GSAW 2013 Tutorial E:

Cybersecurity in the Acquisition Process: The Transformed Lifecycle Risk Management Process

Length: Full day

Overview:

Addressing the confidentiality, integrity, and availability of information in a ground system—as well as ensuring information resiliency—is one of the goals of integrating security engineering into the system engineering process. This integration is fundamental to the emerging Risk Management Framework, which is replacing the previous notion of "Certification and Accreditation" as the means of ensuring a ground system has adequate security to operate. This tutorial will provide an overview of this transformation to an assessment and authorization process that emphasizes system security engineering. It will address how to integrate information assurance into the lifecycle of a ground system, from the early concept stages and requirement selection to the assessment and continuous monitoring of security requirements. It will provide an overview of the applicable NIST documents (NIST SP 800-53 Revision 3, NIST SP 800-37 Revision 1, NIST SP 800-30, NIST SP 800-39) and their interpretation and applicability to space systems. This will include CNSSI 1253, the Space Overlay, and (based on the latest information) the updates to DOD 8500.1 and 8500.2.

The Joint Task Force Transformation Initiative Working Group with representatives from the Civil, Defense, and Intelligence Communities is an ongoing effort to produce a unified information security framework for the U.S. Federal government including a consistent process for selecting and specifying safeguards and countermeasures (i.e., security controls) for federal information systems. The initiative has addressed the transition from periodic Certification & Accreditation to continuous monitoring and Integrated Enterprise-Wide Risk Management.

Instructors: Daniel Faigin, The Aerospace Corporation; Ron Ross, National Institute of Standards and Technology

Biographies:

Mr. 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 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 overlay, and is one of the authors of the IA section of the Mission Assurance Guide.

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 since 1990.

Dr. Ron Ross is a Fellow at the National Institute of Standards and Technology (NIST). Dr. Ross currently leads the Federal Information Security Management Act (FISMA) Implementation Project for NIST, which includes the development of key security standards and guidelines for the federal government, contractors supporting the federal government, and the critical information infrastructure. Dr. Ross is also the principal architect of the Risk Management Framework (RMF) that integrates the suite of NIST security standards and guidelines into a comprehensive enterprise-wide information security program. Dr. Ross is a graduate of the United States Military Academy at West Point and the Program Management School at the Defense Systems Management College. He holds both Masters and Ph.D. degrees in Computer Science from the United States Naval Postgraduate School.

What Participants Should Expect to Learn:

After completion of this course, participants in the course should be familiar with the basic NIST SP 800-53 Control Catalog and have a rough familiarity with the IA controls therein. They should also know the six steps of the risk management framework, and how these steps are applied to national security systems. They should also understand how overlays work, and the specific overlays applicable to the segments of a space system.

Who Should Attend:

Participants in this tutorial should be individuals interested with the integration of information assurance into the system engineering process, and the subsequent assessment of the security requirements. Familiarity with the current DIACAP or NIACAP processes is beneficial, but not required.