IT SECURITY COMPONENT DEFINITIONS

This handout lists the IT security terms presented in the Requirements Overview section of the NIST *Integrating IT Security into Capital Planning and Investment Process Workshop*. The handout defines the applicable terms and crosswalks them to relevant NIST Guidance.

Term	Definition	Source
Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.	NIST SP 800-30, Risk Management Guide for IT Systems
Security Planning and Policy	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.	NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
Certification and Accreditation	Certification is the comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. Accreditation is the authorization of an IT system to process, store, or transmit information, granted by a management official. Accreditation, which is reaquired under OMB Circular A-130, is based on an assessment of the management, operational, and technical controls associated with an IT system.	NIST SP 800-37 (draft), Guidelines for Security Certification and Accreditation of IT Systems

Term	Definition	Source
Specific management, operational, and technical security controls	Management Controls 1. Risk Management 2. Review of Security Controls 3. Life Cycle Maintenance 4. Authorize Processing (Certification and Accreditation) 5. System Security Plan Operational Controls 6. Personnel Security 7. Physical Security 8. Production, Input/Output Controls 9. Contingency Planning 10. Hardware and Systems Software 11. Data Integrity 12. Documentation 13. Security Awareness, Training, and Education 14. Incident Response Capability Technical Controls 15. Identification and Authentication 16. Logical Access Controls 17. Audit Trails	NIST SP 800-26, Security Self Assessment Guide for Information Systems NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook *And multiple other guides addressing individual security controls.*
Authentication or cryptographic applications	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.	NIST FIPS 140-2, Security requirements for Cryptographic Modules NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure NIST SP 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication NIST SP 800-21, Guideline for Implementing Cryptography in the Federal Government,
Education, awareness and training	Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge.	SP 800-16 Information Technology Security Training Requirements: A Role - and Performance-Based Model
System reviews/evaluations (incl. ST&E)	Tests the effectiveness and efficiency of the security controls of an IT system as they have been applied in an operational environment, considering impact on the mission. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.	NIST SP 800-30, Risk Management Guide for IT Systems

Term	Definition	Source
Oversight or compliance inspections	Process of verifying the legally and technically correct implementation of security controls.	*No specific guidance to support external review. For internal review use:* NIST SP 800-26, Security Self Assessment Guide for Information Systems
Development or maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment	Guides agencies on compliance with legislative and executive branch data collection mandates.	OMB Memorandum 02-09, Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones (July 2, 2002) *No specific NIST guidance exists.*
Contingency planning and testing	Management policy, procedures, and technical measures designed to enable the recovery of IT systems, operations, and data after a disruption. This planning generally includes restoring IT operations at an alternate location, recovering IT operations using alternate equipment, performing some or all of the affected business processes using non-IT (manual) means (typically acceptable for only short-term disruptions, or any combination of these approaches.	NIST SP 800-34, Contingency Planning Guide for Information Technology Systems
Physical and environmental controls for hardware and software	Physical security and environmental controls are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment.	NIST FIPS 31, Guidelines For ADP Physical Security And Risk Management.
Auditing and monitoring	Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems.	SP 800-31, Intrusion Detection Systems NIST SP 800-26, Security Self Assessment Guide for Information Systems
Computer security investigations and forensics	Provides "advice for federal agencies and other organizations on establishing a Computer Security Incident Response Capability (CSIRC). A CSIRC provides computer security efforts with the capability to respond to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities, in an efficient and timely manner. A CSIRC further promotes increased security awareness of computer security-related risks so that agencies are better prepared and protected."	NIST SP 800-3, Establishing a Computer Security Incident Response Capability (CSIRC).

Term	Definition	Source
Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations	Significant quantities of data storage and processing occur on contractor systems. The federal government is increasingly sensitive to security of such systems that are outside of its direct control.	*No direct guidance supports this activity. Some associated guidance includes:* NIST SP 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials NIST SP 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, Draft NIST 800-35, Guide to Information Technology Security Services
Configuration or change management (CM) control	A management discipline applying technical and administrative direction to the development, production and support life cycle of a configuration item. This discipline is applicable to hardware, software, services, and related technical documentation. CM is an integral part of life cycle management and is a critical element of effective IT security.	*This topic is not discussed in NIST guidance*
Personnel security	Addresses special considerations regarding the management of people in an IT security environment. Includes topics such as background investigations, rules of behavior, controlling access to sensitive information, separation of duties, rotation of duties, and separation from service.	*NIST FIPS 31, Guidelines for ADP Physical Security and Risk Management*
Physical security	Refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.	NIST FIPS 31, Guidelines For ADP Physical Security And Risk Management NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
Operations security	Broad concept referring to these security controls: Personnel Security Physical Security Production Input/Output Controls Contingency Planning Hardware and Systems Software Data Integrity Documentation Security Awareness, Training, and Education Incident Response Capability	*No specific omnibus guidance exists on all these topics; many of these topics are discussed on an individual basis in NIST documents.* NIST SP 800-26, Security Self Assessment Guide for Information Systems

Term	Definition	Source
Privacy training	Supports compliance with the strict and varied federal regulations regarding the privacy of citizens, of businesses, and of employees.	*NIST has no guidance on this topic.*
Program/system evaluations whose primary purpose is other than security	See above, "System reviews/evaluations (incl. ST&E)". System security reviews are not driven by their business purposes, but rather by issues of sensitivity and criticality.	
System administrator functions	A system administrator is the hands-on technician who configures and maintains a computer system. This role may be formal or *ad hoc* and can apply to a wide range of technology platforms (e.g., Windows PC, Macintosh, Unix).	*No single guide exists for System Administrators. The following guides broadly address aspects of all System Administrators' work:* SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices SP 800-47 Security Guide for Interconnecting Information Technology Systems SP 800-46 Security for Telecommuting and Broadband Communications SP 800-45 Guidelines on Electronic Mail Security SP 800-44 Guidelines on Securing Public Web Servers SP 800-41 Guidelines on Firewalls and Firewall Policy SP 800-40 Procedures for Handling Security Patches *More specific guidance:* SP 800-43 Systems Administration Guidance for Windows 2000 Professional
System upgrades with new features that obviate the need for other standalone security controls	Vendors may implement security features into system upgrades that incorporate functionalities that have previously been handled by standalone pieces of software.	*NIST has no guidance on this topic.*