is a balance of reducing cyber risk while maintaining availability and system reliability.

Peraton Labs experience in providing cyber integrity solutions for critical infrastructure systems has been recognized by the cyber insurance industry. Peraton Labs offers unique technology as part of its SecureSmart™ Critical Infrastructure Protections Products and Services Line that have been designed as cyber catalyst technologies by the eight largest providers of cyber insurance.

We understand the RMF process intimately and its application to control systems. DoD Instructions 8500.01 and 8510.01 define the Risk Management Framework (RMF) and establish a category for ICS or “special purpose” systems that are not traditional information technology, called Platform Information Technology (PIT) systems. PIT systems, which include ICS, use specifically tailored security controls sets and require the cybersecurity architect to have expertise in the system.

Our Information Systems Security Managers (ISSM) and Information Systems Security Officers (ISSO) have expertise in developing artifacts, assigning controls, demonstrating compliance, and achieving ATO for control system infrastructure. Our ISSOs support the entire accreditation lifecycle and security engineering activities from the base system design -- guiding development teams on applicable Information Technology (IT) and Operational Technology (OT) control requirements, including AR 25-2, DODI 8500, NIST SP 800-53, DoD Security Technical Implementation Guides (STIGs), and CNSSI 1253 security requirements at all sensitivity levels.

For the OT UFC and UFGS mentioned above, Peraton Labs uses the Intelligence Community Standards 705-1 and 705-2 along with Department of Defense Manual 5200.01 volume 3 for construction and management in our Sensitive Compartmented Information Facilities in 5 company CONUS locations. Post initial deployment, our ISSOs create and manage Continuous Monitoring control activities, ATO Change Requests, FISMA reports, Continuity of Operations (COOP) periodic reviews, and Certification yearly reviews. We conduct verification testing and produce risk assessments for the solution based on test results.

Our ISSMs ensure the data ownership and responsibilities are established for each Information System (IS), and specific requirements to include accountability, access and special handling requirements are enforced. Further, the ISSMs work with industry partners to ensure physical security measures are met and compliant with applicable NIST/DoD policy. Technical and procedural IS Security advice is always available to government and industrial teams, and together we develop and oversee operational information systems security implementation policy and guidelines.

CONTACT US

For more information on Peraton Labs RMF service offerings, including Rough Order of Magnitude pricing, contact:

Stan Pietrowicz
Director
Secure Infrastructure Solution

spietrowicz@peratonlabs.com

or info@peratonlabs.com

RESOURCES

Information assurance and compliance - Peraton Labs

Network migration and modernization - Peraton Labs

ABOUT PERATON

Peraton is a next-generation national security company that drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As the world's leading mission capability integrator and transformative enterprise IT provider, we deliver trusted, highly differentiated solutions and technologies to protect our nation and allies from threats across the digital and physical domains. Peraton supports every branch of the U.S. Armed Forces, and we serve as a valued partner to essential government agencies that sustain our way of life. Every day, our employees do the can't be done by solving the most daunting challenges facing our customers. Visit Peraton.com to learn how we're safeguarding your peace of mind.

Scan to learn more at
peratonlabs.com