Tutorial
Developing Security Plans for Information Technology Systems

Instructor: Marianne Swanson, National Institute of Standards and Technology

The objective of system security planning is to improve protection of information technology (IT) resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987."

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager.

In order for the plans to adequately reflect the protection of the resources, a management official must authorize a system to process information or operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, a periodic review of controls should also contribute to future authorizations. Re-authorization should occur prior to a significant change in processing, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm.

The new NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems" provides a guideline for federal agencies to follow when developing the security plans that document the management, technical and operational controls for federal automated information systems. This tutorial is intended to guide the participant in documenting the management, technical, and operational controls for Federal automated information systems. The tutorial will introduce the new NIST document, provide background behind the various requirements, and explain how to use the document to complete security plans.

Marianne Swanson

Marianne Swanson is presently a Computer Specialist in the Computer Security Division at the National Institute of Standards and Technology (NIST). She works in the area of computer security and was the project manager for the government wide incident handling capability, FedCIRC. She was a founding member of the Forum of Incident Response and Security Teams (FIRST) and served as the Secretariat for the first five years. She is currently Acting Chair of the Federal Computer Security Program Managers' Forum. She co-authored the NIST Special Publication, "Generally Accepted Principles and Practices for Securing Information Technology Systems," and the NIST Special Publication, "Guide for Developing Security Plans for Information Technology Systems."

In 1996, Ms. Swanson received the Industry Advisory Council Leadership and Achievement Award for promoting support mechanisms for government wide security initiatives. Also in 1996, she received the Department of Commerce Bronze Medal Award. Ms. Swanson has over nineteen years of computer security experience. Prior to joining NIST, she worked as a Systems Security Specialist with the Nuclear Regulatory Commission and as a Program Analyst with the Internal Revenue Service.