## GSAW 2011 Tutorial A:

System Life Cycle Security Engineering

**Length:** Full day

### Overview:

Within the discipline of systems engineering (SE), information systems security engineering (ISSE) applies information assurance principles across a system's life cycle. Grounded by underlying security principles and a rigorous methodology, ISSE follows the "system thinking" approach for assessing system security behaviors based on dependencies, interactions and emergent properties of its components in the context of a larger system.

This tutorial aims to provide attendees with an overview of the ISSE methodologies and processes for the design, implementation and assessment of risk-based security solutions. Concepts and practices of information systems security engineering are presented from a system life cycle perspective. Core topics include security requirement engineering, architecture and design analysis, system implementation assessment, requirements-to-implementation traceability correspondence, security test and evaluation strategy, and risk management. In each stage of the system development life cycle, the roles and responsibilities of the ISSE team are explained.

**Instructors:** Thuy Nguyen, Cynthia Irvine, Naval Postgraduate School

### Biographies:

Ms. Thuy D. Nguyen is a Senior Research Associate of Computer Science at the Naval Postgraduate School in Monterey, California. She has 25 years of experience and specializes in high assurance software and systems development, security evaluation and information systems security engineering. Ms. Nguyen performs research on high assurance platforms, trusted operating systems and separation kernels, secure collaborative applications, MLS federated architectures and dynamic security services. She is the lead architect/engineer of the MYSEA multilevel secure (MLS) project and oversees the construction of a MLS testbed. She coauthored a Common Criteria Protection Profile for highly robust separation kernels and a draft Computing Platform Architecture and Security Criteria for the High Assurance Platform Program. She has developed and taught courses on security requirements engineering and applied information systems security engineering. Prior to NPS, she developed commercial security products, including a TCSEC Class A1 security kernel.

Dr. Cynthia E. Irvine is a Professor in the Department of Computer Science and Director of the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School, where she has worked since 1994. She was the founding director of the Cebrowski Institute at NPS from 2001 to 2003. A graduate of Rice and Case Western Reserve Universities, her research centers on the design and construction of high assurance systems and multilevel security. The author on over 150 papers and reports on cyber security, she has supervised over 120 Masters and PhD students. Dr. Irvine has served on numerous government computer and network security committees and review boards. Her memberships include: the ACM, ASP (life), IEEE (Senior) and the IEEE Computer Society Golden Core. A recipient of the Navy Information Assurance Award as well as numerous research and service awards, she served as Chair of the IEEE Technical Committee on Security and Privacy from 2007 to 2009.

### What Participants Should Expect to Learn:

Tutorial participants will understand the importance of capturing user's needs in a tractable form to guide development and risk analysis activities. They will be familiar with the properties used to evaluate different security architectures, the inherent trust problems relating to the composition of systems and

components, and security issues associated with the adaptation of existing systems to meet the need for technological and environmental evolution.

## Who Should Attend:

General knowledge of basic security principles and fundamentals of computer, software and network security is mandatory. Familiarity with system life cycle assurance (including threat characterization and risk analysis) and general systems engineering processes would be useful.