GSAW 2017 Tutorial B:

Integrating Cybersecurity into the System Lifecycle Using the Risk Management Framework (RMF)

Length: Half day

Overview:
Abstract

The Risk Management Framework developed by NIST and documented in NIST SP 800-37 Revision 1 has become the standard across the entire US Government – both National Security Systems (NSS) and non-NSS — for determination of security requirements, assessment of security requirements, and authorization for operation. This tutorial provides a detailed introduction to the Risk Management Framework, explores how to integrate it into the acquisition lifecycle, and stresses the importance of doing so early as part of the process of system security engineering. This tutorial examines the set of security controls defined for Federal systems in NIST SP 800-53 Revision 4, as well as the process for selecting, tailoring, and supplementing those controls. It also discusses how this process is adapted for use in National Security Systems through CNSS Instruction No. 1253 and goes through the tasks involved in the Risk Management Framework. The tutorial provides an overview of the applicable NIST documents (NIST SP 800-53 Revision 4, NIST SP 800-37 Revision 1, NIST SP 800-30, NIST SP 800-39), and the corresponding application to National Security Systems (CNSSI No 1253, DODI 8500.01, DODI 8510.10, and ICD 503).

Outline

I. Background: A Paradigm Shift
    a. Where We Were
    b. The Realizations Hits
        i. Realization One: Its Part of the Mission
        ii. Realization Two: There's Only So Much Money
        iii. Realization Three: Techniques Invariant Among Applications
    c. Joint Taskforce Transformation Initiative
    d. The Unified Framework
    e. The Risk Management Framework
II. Understanding Risk in the Enterprise
III. Using the RMF to Engineer Security
    a. The Cybersecurity Control Catalog
    b. Control Selection, Supplementation, and Tailoring
    c. Reviewing The Control Catalog
    d. RMF and System Security Engineering
    e. RMF Steps 1-3: Categorize, Select, Implement
IV. Using the RMF to Ensure and Maintain Effective Cybersecurity
    a. RMF Steps 4-6: Assess, Authorize, Maintain
    b. Transitioning to the RMF
V. Conclusion

Instructor: Daniel Faigin, The Aerospace Corporation

Biography:
Daniel Faigin has been involved with computer security since 1985, when he was one of the architects on the BLACKER program at SDC. Since joining Aerospace in 1988, he has been closely involved with both the commercial product evaluation programs of the NCSC/CCEVS (i.e., TCSEC, Common Criteria), as well as certification and accreditation efforts on a number of space programs. He is the author of a number of reports providing information assurance guidance, including in-depth extensive analysis of both the 8500.2 controls and the 800-53 controls, exploring how these controls are applied to space systems. He is a contributor to the development of the Space Platform Overlay, is one of the authors of the IA section of the Mission Assurance Guide, and is the developer of the CSI:53 tool.

Mr. Faigin has an M.S. and B.S. degrees from UCLA, and is a CISSP. He has been the education chair of the Annual Computer Security Applications Conference (ACSAC) since 1990, and is currently both education and local arrangements chair for ACSAC.

Description of Intended Students and Prerequisites:
No particular prerequisites; perhaps a familiarity with acquisition and some form of security criteria?

What can Attendees Expect to Learn:
Tutorials can expect to learn what the NIST SP 800-53 Rev 4 controls are, how the Risk Management Framework works, how it is applied to National Security Systems, and how one can leverage the RMF during the early acquisition process.