Incorporating Updates to Security and Privacy in 2021

An Urgent Need to Implement NIST 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations

NIST Revision 5

NIST Revision 5 is a **major update** to the NIST 800-53 Special Publication Series. NIST's rationale for undertaking Revision 5 is that "the cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more proactive and systematic approach to U.S. cyber deterrence is urgently needed." (Defense Science Board, 2017). U.S. infrastructure, including Federal government systems, private and/or public systems for water, electrical power, healthcare, and others, are at greater risk. NIST therefore saw the need for a "comprehensive catalog of security and privacy controls" that can be used to manage risk for organizations of any sector and size, and all types of systems—"from super computers to industrial control systems to Internet of Things (IoT) devices." (Rev. 5, NIST blog)

Among the changes in Revision 5 are:

- The names of security control families remain the same but there are significant additions to the numbers of controls.
- The controls have been rewritten to have an outcome-based focus.
- Due to the widespread move to digital transformation from paper files, the threat to the security and privacy of data - either in transit or at rest, either in the cloud or on premise - is heightened. NIST has included a new family of privacy controls (PT – PII Processing and Transparency) as well as incorporating privacy controls into the existing Program Management control family.
- A new Supply Chain Risk Management (SR) control family incorporates risk management to address supply chain vulnerabilities.
- The Program Management controls, which are on the enterprise (not system) level, have been moved from Appendix G to the body of the document.

"The cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities… a comprehensive catalog of security and privacy controls… is urgently needed."

- Where Revision 4 had 17 control families, Revision 5 has 20 control families.

Since Revision 5 is targeted to wider communities of interest, it acknowledges that different organizations may want to use different methods for the selection of applicable controls for their systems. Thus, the new revision does not supply guidance for selecting controls, but moves that guidance to NIST SP 800-37, Revision 2, which describes the Risk Management Framework (RMF). Revision 2 of the RMF was published in December 2018 and adds the Prepare step to the six steps – now seven - of the Risk Management Framework.

Due to the urgency of the needed update, Revision 4 will be withdrawn on September 23, 2021 and Revision 5 will take its place. Because NIST has developed 800-53 Revision 5 into a "consolidated security and privacy control catalog", the control baselines for systems have also been moved, to NIST SP 800-53B, Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations, published on 12/10/20.

NIST has outlined a four-step process for the transition from Revision 4 to Revision 5

The first (and current step, as of December 2020) includes reviews and updates to baselines, parameters, and control guidance, as well as the development of an implementation guide for Cloud Service Providers (CSPs). Step Two will include a public comment period lasting from 90 to 120 days. In Step 3, NIST will review public comments and update FedRAMP baselines and templates accordingly. In Step 4, NIST will release the final Revision 5 documentation updates. NIST will also provide training forums on the updates and will be available to answer questions.

Information System Security Officers (ISSOs) and Security personnel should note that the FedRAMP templates page, which includes the System Security Plan (SSP) templates for Low, Moderate, and High systems, continues at this time to maintain the templates for Revision 4. Revision 5 templates will not be finalized until sometime in 2021.

A new development of note that is separate from, but related to, NIST 800-53 Revision 5, is OSCAL. NIST is developing the Open Security Controls Assessment Language (OSCAL) in collaboration with industry. As planned, OSCAL will make significant innovations in the way that System Security Plans (SSPs) and security packages are generated for FedRAMP. Future NIST 800-53 revisions will include the OSCAL format. Today's security packages are manually prepared in Word or Excel documents, which is always a labor-intensive process. NIST and FedRAMP are planning a format in which security packages are digitized and generated in a standard language, which is both human and machine-readable. This will expedite the reviews of security packages and make possible a faster route to authorization, while

Innovations from NIST in Digitization, Privacy, and Supply Chains – OSCAL and two new control families

© 2021 CGI Inc.

cutting the costs and improving quality. Federal agencies, third-party assessors, the FedRAMP PMO, and cloud service providers will all benefit. FedRAMP has released three pre-releases and is set to release OSCAL Version 1.0 in the near future. FedRAMP's "A Guide to OSCAL-Based System Security Plans" (Version 2, Draft) was released in August 2020. FedRAMP guides, training, and content converters are available on the FedRAMP GitHub site and from NIST.

The new family of Privacy Controls in NIST 800-53 Revision 5 (PT – PII Processing and Transparency) emphasizes the heightened profile for the privacy of data that is processed in Federal systems. CGI supports systems that process the data of both U.S. and foreign nationals, and is a participant in the Privacy Shield framework. Privacy Shield is currently in the process of renegotiation. Laws governing data privacy vary widely at the national and international levels, and CGI is committed to awareness and compliance with this important and changing issue.

Revision 5 provides guidance for the next generation of NIST's security and privacy controls framework. It addresses the need for a more proactive and systematic approach to cybersecurity in order to have the resilience to withstand sophisticated cyber attacks.

As consultants to government and industry, CGI has an important role in alerting our clients to upcoming changes, understanding what the changes will mean to client systems, while supporting planning and preparations for the changes. In this effort, CGI strives to support the best security possible for Federal systems and data.

For more information, please contact Lynn Goodrich at lynn.goodrich@cgifederal.com.

CGI is committed to awareness and compliance in the important and changing area of data privacy

We are CGI

Connected by a common dream, management approach and vast network of expertise.

"Insights you can act on."

© 2021 CGI Inc.