NIST SP800-53 Rev. 3: 
Applicability to Government and Non-Governmental Organizations

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The National Institute of Standards and Technology (NIST) Special Publication (SP) SP 800-53 provides a unified information security framework to achieve information system security and effective risk management across the entire Federal Government. In previous articles in this series, Dr. Paul J. Brusil summarized the risk management framework and the catalog of security controls offered in SP 800-53. In this last of four articles, Dr. Brusil reviews the relationship of Recommended Security Controls for Federal Information Systems and Organizations, Rev. 3<http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf> to other standards as well as its suitability for government and non-governmental organizations. Everything that follows is Dr. Brusil’s work with minor edits.

***

Communities Impacted by SP800-53


SP 800-53 (Appendix I) also contains additions to the SP 800-53 Appendix D security control baselines so that such augmented security control baselines (in Appendix I) can be used in the Industrial Control Systems community. SP 800-53 (Appendix I) also contains community-specific, security control tailoring guidelines and other supplemental guidance for 64 of the security controls applicable to Industrial Control Systems from the SP 800-53 (Appendix D) security control catalog.

develop, document and implement agency-wide IA programs that support operations and assets and provide “adequate security.” Every year, Inspectors General evaluate agency progress to achieve such requirements in the context of each agency’s unique mission, environment, and organization. SP800-53 is used as a guiding document to implement and to improve security under FISMA.

What the Critics Say

Although SP 800-53 is generally getting high marks from the IA community, it, and FISMA, are not without their critics.

Some say that certain agencies are not proficient in conducting a meaningful risk assessment and therefore will have difficulty identifying vital risks. Some feel that SP800-53 should have included measurable testing, third party validation and certification that IT systems meet their security requirements. Yet others argue that most threats are now high-end threats. Since systems are so interconnected and often have ill-defined, inadequate, leaky borders, low-impact systems are effectively higher-impact systems because low-impact systems can become insider attack platforms against interconnected higher-impact systems. Accordingly, they dismiss SP800-53’s discussion of low-impact and moderate-impact targets as irrelevant; all systems need to be protected against the types of attacks/attackers associated with high impact systems.

Some say that FISMA and the SP800-53 revision process are too static to keep up with quickly emerging threat landscapes or emerging protection technologies. Others say SP 800-53 is too flexible and is overly complex because so many security control choices are offered.

With regard to the latter point, some believe that a narrower subset or profile of SP800-53 provides the most critical security controls that address the most critical risks common to all parties. They feel some of the basic critical risks include:

- Not knowing the instantaneous inventory of hardware, software and configurations
- Providing “good” security features but not necessarily the “necessary” security features, and
- Not providing auditing to validate security and to verify on-going protection over time.

Unlike SP 800-53’s security control baselines, proponents of an alternative feel there is only a small set of common and critical technical and operational controls that are applicable to all parties. Additional, organization-unique controls may be added as necessary. These common controls, called the “20 Critical Security Controls” can also be used by auditors to check if organizations are compliant with the standards of SP 800-53. The majority of these Critical Security Controls can also be automated for testing.

Still others feel the burden of multiple, independent, overlapping and/or redundant compliance
Some feel that periodically demonstrating compliance to regulations is overly complex and time-consuming leaving less time to focus on an organization’s missions. In part to address such concerns, an updated version of NIST’s SP 800-37 Certification and Accreditation (C&A) Guidelines will refocus C&A from a periodic, one-time event to a more continuous process. Furthermore, new helpful technologies, such as continuous file integrity monitoring (see for example the white paper on “Continuous File Integrity Monitoring with Minimal System Impact and No Repeat Scans” from McAfee), are emerging to facilitate a shift from point-compliance testing to continuous compliance assurance.

Some believe that certain agencies may use FISMA – and by indirection SP 800-53 – as a paperwork exercise just to fill out FISMA reporting documents due to the OMB rather than to verify or to improve information assurance. They also feel there should be detailed metrics for measuring the readiness and effectiveness of an organization’s security program on an ongoing basis.

This begs the question as to whether there is an over reliance on compliance just for the sake of compliance. The credibility issue of using compliance to guarantee security has been elevated given risks that were recently revealed in the financial industries and electric industries. Some systems were deemed compliant to the Payment Card Industry Data Security Standard (PCI DSS), or the North American Electric Reliability Corp (NERC). Security could be compromised by ambiguities and shortcomings in the guiding standards. A recent GAO finding pertinent to reports of FISMA compliance associated with use of the previous version of SP 800-53 indicated disconnects between FISMA compliance reports and agencies’ actual security posture. Whether or not the newly revised SP800-53, Revision 3, may have any such issues is not known.

The Bottom Line: SP 800-53 is Good for IA

Regardless of viewpoints on FISMA, many trust that when SP800-53 is followed, information assurance does improve. DoD and Federal government agencies will use SP800-53 and those that do so as an opportunity to improve security rather than to conduct a fill-out-the-form exercise will benefit. They will establish a level of security due diligence. The private sector would do well to follow suit.

* * *
Dr Paul J. Brusil, PhD, MD <brusil@post.harvard.edu> graduated from Harvard University with a joint degree in Engineering and Medicine. He has authored over 100 papers and book chapters in his distinguished career and worked in a wide range of industry and government sectors as a respected security network management and program management consultant. He on the editorial boards of several journals including the Journal of Network and Systems Management <http://www.csee.umkc.edu/jnsm/> and is a Lead Instructor for the Master of Science in Information Assurance at Norwich University.<http://infoassurance.norwich.edu/> 

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/> 

Copyright © 2009 Paul Brusil & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.