Standards play a critical role in information assurance. Given the impossibility of defining a deterministic model that includes billions of users, millions of computers, and thousands of programs and protocols potentially interacting with each other unpredictably, we have to rely on human consensus about best practices if we are to progress in our field. Standards also provide a basis for demonstrating due care and diligence in fulfilling our fiduciary responsibilities to stakeholders.

In this first of four articles about the latest revision of a landmark Special Publication (SP) from the Joint Task Force Transformation Initiative in the Computer Security Division of the Information Technology Laboratory of the National Institute of Standards and Technology (NIST), Dr Paul J. Brusil reviews the key recommendations and strategic guidance offered in 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> which has been prepared by a panel of experts drawn from throughout the US government and industry. Everything that follows is Dr Brusil’s work with minor edits.

* * *

From the furthest corners of the U.S. Defense and Intelligence communities to every civil office in the U.S. Federal government, a single new security standard applies to all government information systems – including national security systems. Traditionally, the Department of Defense (DoD) and the civilian federal agencies independently develop their own standards. Harmonizing the security needs of all government agencies has been a long time coming; but, for the first time ever, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, 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> dated August 2009 does just that.


SP 800-53 is part of an extensive library of guidelines, recommendations and standards NIST publishes and continually updates to help organizations protect their information systems and data <http://csrc.nist.gov/publications/PubsDrafts.html>. Protected information systems include all constituent components – local and remote – for processing, storing and transmitting information.

The purpose of SP800-53 is to achieve information system security and effective risk management, in part, by providing a common information security language for all information systems and by providing consistent and repeatable guidelines for selecting and specifying standard security controls. With the aid of SP 800-53, organizations are able to select appropriate security controls to meet security requirements, to implement the selected controls correctly and to demonstrate the confidence and effectiveness of selected controls in complying with security requirements. SP 800-53 guides security managers, security service providers, security technology developers, system developers, system implementers and system assessors.

Office of Management and Budget (OMB) policies mandate all Federal agencies, their contractors and their external service providers use SP 800-53. The existence of SP800-53 as a government regulation has many benefits beyond the stipulation of security best practices. For one, it elevates security awareness to senior management. Correspondingly, security funding can be positively impacted.

SP800-53 is a living document updated periodically. The just-released Revision 3 supersedes the previous revision released 18 months earlier. It contains or amplifies a risk management framework, a security control catalog, a security control selection process, traceability of security controls to underlying security requirements, assurance requirements for security controls, and extensions for use in communities outside the U.S. government.

In the next part of this four-part series, Dr Brusil discusses the risk management section of SP 800-53 Rev. 3.

* * *

Dr Paul J. Brusil, PhD, MD <mailto: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 is 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.