At Norwich University, we always encourage our students to write for publication rather than simply to meet course requirements. As a result, many of our students forward interesting articles for possible publication to me. I am delighted to present a two-part analysis of compliance in information assurance by Norwich MSIA student Graydon S. McKee IV, CISSP, GSEC and his colleague at Unisys Corporation, Joseph Faraone, CISSP.

The remainder of today’s and the next column are entirely my guests’ work (with minor edits).

* * *

Sometimes we hear top security executives expressing frustration with government regulation by saying that the issue has come down to a choice of either being secure or being compliant.

As reported by _Information Security_ magazine in their October 2005 issue, security managers were asked to respond to the question: “What is your biggest obstacle to implementing and managing security-related government regulations?” Responses reveal that the top two obstacles faced were unclear compliance-related responsibilities and interpreting regulatory language.

As information security professionals, we are dismayed at hearing this kind of talk, especially from senior agency officials and corporate board members. This point of view appears to be more prevalent in the private sector than the public sector. This discrepancy leads one to inquire into the cause.

One of the reasons for this discrepancy is that the public sector must follow a specific framework for measuring the maturity and effectiveness of their information security programs: certification and accreditation (C&A). The Federal Information Security Management Act of 2002 (FISMA) (Title III of the e-Government Act), was intended to provide for the development of and maintenance of minimum controls required to protect information systems and to provide for a framework for ensuring the effectiveness of these controls. While many of the overriding principles followed in C&A are contained within the Act, nowhere are the words “certification” or “accreditation” found.

FISMA points to the Office of Management and Budget (OMB) as well as the National Institutes of Standards and Technology (NIST) to obtain guidance. OMB has issued their Circular A-130 which requires that all federal information systems to be certified and accredited following guidelines developed by NIST. To the private sector, this may seem like just another paper exercise, but this perspective seems to us like losing the view of the forest.

NIST has done a laudable job of developing and revising this guidance. It provides a methodology to fully document, measure, assess, track, and report on the health of information systems from the aspect of security. These guidelines show how to integrate the information security program with the systems development life cycle and with the recent publication of their
“Special Publication 800-53: Recommended Security Controls for Federal Information Systems” <http://tinyurl.com/mq3cp> provide a minimum recommended baseline of controls tied to the type of information (and information criticality) that is within an information system. This guidance is recommended until the release of Federal Information Processing Standard (FIPS) 200. FIPS 200 will make the minimum baseline controls found in NIST Special Publication 800-53 mandatory for all federal information systems.

* * *

More in the concluding part of this two-part article.

* * *

About the authors:

Mr McKee has recently been delivering an ongoing series of national level seminars through the Potomac Forum, Ltd, a non-profit Educational Foundation founded in 1982 <http://www.potomacforum.org/>. These seminars focus on the process of Certification and Accreditation under both FISMA and DITSCAP and to date have been delivered to senior officials and technical personnel from every government agency and a majority of the Department of Defense. Mr Faraone has extensive experience in risk analysis and incident response management with many years of consulting with Booz|Allen|Hamilton, Deloitte Touche and Unisys. He has made several public speaking appearances at the University of Florida, University of South Florida, at regional meetings of FBI Infragard chapters, and professional organizations.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay, G. S. McKee & J. Faraone. 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.