**GSAW 2014 Tutorial F:**

Software Assurance Engineering: Integrating Security into the Acquisition and Development Life Cycle

**Length:** Full day

**Overview:**
Much of what is in place today for information protection is based on principles established by Saltzer and Schroeder in their paper titled “The Protection of Information in Computer Systems” which appeared in Communications of the ACM in 1974. Security is described as “techniques that control who may use or modify the computer or the information contained in it” and described the three main categories of concern: confidentiality, integrity, and availability (CIA). While these principles are still usable today in consideration of security within an individual piece of technology, they are no longer sufficient to address the complexity and sophistication of the environment within which that component must operate. We must broaden our horizon to consider the large scale, highly networked, software dependent systems upon which all of our critical infrastructure from phones to power and water and industries such as banking, medicine, and retail depend. Software assurance is the term that has come into common usage to describe this broader context. The Committee on National Security Systems (CNSS) defines software assurance as follows: software assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software.

The purpose of this course is to expose participants to concepts and resources available now for their use to address software security assurance across the acquisition and development life cycles. The course combines lecture material with exercises and discussions.

**Course Topics**

- What is software assurance and why is it necessary
- Software assurance principles and practices
- Security requirements – an overview of security requirements engineering, covering topics from elicitation through review, along with pointers and links to additional resources
- Mission Thread Analysis – an evaluation approach for technology (software and systems) within the context of the mission to establish the role of technology in mission success, analyze the technology impact on potential mission failure, identify mission-critical technology dependencies and consider threats to mission success
- Supply Chain Risk Management to identify sources of vulnerabilities through a software supply chain, challenges in evaluating assurance of products and integrated solutions, emerging international standards, and acquirer actions needed to address software supply-chain risk

**Instructor:** Carol Woody, Software Engineering Institute

**Biography:**
**Dr. Carol Woody** has been a senior member of the technical staff at the Software Engineering Institute (SEI), Carnegie Mellon University since 2001. Currently she is the technical lead of the cyber security engineering team whose research focuses on building capabilities in defining, acquiring, developing, measuring, managing, and sustaining secure software for highly complex networked systems as well as systems of systems.Dr. Woody is an experienced technical researcher whose work has focused on government agencies, higher education, and financial organizations. She has helped them identify effective security risk management solutions, develop approaches to improve their ability to identify security and survivability requirements, and field software and systems with greater assurance. She holds a B.S. in mathematics from the College of William & Mary, an M.B.A. from Wake Forest University, and a Ph.D. in information systems from NOVA Southeastern University.

**Description of Intended Students and Prerequisites:**
The target audience includes software managers and technical leads, software and lead engineers, software and system acquisition experts, and program/project management who are concerned with software security assurance across the acquisition and development life cycles.

**What can Attendees Expect to Learn:**
Students who take this course will:

- Develop awareness of the value for software assurance and the challenges of integrating it into the software life cycle
- Develop an understanding of practices and methodologies available for addressing key areas of software assurance across the life cycle
- Recognize the need and be aware of what to do to address the following critical areas of software assurance: security requirements, mission thread analysis, and supply chain risk management.