U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT-03-11
(REDACTED VERSION)

To:	NRC Management Directives Custodians
Subject:	Transmittal of Management Directive 12.5, "NRC Automated Information Security Program"
Purpose:	Directive and Handbook 12.5 are being revised to incorporate the revised security processes and procedures of the Federal Information Security Management Act, which was passed in December 2002. The act introduced a number of refinements to automated information security processes, procedures, and guidelines. MD 12.5 is now fully aligned with the new law. Because of the extent of the revision, no change bars have been used in MD 12.5.
Office Origin:	Office of the Chief Information Officer
Contact:	Kathy Lyons-Burke, 301-415-6595
Date Approved:	February 1, 1999 **(Revised: September 12, 2003)**
Volume:	12 Security
Directive:	12.5 NRC Automated Information Security Program
Availability:	Rules and Directives Branch Office of Administration Michael T. Lesar, 301-415-7163 Christy Moore, 301-415-7086

NRC Automated Information Security Program

Directive 12.5

Contents

NRC Automated Information Security Program Directive 12.5

Policy
(12.5-01)

It is the policy of the U.S. Nuclear Regulatory Commission to implement and maintain an agencywide automated information security program to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure— (011)

- confidentiality, that is, preserving authorized restrictions on access and disclosure, including the means for protecting personal privacy and proprietary information (a)

- integrity, that is, guarding against improper information modification or destruction and ensuring information nonrepudiation and authenticity (b)

- availability, that is, ensuring timely and reliable access to and use of information. (c)

The information security protections shall be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that are operated, maintained, or sponsored by the agency. (012)

Objectives
(12.5-02)

- To implement appropriate security measures to protect NRC information and information systems. Security measures include any computer-based hardware, software, or associated administrative procedures that are used to process, store, or transmit NRC information, whether it is classified, unclassified Safeguards, or sensitive unclassified. (Unclassified Safeguards Information (SGI) is defined in Management Directive (MD) 12.6, "NRC Sensitive Unclassified Information Security Program"). (021)

- To ensure that security measures provide the appropriate level of protection and reliable access to NRC information and information systems by authorized individuals and only by authorized individuals. (022)

- To ensure that the NRC automated information security program complies with the requirements of the Federal Information Security Management Act (FISMA), the Office of Management and Budget (OMB) policy guidance, and related policies, procedures, standards, and guidelines, including information security standards and guidelines for national security systems issued in accordance with law and as directed by the President. (023)

- To ensure that the NRC automated information security program integrates information security management processes with agency strategic and operational planning processes. (024)

- To ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control. (025)

- To ensure the secure interoperability and integration of NRC information systems, which shall be achieved through an adherence to the NRC enterprise architecture (EA) maintained by the Office of the Chief Information Officer (OCIO). (026)

Organizational Responsibilities and Delegations of Authority
(12.5-03)

Executive Director for Operations (EDO)
(031)

- Ensures that information collected or maintained by or on behalf of the agency, and information systems used or operated by the agency, provide automated information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, or destruction. (a)

- Ensures agency compliance with the requirements imposed on the agency by the FISMA and related policies, procedures, standards, and guidelines, including automated information security standards and guidelines for national security systems issued in accordance with law and as directed by the President. (b)

- Ensures that automated information security management processes are integrated with agency strategic and operational planning processes. (c)

- Ensures that senior agency officials provide automated information security protections for the information and information systems that support the operations and assets under their control. (d)

- Delegates to the agency Chief Information Officer (CIO) the authority to ensure compliance with the requirements imposed on the agency by the FISMA and related policies, procedures, standards, and guidelines. (e)

Organizational Responsibilities and Delegations of Authority
(12.5-03) (continued)

Executive Director for Operations (EDO)
(031) (continued)

- Ensures that the agency has trained personnel sufficient to assist the agency in complying with FISMA and related policies, procedures, standards, and guidelines. (f)

- Ensures that the agency CIO, in coordination with other senior agency officials, reports annually on the effectiveness of the agency automated information security program, including progress of remedial actions. (g)

Office of the Inspector General
(032)

Investigates, audits, and takes other action in accordance with the Inspector General Act to detect, prevent, and investigate wrongdoing in connection with NRC automated information systems (AISs).

Chief Information Officer (CIO)
(033)

- As delegated by the agency head, develops and maintains the agencywide automated information security program. (a)

- Designates a senior agency information security officer to carry out the CIO's responsibilities for developing and maintaining the agencywide automated information security program. (b)

- Develops and maintains risk-based information security policies, procedures, System Development Life Cycle Management Methodology, and control techniques that

Organizational Responsibilities and Delegations of Authority
(12.5-03) (continued)

Chief Information Officer (CIO)
(033) (continued)

cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each NRC information system. (c)

Director, Office of Nuclear Security and Incident Response
(034)

Manages NRC information security programs that specifically deal with the classification, declassification, and handling of classified, Safeguards, and sensitive information.

Office Directors and Regional Administrators
(035)

- Ensure that automated information security protections are provided for the information and information systems that support the operations and assets under their control. (a)

- Determine the levels of automated information security appropriate to protect such information and information systems in accordance with the FISMA and related policies, procedures, standards, and guidelines, including automated information security standards and guidelines for national security systems. (b)

Organizational Responsibilities and Delegations of Authority
(12.5-03) (continued)

Associate Director for Training and Development, Office of Human Resources (HR)
(036)

- Provides assistance in the development and delivery of appropriate information security awareness and training programs for NRC personnel. (a)

- Provides other information security related training as requested. (b)

- Ensures that an information security briefing is included in the initial orientation for new employees. (c)

- Ensures that employees receive periodic computer security refresher training, including awareness, basics, and literacy instruction. (d)

- Maintains records concerning computer security training provided to NRC employees. (e)

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)
(037)

- Ensures that appropriate support facilities are provided for NRC information systems, including participation in facility planning, installation, and operations and maintenance. (a)

- Coordinates, reviews, and approves, in conjunction with OCIO, physical security proposals and plans for IT support

Organizational Responsibilities and Delegations of Authority
(12.5-03) (continued)

Director, Division of Facilities and Security (DFS), Office of Administration (ADM)
(037) (continued)

facilities originated by NRC organizations, licensees, and contractors. (b)

- Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC personnel security program, including granting access authorization or similar access approval to NRC AISs. (c)

Director, Division of Contracts (DC), ADM
(038)

Ensures that Federal and NRC requirements for information protection, system availability, and continuity of operations, as documented in Volume 12 of the NRC Management Directives System, are included in solicitations and contracts for the design, development, acquisition, or operation and maintenance of information systems.

Applicability
(12.5-04)

This directive and handbook apply to all NRC employees who process, store, or produce classified, SGI, sensitive unclassified, or unclassified information using AISs or IT facilities that are under the security jurisdiction of the NRC.

Handbook
(12.5-05)

Handbook 12.5 contains procedures and guidance to facilitate implementation of the NRC automated information security program. The handbook includes guidance regarding administrative, technical, and physical security measures appropriate for the protection of NRC IT facilities, systems, and classified, SGI, or sensitive unclassified information processed, stored, or transmitted using an NRC IT system. The Federal Information Security Management Act directs the Department of Commerce, National Institute of Standards and Technology (NIST), to prescribe standards and guidelines pertaining to automated information security systems. These standards and guidelines are mandatory. The NRC shall comply with the NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, IT risk assessments, and IT contingency plans), and other applicable NIST automated information security guidance for IT security processes, procedures, and testing.

Exceptions
(12.5-06)

Exceptions to or deviations from this directive and handbook may be granted by the CIO, except for those areas in which the responsibility or authority is vested solely with the Commission, the Executive Director for Operations, or ADM and is not delegable, or for matters specifically required by law, Executive order, or directive to be referred to other management officials. For national security systems, nothing in the directive and handbook shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems. Nothing in this directive or handbook shall supersede any requirement made by or under the Atomic Energy

Exceptions
(12.5-06) (continued)

Act of 1954. Restricted data or formerly restricted data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954.

References
(12.5-07)

Department of Commerce

National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS). See Appendix F to Handbook 12.5 for the complete list of FIPS Publications referenced herein. Copies of FIPS Publications are available at the NIST Website http://csrc.nist.gov.

National Institute of Standards and Technology (NIST), Special Publications. See Appendix F to Handbook 12.5 for the complete list of Special Publications referenced herein. Copies of Special Publications are available at the NIST Website http://csrc.nist.gov.

"U.S. Department of Commerce Abbreviated Certification Methodology Guidelines for Sensitive and Classified Information Technology Systems," December 1, 1992.

Department of Defense

Department of Defense Directive 8500.1, "Information Assurance", October 24, 2002.

Department of Defense Directive 8500.2,"Information Assurance Implementation", February 6, 2003.

National Industrial Security Program Operating Manual (NISPOM), U.S. Department of Defense, October 1, 1994.

References
(12.5-07) (continued)

Director of Central Intelligence Directives

Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information Within Information Systems", June 5, 1999.

Nuclear Regulatory Commission

Division of Contracts and Property Management (DCPM) Instruction 94-3, Revision 2, "Incorporation of Security Requirements for Information Technology (IT) Services," October 12, 2000.

"Security" (NRCAR 2052.204-70).

NRC Management Directives

2.2, "Capital Planning and Investment Control."

2.5, "System Development Life Cycle Management Methodology (SDLCMM)."

2.7, "Personal Use of Information Technology."

4.3, "Financial Management Systems."

11.7, "NRC Procedures for Placement and Monitoring of Work With the U.S. Department of Energy (DOE)."

12.2, "NRC Classified Information Security Program."

12.3, "NRC Personnel Security Program."

12.4, "NRC Telecommunications Systems Security Program."

References
(12.5-07) (continued)

12.6, "NRC Sensitive Unclassified Information Security Program."

13.1, "Property Management."

NRC Management Directives System Volume 12, "Security," which contains a Glossary of terms applicable to the volume.

"The Nuclear Regulatory Commission's Procedures for Use of the U.S. Government Bankcard," Office of Administration, October 1998.

NUREG/BR-0167, "Software Quality Assurance Program and Guidelines," February 1993.

Office of Management and Budget

Circular A-123, "Management Accountability and Controls," June 21, 1995.

Circular A-127, "Financial Management Systems," July 23, 1993.

Circular A-130, Transmittal Memorandum No. 4, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems," November 28, 2000.

United States Code

Computer Fraud and Abuse Act of 1986, as amended (Pub. L. 99-474, 18 U.S.C. 1001 note).

Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512 et seq. and 31 U.S.C. Chapter 11).

References
(12.5-07) (continued)

Federal Information Security Management Act of 2002 (Pub. L. 107-347, 116 Stat. 2899).

Inspector General Act, 5 U.S.C. App 3.

NRC Automated Information Security Program

Handbook 12.5

Contents

Part 1

Part 2

Contents (continued)

Part 3

Part 4

Tables

Appendices

Part 1
The NRC Automated Information Security Program

1.1 Introduction

The Clinger-Cohen Act calls for the Office of Management and Budget (OMB) to issue clear and concise direction related to Federal information security policies, processes, and practices. Protecting the information and systems that the Federal Government depends on is important as agencies increasingly rely on new technology. Federal computer systems are vulnerable to many threats that can inflict various types of damage to our automated information systems (AISs). The threats include computer fraud and theft, employee sabotage, malicious hackers, industrial espionage, foreign government espionage, and malicious software code (such as viruses and worms). Damage to Federal AISs is most often focused on the activities of external Government entities, but Federal AISs must also be made secure to protect against "insider" threats posed by disgruntled employees or other authorized users of agency systems who may be attempting to intentionally disrupt computer operations, gain unauthorized access to network resources or services, or perform other related unauthorized activities.

OMB has issued a set of principles to support more effective implementation of agency automated information security programs and related critical information infrastructure protection initiatives. In terms of Federal information systems, critical infrastructure protection starts with an effort to prioritize key systems (e.g., those that are most critical or essential to agency operations). The OMB principles guide NRC efforts to incorporate security and privacy into the agency's AISs:

- Effective security is an essential element of all NRC AISs.

- Effective privacy protections are essential to all NRC AISs, especially those that contain substantial amounts of personally identifiable information. The use of new information technologies should sustain, and not erode, the privacy protections provided in all statutes and policies relating to the collection, use, and disclosure of personal information.

- The increase in efficiency and effectiveness that flows from the use of interconnected computers and networks has been accompanied by increased risks. The protection of NRC AIS resources must be commensurate with the risk of harm resulting from any misuse or unauthorized access to such systems and the information flowing through them.

- Security risks and incidents must be managed in a way that complements and does not unnecessarily impede agency business operations. By understanding risks and implementing an appropriate level of cost-effective controls, NRC can significantly reduce risk and potential loss.

- A strategy to manage security is essential. Such a strategy should be based on an ongoing cycle of risk management and shall be described in system security plans. It should identify significant risks, clearly establish responsibility for reducing them, and ensure that risk management remains effective over time.

- NRC must understand the risk to systems under NRC control and determine the acceptable level of risk, ensure that adequate security is maintained to support and assist the programs under NRC control, and ensure that security controls support program needs and appropriately accommodate operational necessities. In addition, security measures shall support the agency enterprise architecture (EA).

Securing the integrity and availability of NRC AISs requires the coordinated efforts of everyone involved: users, system administrators, system developers, and management. This coordination must ensure that potential vulnerabilities are identified and addressed and that immediate action is taken whenever there is an event that might be indicative of a potential attack.

The policy basis in Management Directive (MD) 12.5 for the NRC automated information security program defines the information assets that must be protected, assigns responsibilities for protecting those assets, and identifies the objectives for the NRC automated information security program. Handbook 12.5 expands on the policies of MD 12.5 to provide guidelines and procedures for achieving the security objectives of Directive 12.5. Specifically, the NRC automated information security program is designed to ensure that—

- Access to information assets (i.e., data and systems) is restricted to only those individuals who are authorized access (confidentiality);

- Information contained in or processed by an NRC AIS is not deleted or changed (intentionally or unintentionally) without authorization (integrity); and

- NRC AISs are available to their users to accomplish the agency's mission (availability).

The automated information security policy defined in MD 12.5 and the guidelines and procedures contained in this handbook apply to all NRC AISs. All NRC employees (or other personnel who have been provided authorized NRC AIS user accounts) who use, maintain, or develop an NRC AIS or who process NRC data through an AIS that is owned or sponsored by the NRC are subject to the requirements of MD 12.5.

Security controls for classified national security AISs shall be implemented in accordance with appropriate national security directives. Contact the OCIO Computer Security Staff for assistance with the national security directives.

1.2 Information Requiring Protection

NRC receives, processes, stores, and disseminates information in the performance of its mission objectives. Much of this information is considered sensitive because of the potential harm that might result to the security of the country, to NRC business partners, or to individuals if the information is not protected. Federal law and NRC policy require that sensitive information be afforded appropriate levels of protection on the basis of the level or magnitude of harm that might result from unauthorized access to such information were it to be compromised.

Sensitive data used within NRC operations fall within three categories: classified (data that relate to protection of national security - National Security Information, Restricted Data, Formerly Restricted Data); sensitive unclassified (all sensitive data that are not classified); and Safeguards Information (data requiring protection as specified in the Atomic Energy Act). NRC has determined that requirements for protecting SGI data will be equivalent to those requirements for classified data at the Confidential level. Requirements for protecting sensitive unclassified Government data are established by the Government owner of that data (i.e., the Government individual who is held accountable if the data are released without proper authorization or are otherwise compromised). When data fall within multiple protection categories, the requirements for the higher category shall be used.

The guidelines contained in this handbook address all types of information used by the NRC. Selection of procedures appropriate for a particular system requires analysis of the type of data that will be processed and/or stored and the associated protection requirements. For additional examples of categories of sensitive information, see NRC Management Directive 12.6, "NRC Sensitive Unclassified Information Security Program."

1.3 Defense in Depth

The security guidelines, processes, and procedures identified in this handbook, when appropriately implemented, will establish a security environment that relies on "defense in depth." Under the defense-in-depth approach, security controls and countermeasures are established so that the failure of a single control will not compromise the information system. The controls may be related to personnel issues, such as background screening of all individuals; administrative, such as sign-in logs and audit trail reviews; physical concerns, such as guards or locked doors; or technical, such as passwords. For example, at NRC headquarters and the regional offices, physical access to NRC workplaces is controlled, and a password is required to access the local-area network (LAN) through a workstation.

When using this handbook as a guide to establish or administer a security environment for an information system, defense in depth should be a primary goal. Specifically, multiple layers of security protection mechanisms should be put in place to mitigate the concurrent failure of more than one independent security control.

1.4 Authorities

The documents listed under References (12.5-07) in the directive provide the legal foundation for the NRC AIS security program.

1.5 Additional Guidance

The Federal Information Security Management Act (FISMA) directs the Department of Commerce, National Institute of Standards and Technology (NIST), to prescribe standards and guidelines pertaining to automated information security systems. These NIST standards and guidelines are mandatory. The NRC shall comply with the NIST security guidance to include guidance related to the preparation of security

documentation, (such as security plans, IT risk assessments, and IT contingency plans), and other applicable NIST automated information security guidance for IT security processes, procedures, and testing. The NIST guidance is available at the NIST computer security Web site at http://csrc.nist.gov and can also be obtained by contacting the NRC OCIO Computer Security Staff. NIST issues such guidance in the form of Federal Information Processing Standards (FIPS) and Special Publications, which were considered in the preparation of the procedures and guidelines contained in this handbook (see Appendix F).

Additional network security technical guidance specific to the NRC IT (information technology) network operational environment is contained on the IT customer support internal Web site at http://csb.nrc.gov that is maintained by OCIO. Because of the dynamic nature of network operations, the network security technical guidelines, processes, and procedures are subject to frequent changes. The most current network security operational technical guidance shall be maintained on the IT customer support internal Web site.

Part 2
Roles and Responsibilities

At the NRC, maintaining an effective automated information security environment is the responsibility of everyone who uses an NRC information system or who processes NRC data using an NRC information system. Responsibilities include compliance with established security policies and procedures, as well as performance of specific roles within the NRC automated information security program. The roles and responsibilities described in Section (12.5-03) of Directive 12.5 also include the following:

2.1 Chief Information Officer (CIO)

- Reports annually to the agency head, in coordination with other senior agency officials, on the effectiveness of the NRC automated information security program, including the progress of remedial actions. (a)

- Maintains a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency. (b)

- Establishes and maintains the procedures for detecting, reporting, and responding to automated information security incidents and for mitigating risks associated with such incidents before substantial damage is done. (c)

- Ensures that plans and procedures are established to ensure continuity of operations for information systems that support the operations and assets of NRC. (d)

- Ensures, through coordination with the Security Branch, Division of Facilities and Security (DFS), Office of Administration (ADM), that individuals designated to participate in the management, design, planning, operation, or maintenance of NRC information systems and/or having access to sensitive data are properly screened and eligible for access to this information or these systems in accordance with the personnel security requirements contained in MD 12.3, “NRC Personnel Security Program.” (e)

- Ensures, in conjunction with DFS, the adequacy of personnel security requirements included in contracts, interagency agreements, and designs for NRC information systems. (f)

- Appoints the Observer and the Alternate Observer for the Subcommittee for Information Systems Security (SISS) of the Committee for National Security Systems (CNSS). (g)

- Reviews and approves security certifications and accreditations for NRC information systems, including risk analysis results, security plans, contingency plans, and security-related elements of investment justifications submitted in accordance with NRC Capital Planning and Investment Control (CPIC). (h)

- Approves the designation of NRC information technology systems as Major Applications (MAs), General Support Systems (GSSs), or other categorization. (i)

- Serves as the Designated Accrediting Authority (DAA) for all MAs and GSSs, and also for all classified systems, Safeguards Information (SGI) systems, and sensitive systems. (The CIO may delegate the DAA responsibilities to other NRC senior agency officials, as required.) (j)

- Establishes the procedures for interconnection of any information technology (IT) device or system with the NRC IT infrastructure systems. (k)

- Ensures through coordination with the Office of Human Resources that NRC employees and contractor staff have appropriate initial and refresher, basics and literacy, and role-based computer security training. (l)

- Approves cryptographic hardware and software mechanisms used for the protection of classified information, SGI, or sensitive unclassified information in NRC automated information systems (AISs). (m)

- Develops and maintains an annual inventory of NRC AISs (including major national security systems) operated by or under the control of the agency. The identification of all major information systems in the inventory must include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency.(n)

- Monitors compliance with this directive. (o)

- Prepares and submits reports, as required, regarding the status of the NRC automated information security program to the Office of Management and Budget (OMB) and other entities external to the NRC. (p)

- Provides guidance and assistance to other NRC organizations regarding implementation of the requirements of this directive and associated handbook. (q)

2.2 Regional Administrators and Office Directors

- Periodically test and evaluate automated information security controls and techniques to ensure they are effectively implemented. (a)

- Identify all AISs for which their office is the system sponsor or funding organization. (b)

- Identify those information systems that are GSSs or MAs as defined in OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources,” and obtain concurrence from the CIO for system categorization. (c)

- Identify those information systems processing classified information, SGI, or sensitive information that are not MAs or GSSs. (d)

- Ensure that information systems sponsored by their office are included with the OCIO maintained master inventory of agency information systems. (e)

- Ensure that all information systems sponsored by their office are covered by a security plan, and an IT contingency plan, and that those designated as GSSs, MAs, or that process or store classified information, SGI, or sensitive information have individual security plans. (f)

- Working in conjunction with OCIO, assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems under their control and implement policies, procedures, and security controls to cost- effectively reduce risk to an acceptable level. (g)

- Ensure the preparation and periodic updates of required system security documentation are completed in order to facilitate the design, implementation,

operation and maintenance, testing, and security certification and accreditation of information systems for which their office is the system sponsor. (h)

- Ensure that information systems sponsored by their office and operated by NRC comply with the requirements of this directive and handbook. (i)

- Ensure that all Federal and NRC automated information security requirements for the protection of classified, SGI, or sensitive unclassified information are provided in Requests for Procurement Actions involving automated systems processing such information. (j)

2.3 System Sponsor/Owner

"System sponsor" is synonymous with the term "system owner" used in the National Institute of Standards and Technology (NIST) SP 800-18, "Guide For Developing Security Plans for Information Technology Systems." A system sponsor is an office director, a regional administrator, or a responsible division director in OCIO for an NRC AIS. The system sponsor is responsible for—

- Ensuring that security requirements and planning are included in life cycle budgets for information systems and included in project screening forms and business cases that are completed in accordance with the CPIC policy (Management Directive [MD] 2.2) guidelines.

- Ensuring that security plans for information systems include a strategy for security risk management. Significant risks should be identified, along with responsibilities and mitigation strategies to reduce the security risks.

- Ensuring that a plan of action and milestones (POA&M) is developed, implemented, and maintained to track the major weaknesses that have been identified for office-sponsored information systems. Each office shall regularly update OCIO on its progress in correcting system weaknesses in order to enable the CIO to provide the agency's quarterly Federal Information Security Management Act (FISMA) update report to OMB.

- Ensuring that required security documentation is prepared and maintained for MAs and GSSs (see Part 3, Table 3-1, of this handbook):

  – Risk Assessment Report

  - System Security Plan
  - Security Test and Evaluation (ST&E) Plan and ST&E Report
  - Contingency Plans for business continuity and disaster recovery, with associated test reports
  - Information System Security Officer (ISSO) Appointment Letter
  - Certification Report
  - Certification Signature
  - Accreditation Signature

- Ensuring that security plans are completed for all office systems that are processing classified information, unclassified Safeguards Information, and sensitive information. (See Part 3, Table 3-1, of this handbook.)

- Ensuring that all office-sponsored IT systems are properly categorized and accurately reflected in the NRC OCIO-maintained master inventory of systems. Each office will work with OCIO to update and revalidate the master inventory of systems on an annual basis. Federal critical information infrastructure protection guidelines require that NRC identify and prioritize its key systems (e.g., those that are most critical or essential to agency operations). Systems sponsors/owners shall support agency efforts to identify and prioritize the agency critical and essential systems, as coordinated by OCIO.

- Ensuring that all IT system security documentation (risk assessments, security plans, contingency plans) comply with the guidance and format specified by the NIST special publication series of guidance documents. (See Appendix F for references.)

- Ensuring that an ISSO is appointed for all MAs, GSSs, classified systems, SGI systems, and sensitive systems as specified in Part 3, Table 3-1, of this handbook. Regional administrators and the Technical Training Center (TTC) shall appoint at least one primary ISSO with responsibility for IT security program oversight in the region. The regional ISSO shall be the primary point of contact in the region for the coordination with OCIO of all IT security program requirements and issues.

- Ensuring that all office-sponsored MAs, GSSs, classified systems, SGI systems, and sensitive systems complete systems security certification and accreditation before being put into operation. Security accreditation (which provides the formal management approval to operate) is also required for any prototype or pilot project before that project is put into operation within the NRC network infrastructure.

- Ensuring that appropriate security features and controls are included with system designs for applications and systems that are available for use by the general public (such as public Web servers and other externally hosted applications) in order to ensure that NRC data and infrastructure systems are adequately protected.

- Ensuring that office procedures for controlling visitors are established and enforced, in order to safeguard sensitive data from disclosure to unauthorized or uncleared personnel.

2.4 Information System Security Officer (ISSO)

An ISSO is the designated representative of a system sponsor for an AIS. The system sponsor shall appoint an ISSO for each AIS for which he or she is responsible, as specified in Part 3, Table 3-1, of this handbook. An ISSO may be responsible for more than one AIS. The ISSO position is a trusted position with special access to and authority for an AIS. Thus, ISSO responsibilities should not be assigned to an individual who has other trusted responsibilities (e.g., a System Administrator should not be assigned ISSO responsibilities). In some cases, however, due to staffing limitations or other constraints, it may be necessary to assign responsibilities of multiple trusted positions to a single individual. In such cases, the increased vulnerability should be noted in the ISSO appointment letter, which will also serve as the system sponsor's acknowledgment and acceptance of the increased risk.

The ISSO shall have a clearance and background investigation appropriate for the highest security level of information processed by the AIS. The ISSO is responsible for implementing the requirements of this handbook and any other system-specific security activities. (For externally hosted applications that have been established via NRC contracts or other agreements, the ISSO shall monitor compliance with the security requirements specified in the contract or agreement.) The ISSO's responsibilities shall include the following:

- Developing (or assisting in the development of) the security rules of behavior specific to the office-sponsored AIS.

- Monitoring compliance with the AIS security rules of behavior and other security controls.

- Ensuring that the AIS certification and accreditation process is completed before systems are put into operation (or if the system undergoes a significant upgrade). The ISSO will coordinate for the system sponsor with OCIO for any assistance required to support system security accreditation (which is the formal management approval to operate the system).

- Ensuring that AIS security program reviews and periodic security testing are completed. The FISMA requires that security program reviews for a system be conducted annually. The ISSO shall assist the system sponsor in the coordination of the accomplishment of these security program reviews and any other related periodic security testing.

- Ensuring that the status of remediation activities is tracked and reported until successfully completed.

- Responding to, investigating, and reporting security incidents.

- Performing periodic reviews of system audit trails. The ISSO shall review audit reports or audit trails periodically, depending on the criticality of the system (or the criticality of the data processed by the system). Federal IT security guidance specifies that appropriate security controls, processes, and procedures should be applied, commensurate with the risks and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the IT system, or the information it processes. For MAs and GSSs, and for systems that are processing sensitive information, auditing controls should be addressed in the individual system security plans on the basis of this risk management process. For other systems that do not process sensitive data, auditing frequency can be established by the system owner, also on the basis of a reasonable assessment of the risk to the system. **[REDACTED]**

2.5 Rules of Behavior for NRC AIS Users

AIS users are any individuals who have been authorized access to or use of an NRC AIS for any reason (e.g., support of an agency mission or developing or maintaining an AIS). For the purposes of this management directive, individuals in the general public who only access the NRC public Web site are not considered users.

Users of an AIS are often the first to encounter an anomaly that may be indicative of an attack or unauthorized actions of a malicious program code. Thus, an AIS user community can serve as a control or countermeasure to identify potential attacks and mitigate the resulting adverse impacts through early recognition, reporting, and compliance with NRC security measures.

Users of an NRC AIS must be authorized before being granted access to an NRC AIS. The assets to which the user is authorized access are to be used in support of NRC mission objectives. These assets may not be used for any non-Government activity, except in accordance with the NRC limited personal use policy (see MD 2.7, "Personal Use of Information Technology").

The NRC user rules of behavior are to be followed by all users of the NRC local-area network/wide-area network (LAN/WAN) system and all users of any NRC AIS. Users shall be held accountable for their actions on the NRC LAN/WAN system. If an employee violates NRC policy regarding the rules of behavior for use of any NRC AIS and the NRC LAN/WAN system, they may be subject to disciplinary action at the discretion of NRC management.

Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, termination, or prosecution under applicable Federal law consistent with the nature and the severity of the violation. The Office of the Inspector General (OIG) is charged with investigation of allegations of misconduct related to misuse of the systems, and all allegations of violations shall be reported to the OIG.

Users shall take appropriate precautions to protect the assets (hardware, software, data) provided for their use or to which they have been granted access (e.g., workstations, microcomputers, local-area networks (LANs), and associated data).

An AIS user—

- Shall have no expectation of privacy for information processed by, stored within, or transmitted through the NRC computing environment. Others with access to NRC resources may view such information accidentally or intentionally as they also use, manage, or maintain those resources.

- Shall protect sensitive unclassified information in his or her possession from unauthorized access, disclosure, modification, misuse, damage, or theft.

- Shall not knowingly introduce any malicious code into the computing environment nor attempt to bypass or circumvent security features.

- Shall take appropriate precautions to avoid malicious software when introducing files into the NRC computing environment through physical media (e.g., diskette) or communications (e.g., e-mail attachments, downloading from the Internet).

- Shall not knowingly access or download material (e.g., pornography) that could create a "hostile work environment."

- Shall not install any computer program into the NRC computing environment if there is any question that the computer program may not be properly licensed.

- Shall protect all user IDs and associated passwords issued to him or her and will not disclose the password to anyone. **[REDACTED]**

- Shall immediately notify the NRC Customer Support Center of any events that may be perceived to be a potential security incident. The user will also support investigation and resolution of the reported incident. For NRC employees assigned outside of headquarters, the regional office IT staff shall also be contacted.

- Shall attend initial indoctrination and annually complete the computer security awareness refresher training and implement security instructions as directed by NRC security and supervisory personnel.

- Shall comply with all policies and procedures related to the security of NRC LAN/WAN system data and NRC AISs. Classified information and SGI shall not be processed on the agency unclassified LAN. **[REDACTED]**

- Shall report security-relevant events to the OIG and to supervisors, or to the personnel responsible for the security of the NRC LAN/WAN or NRC AISs. These events include security infractions by coworkers, attempted access by unauthorized personnel, violations of procedures, disclosure of sensitive information, loss of availability of NRC LAN/WAN system resources, destruction of data, or detection of erroneous information or unexplained system activity.

- Shall provide immediate notification to supervisory personnel when a decision is made to retire, resign, transfer, or otherwise change the basis for which access to NRC AIS or the NRC LAN/WAN system has been granted.

[REDACTED]

- Shall safeguard passwords and user account numbers from other personnel by not disclosing them either verbally or in written form. Do not at any time record a password in writing.

- Upon observation of unknown personnel in areas in which sensitive NRC LAN/WAN system data are used or stored, shall challenge them immediately to ensure that their access is authorized.

- Users of NRC AIS property and supplies, including portable computing devices, shall comply with the requirements of MD 13.1, "Property Management," to ensure that NRC AIS and portable computing devices are protected against loss, theft, or destruction. Because of their portability, security risks to sensitive data on laptop computers, personal digital assistants (PDAs), cell phones, and other portable computing devices are greater than for stationary systems.

- Shall ensure that essential user data residing on the individual workstation or laptop are backed up **[REDACTED]** and that media containing backup data are relocated to an area physically removed from the workstation.

- Shall scan all files received from external sources for malicious code (viruses) before introducing them to networked NRC systems.

- When leaving a workstation unattended, manually log off the system to prevent access to NRC LAN/WAN system data, or lock the workstation by selecting the appropriate action after pressing the Ctrl-Alt-Delete keys on the keyboard.

- Shall position their workstation monitors to preclude casual viewing of sensitive data during processing.

- Shall ensure that the screen-saver password protection option is selected **[REDACTED]**.

- Shall power-off individual workstations at the end of each duty day. (Staff at the regional offices or remote locations may receive guidance from the regional IT staff to leave the workstations powered on in order to support maintenance activities.)

- Shall ensure that user printers are placed in an area in which access can be controlled to ensure that only authorized personnel access sensitive hard copy output. Classified information and SGI shall not be sent through an unclassified LAN server to a printer.

- Shall never copy any classified information or SGI on a copy machine that is connected to the NRC unclassified network.

- Shall never connect to other networks or hosts (via dial-up modems or network connections) without prior permission of NRC IT security personnel.

- Shall seek OCIO approval before using personal hardware and software on NRC systems. Any installation of software on NRC systems shall be approved by OCIO. Installation of software on NRC systems in the regions shall be coordinated with the regional IT staff.

- Shall obtain OCIO approval and adhere to software copyright laws before installing software on NRC systems, including standalone personal computers (PCs) and laptops. Comply with software copyright license laws and policies that prohibit unauthorized use or copying of commercial software.

- Shall never attempt to circumvent or defeat security safeguards and countermeasures implemented for the protection of NRC LAN/WAN system data or NRC processing systems.

- Shall comply with NRC processes and procedures for secure dial-in access to NRC AISs. Direct dial-in access to NRC desktops and LAN/WAN system servers is normally not permitted. If such access is required because of special business needs (e.g., remote troubleshooting by vendors or remote access to resident site computers), this access may be approved on a case-by-case basis by the Director of the Information Technology Infrastructure Division, OCIO. It is understood that dial-in access would pose additional security risks but may become necessary for certain job functions.

- Shall ensure that only NRC-authorized Internet connections are being used. All proposed connections shall be authorized and approved by OCIO.

- Shall comply with NRC policies related to the personal use of Government IT. MD 2.7 specifies that it is NRC policy to permit employees limited use of agency IT for personal needs if the use does not interfere with official business and involves

minimal or no additional expense to the NRC. MD 2.7 defines the acceptable conditions for NRC employees' personal use of IT.

2.6 Additional Guidance Pertaining to the Secure Use of NRC Automated Information Systems and the Network Infrastructure

NRC provides its personnel with an infrastructure that can provide connectivity to a variety of applications. The following are procedures for ensuring that use of the NRC infrastructure is accomplished securely, with reduced potential for a security failure. The regional offices and the TTC are authorized to make minor variations to these processes and procedures to accommodate the requirements of the local environment. Variations shall be submitted to OCIO (ITID or the Senior Information Technology Security Officer [SITSO]) for review and approval.

2.6.1 Requesting a User Account

A user identifier (user ID) and associated passwords are required to access the LAN/WAN. User IDs are issued to specific individuals so that privileges granted and actions taken can be associated with these individuals. Sharing of user IDs and passwords is not permitted. At headquarters, requests for user IDs must be submitted to the Customer Support Center (CSC) by the users's office director or Office IT Coordinator. Requests for regional office/TTC user IDs must be submitted to the local Division of Resource Management and Administration or Information Resources Branch.

For NRC employees requiring access to the NRC LAN, the office director or the Office IT Coordinator must verify that NRC employees for whom they request a user ID have been granted **[REDACTED]** an appropriate security clearance.

For NRC contractors requiring access to the NRC LAN, after the appropriate verification and checks are made, the Division of Facilities and Security (DFS) provides documentation to NRC Project Officers (POs) that contractor employees working under their contract have been issued **[REDACTED]** an appropriate access authorization.

2.6.2 Processing Classified Data

Information designated as "National Security Information," "Restricted Data," or "Formerly Restricted Data" is classified information. With the exception of those systems located in an NRC Sensitive Compartmented Information Facility (SCIF) or another facility approved by DFS, this information may only be processed or produced on an AIS that is a standalone unit not physically or logically connected to any unclassified network, and that has a removable storage medium used for both programs and data (or the complete system is a mobile device [laptop] that can be secured). Classified information may only be stored on a removable medium and that medium must be secured in an approved security container when not in use. Classified information may only be transmitted using a system that is considered protected. Examples of protected systems can be found in Part II of Handbook 12.4. Except for a minimal number of special cases involving standalone computers and laptops approved by OCIO and DFS, classified processing shall be conducted only within NRC facilities or spaces that have been specifically approved for classified processing in accordance with policy guidance specified by the Committee for National Security Systems (CNSS), the National Security Agency, the Department of Defense, and MD 12.1, "NRC Facility Security Program." Contact OCIO computer security staff for any assistance with security requirements for classified systems.

The following rules are enforced while processing classified information (see also MD 12.2, "NRC Classified Information Security Program").

- The AIS must not contain or use a permanent fixed disk for any data storage (intermediate results, final results, overflow, or backup) unless the AIS can be provided with adequate security for the open storage of such information and provision is made in the plan for sanitization or destruction of the hard drive if the AIS is to be removed from the protected area.

- The AIS, with the exception of those systems located in an NRC SCIF or another DFS-approved facility, must be physically disconnected from unclassified LANs, modems, and shared printers.

- The AIS must be protected in a manner that prevents unauthorized personnel from having visual access to the information being processed. This protection may be accomplished by screens, hoods, or positioning the equipment (monitors or printers) so that it faces away from doorways, windows, or open areas.

- The AIS must never be left unattended when processing classified data.

- All media (e.g., diskettes, tapes, printouts, ribbons) must be properly labeled, stored, sanitized, and disposed of as specified in MD 12.2.

- All users of an AIS that has multiple users and that is used intermittently for classified processing must be recorded on a manual audit log. Each user must be individually identified by a unique user ID and password. (Sharing of user IDs and passwords is not authorized.) Logging for systems that are online each day, located in protected facilities such as a SCIF, and that are in existence expressly for classified processing is not required. These logs must provide the following information:

  – Date and time of day classified processing began.

  – Name of the user of the classified AIS.

  – Date and time of day classified processing was completed. **[REDACTED]**

  – An entry must be made indicating that the user verified that the previous user sanitized the AIS checking log entries. If the AIS was not sanitized, the user shall sanitize the AIS and will inform the previous user of the omission. If the previous user is not available, the user will notify the ISSO.

  – An entry must be made indicating the date and time of day the classified AIS was sanitized.

Special approaches should be used to delete classified data from electronic storage media. These approaches may include destruction of the physical media, obliteration of the sensitive data through the use of an approved software product **[REDACTED]**, or erasure of all data through degaussing. Questions regarding the appropriate method for eliminating classified data from a storage medium should be referred to the Computer Security Staff in OCIO.

2.6.3 Processing Safeguards Information (SGI)

Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material or security measures for the physical protection and location of certain plant

equipment vital to the safety of production or utilization facilities must be protected pursuant to Section 147 of the AEA. This information is categorized as Safeguards Information or SGI.

Information designated as SGI requires protective measures similar to those used for classified data at the Confidential level. With the exception of those systems located in a facility or space approved by DFS, this information may be stored, processed, or produced only on an AIS that is a standalone unit that is not physically or logically connected to the NRC unclassified network and has a removable storage medium used for both programs and data (or the complete system is a mobile device that can be secured). For standalone computers with a removable drive, the operating system and all applications, and data used for SGI processing shall all reside on the same removable drive. SGI may be stored only on a medium that is secured in an approved security container when not in use. SGI may only be transmitted using encrypted transmission techniques or a system that is considered protected. Examples of protected systems can be found in Part II(F) of Handbook 12.4.

The following additional rules are enforced while processing SGI (see MD 12.6, “NRC Sensitive Unclassified Information Security Program”):

- The AIS must not use a fixed hard disk for any data storage (intermediate results, final results, overflow, or backup) unless the AIS can be provided with adequate security for the open storage of such information and provision is made in the plan for sanitization or destruction of the hard drive if the AIS is to be removed from the protected area.

- The AIS, with the exception of those systems located in an NRC SCIF or another DFS-approved facility, must be physically disconnected from LANs, modems, and shared printers.

- The AIS must be protected in a manner that prevents unauthorized personnel from having visual access to the information being processed. This protection may be accomplished by screens, hoods, or positioning the equipment (monitors or printers) so that it faces away from doorways, windows, or open areas.

- The AIS must never be left unattended when processing SGI.

- All media (e.g., diskettes, tapes, printouts) must be properly marked and stored in DFS-approved storage containers when not in use.

- Disks, diskettes, ribbons, and printouts must be disposed of in accordance with MD 12.6.

Special approaches should be used to delete SGI data from electronic storage media. These approaches may include destruction of the physical media, obliteration of the sensitive data through the use of an approved software product **[REDACTED]**, or erasure of all data through degaussing. Questions regarding the appropriate method for eliminating classified data from a storage medium should be referred to the OCIO Computer Security Staff.

2.6.4 Remote Access

Remote dial-in access to the NRC LAN/WAN is permitted with prior authorization. A copy of the NRC Remote Access Agreement is posted on the NRC internal Web site. All users requesting remote access capability must sign and return the agreement to the CSC, or the appropriate regional office Division of Resource Management and Administration, IT branch chief (or regional ISSO).

[REDACTED]

Users should install virus-checking software on all mobile or home computers used to access the NRC LAN/WAN. Viruses and other malicious code can spread from a mobile or home computer and damage or disrupt the NRC LAN/WAN. NRC will provide a copy of virus-checking software for installation on a home or mobile computer. Once such software is installed, it is the user's responsibility to download updates **[REDACTED]** so that the virus protection remains current. Contact the CSC for assistance and guidance on how to perform updates to anti-virus software and virus signature files.

2.6.5 Use of the Internet

NRC staff may use the NRC LAN/WAN to access the Internet. This access may be for official business or personal business in accordance with the NRC minimum personal use policy in MD 2.7. When using the Internet, users shall practice "safe surfing." Specifically, users shall—

- Avoid accessing pornographic or other sites that provide content that is incompatible with the NRC work environment. **[REDACTED]** These sites offer content relating to criminal skills, gambling, hate speech, and pornography or other sexually oriented

material. **[REDACTED]** It is the user's responsibility to avoid such sites and to immediately terminate access to such sites that are reached unintentionally.

- Avoid downloading unknown browser "plugins." Access to the Internet is generally achieved through the use of a software "browser" such as Netscape or Internet Explorer. The capabilities of these browsers can be extended by adding program code to the browser through the use of a "plugin." While many plugins perform useful functions, there are plugins that are actually malicious code that may damage other computer software or the data files stored on the computer. Thus, if a Web site requests that a plugin be downloaded, do not allow the download unless the need for the plugin was anticipated, the provider is known, and a certificate is presented verifying the authenticity of the plugin.

- Avoid acceptance of "cookies." Cookies are small files that a Web site may place on a computer that accesses the site. Cookies can capture and retain personal information about the user or the machine being used. Also, cookies may be used to "trigger" malicious code that can damage files or result in display of disruptive advertising. To minimize the adverse impact of cookies, browsers should be set to block all "third-party" cookies, except cookies that expire within the current session (nonpersistent cookies), and prompt to request user direction regarding all other persistent cookies. The user can then elect to accept those cookies necessary to provide the desired functionality from the Web site accessed.

- Consider installation of a personal firewall on user-owned PC systems that are used at home to access both NRC systems, and also to access other systems on the Internet. When accessing the Internet, a two-way connection is established (i.e., while one is accessing the Internet, others may use the same connection to gain access to the computer). NRC uses a firewall at the LAN/WAN interface with the Internet to avoid such unauthorized access. As a computer security "best practice," users may consider installing a similar firewall (personal firewall) on mobile or home machines they use to access NRC systems and the Internet at the same time.

2.6.6 E-mail Attachments

E-mail has become an easy method for exchanging data files with individuals both internally and externally. These files are generally attached to an e-mail as an "attachment." E-mail attachments, however, have also become popular methods for distributing a computer virus or other malicious program. Modern firewalls often block or quarantine attachments where a virus is detected. The firewall software, however,

cannot detect every instance of malicious code. Thus, opening of any attachment should be approached with caution. Attachments should not be opened if—

- There is no subject
- The sender is unknown or is a “bulk mailing”
- The subject promises “something for nothing”
- The message text is out of character for the sender

2.6.7 Introduction of New Technologies to the NRC Network Infrastructure

New technologies or approaches for using computers and communications are continually being developed. While such new technologies such as wireless technologies, or new uses for existing technologies, can enhance productivity, they also have vulnerabilities that must be considered. Every technology that links to the LAN/WAN might have the capability of allowing unauthorized individuals to have access as well. Thus, no new technologies shall be connected to the NRC LAN/WAN infrastructure without a security risk assessment or without the approval of the CIO, who is the Designated Accrediting Authority (DAA) for the NRC LAN/WAN infrastructure. The security plan and other security documentation for the LAN/WAN shall be updated and the LAN/WAN shall be recertified and reaccredited for each new technology that has been formally authorized for incorporation into the LAN/WAN.

2.6.8 Connections to the NRC Network Infrastructure

NIST Special Publication 800-47, “Security Guide for Interconnecting Information Technology Systems,” provides guidance for planning, establishing, maintaining, and terminating interconnections between IT systems that are owned and operated by different organizations. NRC shall comply with the NIST guidance for all proposed connections to the NRC network infrastructure. The DAA for the NRC LAN/WAN is the CIO, who provides approval to operate on the basis of a risk-based assessment of a reasonably firm configuration for the LAN/WAN.

The issue with any external connection made to the NRC network infrastructure is that it may impact the current accreditation status, current approved security configuration, and the current overall risk posture. Federal guidance requires that written management

authorization be obtained before establishing a connection between the NRC IT infrastructure to another system that is not NRC controlled.

The approved security accreditation documentation package for the NRC LAN/WAN would need to be updated (or supplemented) to reflect the new information related to the connection. The update to the existing LAN/WAN security documentation package is accomplished primarily by the sponsor of the new proposed connection, who will work with OCIO to provide the information and documentation needed for the update. This mini-documentation package would contain just the updates that account for the changes that are introduced with the new proposed connection. The sponsor would submit a memorandum to the OCIO that specifically requests that NRC OCIO accomplish a certification of the proposed connection, and provide an approval (accreditation) for the connection. The CIO approval results in the existing LAN/WAN security accreditation package being supplemented (updated) to reflect this new approved connection. The NRC CIO will then issue a signed memorandum back to the sponsor of the new connection formally noting that the connection is approved and accredited. Connections to other Government-owned systems also may require the establishment of a Memorandum of Understanding/Memorandum of Agreement (MOU/MOA). Additional details are provided in the NIST guidance.

Data communication connections via modems must be limited and tightly controlled to protect agency networks and data. Poorly implemented or unauthorized modems can create holes in the security protecting the NRC computer network and leave our systems open to both active and passive attacks. Active attacks include attackers using auto-dialing machines to detect and dial into modems to gain unauthorized access. Passive attacks include viruses or worms that are unintentionally downloaded via the modem. Normally viruses and worms are recognized by the NRC network security systems and are prevented from causing harm. The NRC CIO is the DAA for the NRC network infrastructure. Any proposed changes or modifications to any part of the infrastructure (such as the introduction of desktop modems) must be assessed for risk, and the DAA must give specific approval. Guidelines for the authorized use of modems on NRC networks are posted on the NRC internal Web site under IT Customer Support.

2.6.9 Guidelines for the Use of Vulnerability-Scanning and Password-Checking Software

These guidelines apply to the proposed use of any software that is specifically designed to test or scan NRC unclassified information systems and/or the NRC network infrastructure for published or unpublished vulnerabilities. These guidelines also apply

to software that checks systems for weak passwords, or any software utility designed to decipher ("crack") passwords, or that provides other unauthorized access to any NRC computer or network device. Various commercial, Government-developed, and freeware versions of this type of scanning software are available to the general public (including the hacker community). Vulnerabilities tested by the software include attempts to access user accounts, user name/password files, and databases or hash tables by methods other than authorized software or methods on authorized systems. If used appropriately and in an authorized manner, these types of tools can potentially help NRC ISSOs, systems administrators, and other security staff in closing up any systems vulnerabilities or weaknesses that may be identified. However, since these tools also have the potential to negatively impact network operational performance, their use shall only be authorized after full coordination with the NRC Information Technology Infrastructure Division (ITID), OCIO, which is responsible for the secure operation of the NRC unclassified LAN/WAN infrastructure.

The NRC LAN/WAN ISSO is currently authorized to conduct periodic scanning of all systems connected to the unclassified network infrastructure. **[REDACTED]** Only personnel specifically authorized by the Director of ITID/OCIO shall be granted approval to use vulnerability-scanning and password-checking software. NRC personnel are not authorized to attempt to introduce any vulnerability-scanning or password-checking tools into NRC, whether by introducing unauthorized media containing such software, downloading this software from network locations, or any other means without specific permission from the Director of ITID/OCIO or his designee. Requests to use this type of software shall be submitted in writing to ITID/OCIO via the senior management of any NRC office that may desire to use this type of software. Any individual who is proposed as an authorized user of scanning software must be properly trained. Since these tools are highly technical, authorized users will normally be limited to NRC systems administrators or ISSOs. Vulnerability-scanning software is typically used during individual system security testing in support of a system certification and accreditation process. Vulnerability scanning may also be useful to system developers who can ensure that vulnerabilities are fixed during the system development process and not after the system has already been deployed in the NRC operational network environment.

Copies of the results of all authorized vulnerability scans of any NRC system shall be provided to the Director of ITID/OCIO and also to the NRC SITSO, and to the systems owners or ISSOs. All NRC personnel who have been authorized to perform system scans shall coordinate those scanning activities with the NRC LAN/WAN ISSO. The NRC LAN/WAN ISSO shall identify the currently approved list of vulnerability-scanning and password-checking software that is authorized for use in NRC systems. Only

products from the approved list are authorized for use in NRC systems. Since this list is subject to frequent changes, please contact the NRC LAN/WAN ISSO for the most recent approved list.

The most recent guidance related to the use of vulnerability-scanning and password-checking software is posted on the NRC internal Web site under the IT customer support link.

2.6.10 Labeling of AIS Media

The following procedures should be implemented to label media containing sensitive data. Labeling should identify the sensitivity level of the information contained within the media to facilitate proper storage of media. Compliance with these procedures reduces the risk of sensitive information being left in unauthorized places and reduces the chance of intentional disclosure, copying, or destruction of the information.

- Sensitive Media Marking – All media containing sensitive information should be clearly labeled to indicate the sensitivity level of the most sensitive information contained on the media. The sensitivity level of the data should be clearly visible in human readable form on its exterior, electronically within the file containing the sensitive information, and on workstation, console, and PC monitor screens whenever sensitive information is displayed.

- Privacy Act Media – Magnetic media containing Privacy Act data should be labeled with the following additional information:

  - Privacy Act Statement – Wording to the effect that the information contained in the media is protected by the Privacy Act of 1974 and should be safeguarded against unauthorized disclosure.

    - Retention period

    - Destruction or deletion guidelines

- Diskette Labeling – Externally label all diskettes containing sensitive information to indicate sponsor, creation date, sensitivity level of the data contained, and a brief description of the data on the storage media. This information should be written in permanent ink on a gummed label affixed to the diskette itself.

- Placement of Labels – The label should be placed on the medium (diskette, microfiche sheet) itself, and if a protective sleeve is used, the label should be either visible through it, or the protective sleeve should be labeled.

- Copied Information – If sensitive information is copied to storage media from a hard disk of a computer or from another network system, the media should assume the sensitivity level of the data that are copied onto them. When information is copied from one medium to another such as from a diskette to a computer or between computers directly and the media have different levels of security, both media shall assume the higher level of security and shall be labeled accordingly.

- Specification of Media Contents – Special-use diskettes, tapes, or optical storage media, such as media containing copies of data to be transported to another workstation, should be labeled to indicate what type of file(s) the media contain, any special instructions, and a point of contact.

- System-Generated Labeling – In the case of computer-generated documents, sensitivity labels should be system generated.

- Marking of Removable Media and Devices – Removable AIS storage media and devices used with AIS should be marked on the front only, with appropriate markings to indicate the highest level of sensitive information contained therein. Pressure tape or labels may be used for this purpose.

2.6.11 Storage of AIS Media

The following is a list of recommended procedures for properly controlling and handling storage media:

- User Storage of Media – Magnetic media produced and utilized by individual users on their workstations should be stored in locked desks or offices and should be afforded protection consistent with the security provided to sensitive information in hard copy form.

- Operating System Media – Media containing operating system information should not be issued to individuals other than system or network administrators.

- Prohibition Against Unattended Media – Media containing sensitive information should not be left unattended in automobiles, at home, or in the workplace when not in use.

- Protection of Media From Heat and Cold – All storage media should be stored away from extreme heat or cold, direct sunlight, extreme humidity, and strong magnetic fields, such as those generated by motors found in fans or office heating and cooling equipment.

- Use of Removable Hard Drives – Whenever PCs are being considered for a standalone application, consideration should be given to the use of removable hard disk drives for storing sensitive information. This practice allows the hard disk to be removed and stored in a secure container.

- Protection Against Static Electricity – Avoid using any plastic diskette containers that can generate static that will damage data.

- Write-Protecting Diskettes – All diskettes should be write protected before their storage. This step will ensure that sensitive data on the diskette are not accidentally overwritten.

2.6.12 Destruction of Storage Media

Desktop workstations, laptop and notebook computers, and other IT devices often contain components for permanent program and data storage (e.g., the hard drive on a desktop workstation). When these components fail or are removed because they are no longer needed (surplus) or are obsolete, the media storage components (e.g., hard drive, bubble memory, flash card) must be purged of all residual data. This purging must be accomplished using specialized software or hardware because standard file delete capabilities only delete the file reference, not the file itself. Thus, the data are easily recoverable. Even reformatting a hard disk does not ensure that the stored data cannot be recovered.

To positively purge any residual data, the media storage device should be degaussed. Alternately, an NRC-approved program **[REDACTED]** should be used to completely overwrite the media multiple times with random patterns. If neither of these options can be performed, the media must be destroyed. Contact the OCIO Computer Security Staff for assistance in purging NRC systems. The following procedures should be implemented when any media containing sensitive information are to be disposed of or

reused. Compliance with these guidelines reduces the risk of exposing sensitive information to the threat of disclosure or copying by unauthorized personnel.

- Prohibitions on Destruction of Media – Removable magnetic storage media, such as diskettes and tapes that contain classified or sensitive information, should not be disposed of in regular waste containers. These media should be sent to DFS for retention or destruction.

- Burning and Shredding of Media – If degaussing is not possible, media should be destroyed by burning or with a crosscut shredder approved for destruction of classified media.

- Overwriting Media – Defective or damaged magnetic storage media that contain sensitive data should not be returned to the vendor who performs maintenance or repair unless the vendor is contractually required to protect sensitive data. The sensitive data should first be overwritten before the media may be released to uncleared personnel. This requirement also applies to media to which an unsuccessful attempt has been made to copy sensitive information.

- Destruction of Defective Media – Defective hard disk drives, diskettes, or magnetic tapes that contain sensitive information and that cannot be erased by degaussing should be destroyed by burning.

- Hard Disk Media – If hard disk drives are removed from or replaced in a workstation, the hard drive that is removed should be unconditionally formatted before removal. If this is not possible, hard disks should be degaussed or sent to DFS for retention or destruction.

- Media Maintenance – If a computer system containing sensitive unclassified information is to be sent out for service, the hard drive should be removed before the system leaves the facility. The hard drive should be stored according to the level of sensitivity of the data processed on that system until the computer system is returned.

- Clearing System Memory – Always clear sensitive information from the system memory of the disk operating system (DOS) **[REDACTED]**.

Part 3
Categories of NRC Automated Information Systems

NRC automated information systems (AISs) vary in size, complexity, sensitivity, criticality, and importance to the agency. Applying equal levels of concern and resources to all AIS is not possible or cost-effective. There are insufficient resources to address security equally for all AISs. Further, focusing management attention on systems of lesser importance to NRC often means that vulnerabilities in systems of greater importance remain unresolved.

The need to focus scarce resources to obtain the best return on investment is recognized in Government-wide security guidance (Office of Management and Budget [OMB] Circular A-130), which identifies Major Applications (MAs), and General Support Systems (GSSs). OMB security guidance then addresses security measures for MAs and GSSs because compromise of those systems would pose the greatest loss to or have the most negative impact on the agency. OMB assumes that security for most all other systems in an agency would be satisfied by controls included in the GSS on which it is installed. The definitions for an MA and a GSS are contained in the OMB Circular A-130, Appendix III, and they are given in Section 3.1 herein.

OMB also provides guidance for budget preparation, submission, and execution in OMB Circular A-11. In the discussion of information technology (IT) projects and investments in OMB Circular A-11, OMB uses the following language to describe a major IT system or project:

"***Major IT system or project*** means a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources." Within this context of a major IT investment, MAs and GSSs are both considered to be major IT systems.

Presidential Decision Directive (PDD) 63, "Critical Infrastructure Protection," issued in May 1998, includes a range of activities intended to enhance the security of cyber and physical public and private infrastructures. PDD 63 requires agencies to identify any assets (such as an IT system) that are critical to national security, national economic security, or national public health and safety. Any IT systems that are critical (as per

PDD 63) would also be considered to be major IT systems. NRC currently has no "critical" IT systems.

3.1 Categories

The definition of an IT system is very broad in current Federal and OMB policy guidance. However, personal software productivity tools, user-developed tracking spreadsheets and databases, and single-user systems are generally not considered to be "systems." Security for these types of small applications and tools is provided by the NRC local-area network/wide-area network (LAN/WAN) GSS. OCIO maintains a master inventory of NRC automated systems, and these small applications and tools are not included in the master inventory unless an office specifically requests that a specific small software application be added to the master inventory as a system. Sponsors are to screen the applications and software tools in their offices to determine which ones merit the attention to appropriately be called systems, which will then be included in the NRC master inventory of systems. For those NRC software applications that have been determined by the OCIO and the sponsor to be systems, the NRC uses four categories to describe its AISs:

- **Major Application (MA)**

  The term "Major Application" means a computerized information system or application that requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Because of their impact on the agency mission and the information they contain or process, MAs require special management oversight. (See OMB Circular A-130, Appendix III.) For example, an agencywide financial management system containing NRC's official financial records would be an MA. A computer program or a spreadsheet designed to track expenditures against an office budget would not be considered an MA. Similarly, commercial off-the-shelf software products (such as word processing software, electronic mail software, utility software, or general purpose software) would not typically be considered MAs.

- **General Support System (GSS)**

  A GSS is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

(See OMB Circular A-130, Appendix III.) The mission objective of a GSS is to provide AIS resources in support of the organizational mission. Typical GSSs are LANs, WANs, servers, and data processing centers.

- **Listed System**

OMB policy guidance requires that a security plan be in place for all sensitive systems. NRC uses the term "Listed System" to refer to a computerized information system or application that processes sensitive information requiring additional security protections, and that may be important to the operations of an NRC office or region, but is not an MA when viewed from an agency perspective. Most NRC systems rely on the security protections provided by the NRC LAN/WAN GSS. However, NRC offices have developed a number of additional non-major applications that are processing sensitive data such as individual privacy act information, law enforcement sensitive information, sensitive contractual and financial information, and other categories of sensitive information that the sponsor has determined will require additional security protections beyond the basic security provided by the NRC LAN/WAN. For those types of non-major applications that the sponsor has built in additional security protections and controls because of the added sensitivity of the information being processed, such a non-major application shall be categorized as a "Listed System." The security plan for a listed system will describe those additional security protections and controls. These additional security controls could refer to the use of additional passwords, or the use of additional security technology such as virtual private networks (VPNs), digital signatures, secure Web sites, or other security solutions based on the use of public key infrastructure (PKI) technology. In addition, any system that processes classified information or unclassified Safeguards Information (SGI) that is not a GSS or a MA shall be categorized as a Listed System. An abbreviated security plan format that is compliant with National Institute of Standards and Technology (NIST) security plan guidance is available on the NRC internal Web site.

- **Other**

If the sponsor for an NRC system does not believe that additional security protections are necessary, and the information being processed by the office non-major application is adequately protected by the security provided by the NRC LAN/WAN, such a system shall be categorized as an "Other" system. This categorization assumes that OCIO and the sponsor have first jointly decided that the application is appropriately called a system and is to be included in the NRC master inventory of systems. Systems in the NRC Other category are typically collections of computer-based activities that while focused on a particular mission function or objective do not have the structure, size,

data sensitivity, or the mission importance to warrant additional special management attention or additional security controls. An office database system used by multiple individuals to support tracking and analysis of licensee reports may be categorized as "other." It is up to each individual sponsor to determine which office non-major applications should be categorized as Listed Systems, Other systems, or systems that are so small that they will not be categorized as a system. The Security Plan for the NRC LAN/WAN GSS covers all of the NRC systems on the network that are categorized as Other.

A summary of the basic security planning and reporting measures required for each type of system is shown in Table 3-1.

Table 3-1
Security Planning and Reporting Requirements
by System Type

Security Requirement	System Type			
	General Support System	Major Application	Listed	Other
Annual System Sponsor Review	X	X	X	X
Included with the Office of the Chief Information Officer Master System Inventory	X	X	X	X
Risk Assessment	X	X		
System Security Plan	X	X	X	
Memorandum of Understanding/Memorandum of Agreement for Interfacing systems	X	X		
Information System Security Officer Appointed	X	X	X	
Tested IT Contingency Plan (Business Continuity)	X	X		
Periodic Certification and Accreditation	X	X	X	
Security Test and Evaluation	X	X		
Annual Self-Assessment	X	X		

(Note: Requirements are specified by the Federal Information Security Management Act and OMB Circular A-130, Appendix III.)

3.2 Category Determination

Final determination of the appropriate category for an NRC AIS is the responsibility of the CIO, based largely on the recommendation of the system sponsor. At least annually, the system sponsor shall review the AIS for which he or she is responsible to ensure that it is properly categorized (i.e., GSS, MA, Listed System, Other). A report identifying the GSS, MA, Listed System, or Other AIS shall be provided to OCIO, revalidating the master inventory of systems. An AIS that changes categories shall have 1 year from the date the change is determined to comply with the requirements in the new category. This report shall also prioritize the systems in the office, as required by Federal AIS automated security policy guidance (OMB Circular A-130).

Part 4
Certification and Accreditation

4.1 Identifying Risk for an Automated Information System

The Federal Information Security Management Act (FISMA) tasked agencies to ensure that automated information systems (AISs) used or operated by the agency provide automated information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, or destruction. FISMA also requires agencies to develop and maintain a risk-based automated information security program with risk-based automated information security policies, procedures, and control techniques that cost-effectively reduce information security risks to an acceptable level. NRC demonstrates its compliance with the FISMA requirement for a risk-based automated information security program primarily through the systems security certification and accreditation processes and procedures that are utilized at NRC. All proposed significant changes, upgrades, and modifications to NRC AISs or to the network infrastructure, including all proposed connections to the NRC network infrastructure, are first assessed to determine the overall impact and risk to the accredited (approved) configuration. This assessment is accomplished through the systems security certification and accreditation process.

FISMA also tasked the National Institute of Standards and Technology (NIST) to develop Federal information processing standards (FIPS) and guidelines related to providing appropriate levels of information security controls according to a range of risk levels. NRC guidance related to risk management and systems security certification and accreditation shall be based on the NIST guidance. (As NIST is developing and updating several current standards and guidelines in this area, NRC staff should contact the OCIO Computer Security Staff for the most recent guidance.) Adherence to the NIST standards and guidelines shall be included in all NRC contracts for systems security support.

All systems operate with a risk of potential compromise. One of the primary objectives of security planning is to ensure that this risk is minimized, at a reasonable cost. Balancing the cost of security controls against the reduction in risk requires an understanding of the characteristics of the threats, vulnerabilities, and risk specific to

the system. An analysis of the risk characteristics for an automated information system (AIS) may be accomplished using a three-step process:[1]

- Examine the system's sensitivity and criticality—

  Examining the system's sensitivity and criticality provides an assessment of its value to the organization. This examination is generally addressed from three perspectives: (1) confidentiality—assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure; (2) integrity—assurance that the system and associated data are protected against unauthorized deletion or modification; and (3) availability—assurance that the system and its associated assets are accessible and protected against denial of service attacks.

- Assess the exposure of the system and its associated assets (hardware, software, data) to both external and internal threats—

  External system exposure relates to the methods by which users (and therefore attackers) may access the system (e.g., dedicated connection, Intranet connection, Internet connection, wireless network), the existence of back-end connections (e.g., desktop modems), and the number of users that access the system. Internal system exposure relates to the types of individuals that have authorization to access the system and the information the system stores, processes, and transmits. It includes such items as individual security background screening and/or clearance levels, access approvals, access by foreign nationals, and need-to-know.

- Assign appropriate levels of concern (low, moderate, high) for both sensitivity/criticality and exposure—

  In determining appropriate levels of concern for an AIS, a number of factors need to be considered, such as the adverse impact that might result from a security breach (e.g., monetary loss or mission impact) and laws establishing specific protection requirements (e.g., Privacy Act of 1974). NIST Special Publication 800-37 (Draft) provides additional guidance that shall be used for assigning levels of concern to AIS risk characteristics.

[1]The three-step process is described in detail in NIST Special Publication 800-37 (Draft). The process will be applied to NRC systems when NIST finalizes the draft guidance.

The level of risk/concern should be determined for the AIS and used within both the risk assessment and the System Security Plan. This determination will help determine the controls and countermeasures appropriate for the AIS.

4.2 Certification and Accreditation Process

GSSs and MAs require specific management approval before being placed in operation. This approval to operate shall be renewed at least every 3 years or when the AIS experiences a significant upgrade or modification.

The purpose of approving an information system for operation is twofold: (1) the process ensures that the potential risk to the AIS and its associated assets (hardware, software, data) are known and documented and (2) an official, the Designated Accrediting Authority (DAA), has reviewed those risks and determined that the level of risk is acceptable. This decision is also documented in writing, thus making the DAA accountable for his or her decisions.

Within the NRC, the DAA is the CIO for all MAs and GSSs. The CIO is also the DAA for all classified systems and systems that process Safeguards Information (SGI). The CIO is also the DAA for all "Listed Systems," which are NRC systems that process sensitive information and require additional security protections as discussed in Part 3 of this handbook.

For MAs and GSSs, the DAA bases his or her approval decision on the information contained in a security certification and accreditation (C&A) package consisting of the following documents:

- Risk Assessment Report

  The risk assessment identifies the threats and vulnerabilities associated with an AIS and provides recommendations for mitigating those risks. The Risk Assessment Report is prepared to document the risk assessment methodology and its findings and recommendations. An assessment of risk shall include the specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time. Risk assessments at NRC shall utilize the guidance provided in NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems."

- System Security Plan

  The System Security Plan (SSP) describes the AIS functionality and production environment. The SSP also documents security controls and countermeasures that are in place or are planned to prevent or detect a security incident or mitigate the impact of a security breach. The SSP shall also include procedures for the ongoing training of individuals who are permitted access to the system; procedures for the ongoing monitoring of the effectiveness of security controls; and provisions for the continuity of operations in the event of system disruption or failure. SSPs at NRC shall utilize the guidance provided in NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."

- Security Test and Evaluation (ST&E) Plan and ST&E Report

  An ST&E Plan describes how specific security controls will be tested and evaluated (e.g., live testing, analysis, observation). Testing of security controls is especially important because since security controls target abnormal or aberrant situations, testing their effectiveness is often overlooked in normal system testing. The ST&E Plan will be accompanied by an ST&E Report that documents the testing process and results.

- Contingency Plan and Contingency Plan Test Report

  NRC is dependent upon the availability of its AIS. Plans must be in place to continue business activity if an AIS should fail or access to the AIS is denied. The contingency plan should consider business continuity, recovery of the AIS, and the occurrence of a catastrophic or less than catastrophic event. The Contingency Plan Test Report documents the results of testing of the contingency plan. IT Contingency Plans at NRC shall utilize the guidance provided in NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems." IT contingency plans for MAs and GSSs shall be tested each year. A live test provides the best indication of the adequacy of a contingency plan test. If a live test cannot be conducted due to operational constraints, a simulated test may be conducted in lieu of the live test.

  The NRC GSS infrastructure provides for system recovery **[REDACTED]** of the occurrence of a catastrophic event **[REDACTED]**. MAs hosted on the infrastructure that require shorter recovery periods or less data loss must provide an independent contingency capability. Many NRC MA contingency plan requirements are satisfied

by the contingency plan applicable to the underlying local- and wide-area network infrastructure.

- Information System Security Officer (ISSO) Appointment Letter

  The ISSO Appointment Letter must be signed by the system sponsor. The letter must also state whether the assigned individual has other responsibilities that may create a separation of duties concern.

- Certification Report With Certification Signature

  A certification review is a technical analysis of an AIS to evaluate the effectiveness of in-place controls and countermeasures and identify risks and vulnerabilities that have not been adequately addressed. The Certification Signature is acknowledgment, by a technically competent individual, that the AIS security environment is adequate, except as stated in the Certification Report. The Certification Report is signed by the system sponsor/owner.

- Accreditation Signature

  The Accreditation Signature is the formal acknowledgment of the DAA that the system security is adequate, except as noted. The DAA may accredit a system without restriction, deny approval to operate, or issue an interim accreditation. When an interim accreditation is issued, it must be accompanied by an action list that defines the corrective actions required and a date for completing all corrective actions. If the completion date is exceeded, the accreditation lapses. The DAA for NRC MAs and GSSs, and for all Listed Systems, is the CIO. The CIO may delegate this accreditation authority to other senior management officials, such as the system owners/sponsors.

Certification and Accreditation (C&A) Process for Listed and Other Systems

For NRC “Listed Systems,” the security C&A effort is tailored. The majority of sensitive systems in this category rely on the security protections provided by the underlying NRC LAN/WAN infrastructure but also have additional security protections that have been incorporated into the system design. The security plan that is prepared for these sensitive Listed Systems shall utilize the abbreviated security plan format that is provided on the NRC internal OCIO IT customer support Web site. The abbreviated security plan is compliant with NIST guidance. The completed security plan should be

submitted to OCIO with a memorandum that documents how the security requirements to protect the sensitive information are being satisfied, along with a discussion of the implemented security controls, and any residual risks that may exist. The memorandum that is submitted with the abbreviated security plan provides the security certification for the Listed System. The security plan is reviewed by OCIO, and approval of the abbreviated security plan for the Listed System results in system security accreditation (which is the management approval to operate). This process shall also be utilized for those NRC Listed Systems that are standalone computers and laptops that are being used to process classified and/or Safeguards Information.

The security C&A requirements for all other systems that rely solely on the security protections of the underlying NRC LAN/WAN infrastructure are covered in the security plan and security accreditation provided by the NRC LAN/WAN. This specifically includes the category of "Other" systems for which the DAA is the CIO. No additional C&A action is required for Other systems. (See Table 3-1 in Part 3 of this handbook.)

4.3 Scheduling a C&A Effort

An AIS must be initially granted an approval to operate before being placed in production. The approval must then be renewed every 3 years or when there is a significant change. A C&A effort for an MA or a GSS can require up to 6 months to complete, depending on system complexity and availability of supporting material and staff. Renewals performed on the 3-year cycle can be scheduled as part of the budget process. Renewals that occur because of a major change need to be anticipated and included as part of the change planning process.

It is the responsibility of the system sponsor to identify all systems that require accreditation, using the guidance provided in this handbook (and Table 3-1 of Part 3). The NIST special publication guidance related to security C&A mentioned earlier in this section also contains useful information to help explain the concepts of C&A. The CIO has responsibility for managing the agencywide AIS security program (as per FISMA), and the CIO maintains program and system metrics in order to respond to periodic Office of Management and Budget FISMA reporting requirements. OCIO maintains the master database of all IT security information and metrics for NRC systems, and keeps copies of all security accreditation documentation for all MAs, GSSs, and Listed Systems.

Appendix A
NRC Systems Development and Maintenance Security Controls

Approved: February 1, 1999
(Revised: September 12, 2003)

Contents

Appendix A
NRC Systems Development and Maintenance Security Controls

1 Introduction

The NRC System Development Life Cycle Management Methodology (SDLCMM) provides life cycle structure and guidance for NRC application systems. It includes the development and the life cycle management of NRC application systems from the definition of the initial project requirements (after a project has been identified) through the decommissioning of a system that is no longer to be used. The development of a security plan is one of the important activities included in the SDLCMM. The security plan should be used to ensure that security is considered during all phases of the system life cycle.

This appendix is intended to provide supplemental guidance to system owners who are sponsoring the development or upgrade to an NRC automated information system (AIS). This appendix describes the minimum-level system controls applicable to a server or an application. The control measures described are grouped by six basic security areas that must be addressed when establishing server-level or application security: identification and authentication, discretionary access, auditing, system integrity, data integrity, and reliability of service.

The control measures described in this appendix are not intended to be system specific but rather to provide a policy-level template that the system owner/sponsor should require when specifying a security environment for a specific system or application. Decisions regarding which control measures are incorporated into a system or application should be risk based and should consider the following factors:

- The control measure is not required

  Specific systems may not require a particular control if the level of sensitivity/criticality of the system and the data it processes, stores, or transmits is sufficiently low that use of the control is not warranted or cost-effective.

Specific systems may not require a particular control if the system is installed on a General Support System (GSS) (e.g., an application installed on a server or a server protected by infrastructure controls) where the GSS provides the necessary level of control. For example, a system might not require system-level access controls if that control is being provided by the GSS.

- System capability

  A particular control, as described, may not be supportable by the system's hardware and software components. If the feature is not supported, it should be considered as a possible inclusion in future upgrades if economically feasible. All new system development and acquisition should include these controls as part of the design specifications.

- Commercial products

  Efforts should be made when using commercial off-the-shelf (COTS) software products to identify and procure those products that support the controls described in this appendix.

- Increased security control requirements

  Individual custodians of information that requires a higher level of protection than that afforded by system-level controls are responsible for coordination with system administrators and/or sponsors to integrate application-specific controls.

2 System Controls

2.1 Identification and Authentication (I&A) Controls

I&A controls provide the capability to establish, maintain, and protect a unique identifier and password for each authorized user. They also provide the capability to establish, maintain, and protect from unauthorized access that information that can be used to authenticate the association of a user with that identifier. I&A protects against attempts by unauthorized users to gain access to the system. I&A mechanisms also prevent authorized system users from accessing resources or using privileges that have not been authorized.

General I&A controls include the following actions:

- Ensuring that all default system accounts (e.g., “admin,” “guest”) and passwords (e.g., “guest,” “test,” “system”) are deleted, disabled, or the password changed before implementation of any new system. This action pertains to both hardware and software systems, including operating systems, servers, and routers.

- Assigning unique user identifiers (IDs) to identify system users. User IDs must be issued on a one-to-one basis, and group user IDs are not permitted without special authorization.

- Requiring users to identify themselves with their user ID before being allowed to access any AIS resource.

- Ensuring that each user ID has an associated, user-selectable password.

- Ensuring that actions taken or processes initiated by a user are associated with that user’s user ID in all system and audit logs.

- Enabling an administrative privilege that will permit the disabling of specific user IDs.

[REDACTED]

- Enabling the password mechanism to authenticate the claimed identity of a user.

- Setting the system to perform entire user authentication when an invalid user ID is entered. The error message should state that the logon information is invalid but not specify which part of the information is incorrect.

[REDACTED]

Specific Password Controls

The implementation and enforcement of proper password standards are essential to protecting system and application components from unauthorized access. The local-area network (LAN) user ID and password will suffice for the majority of NRC applications. Applications that require additional security protections due to data sensitivity may require an additional user ID and password. On the basis of a risk

management review, the NRC Designated Accrediting Authority (DAA) may authorize waivers to these password policies on a limited basis. Where individual systems will support them, systems enforce the following standards:

[REDACTED]

- Limit access to the encrypted passwords to system, network, and application security administrators, as applicable.

- Audit all changes to password files.

2.2 Discretionary Access Controls

Discretionary access controls allow the administrator to configure the system to ensure that authenticated users can access and perform operations on only the system resources for which they have authorization. The resources include directories, files, applications, local-area network (LAN), wide-area network (WAN), and database management systems. The operations include read, write, execute, delete, modify.

- System access should be granted after the user is properly authenticated.

- Only Information System Security Officers (ISSOs) or system administrators should have the authority for the creation, deletion, or modification of user access authorization data.

[REDACTED]

- Permission controls (access control lists) should be used to designate which users and user groups are granted specific access permissions. Access permissions should be modified only by the sponsor or the system administrator.

2.3 Auditing Controls

Auditing controls support accountability by providing a chronology of user actions. These actions are associated with individual users for all security-relevant events and are stored in an audit trail file. The audit trail can be examined to determine what happened and which user was present or initiated a security-relevant event. The audit trail data should be protected from unauthorized access, modification, or destruction. Audit trails should provide user accountability for security administration actions.

Federal information technology (IT) security guidance specifies that appropriate security controls, processes, and procedures should be applied, commensurate with the risks and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the IT system, or the information it processes. For Major Applications (MAs) and GSSs and for systems that are processing sensitive information, auditing controls should be addressed in the individual System Security Plans based on this risk management process. For other systems that do not process sensitive data, auditing frequency can be established by the system owner, also based on a reasonable assessment of the risk to the system. **[REDACTED]**

2.4 System Integrity Controls

System integrity controls promote separation of user and system processes and data; protect software, firmware, and hardware from unauthorized modifications (deliberate and accidental); and control user and maintenance personnel actions. System sponsors should take action to ensure that the following controls are implemented to the greatest extent possible:

- Separate and protect user processes and their data from other user processes. System programs should be separated and protected from any user processes.

- Review modification dates, check sums, and examine digital signature features as part of the auditing process to verify the integrity of delivered software.

- Set the system to restrict the use of privileged instructions to the minimum necessary number of administrators.

- Configure the system to ensure that the execution of system maintenance or repair software, modification, or replacement of system and application software requires administrator privilege.

2.5 Data Integrity Controls

Data integrity mechanisms ensure that data are entered and maintained in a correct and consistent state. The following requirements provide for controls that promote tracking of changes to resources and protect data against exposure, unauthorized modification, or deletion while they are stored or transmitted over a network:

- Configure applications and systems to audit the time and date of the last modification to resources, as well as the identity of the user who performed the modification or transaction.

- Where determined to be appropriate by the risk analyses process, and if technically feasible and cost-effective, employ encryption controls to preserve and verify the integrity of stored or transmitted data.

2.6 Reliability of Service Controls

The following reliability of service requirements ensure continuous accessibility and availability of system resources to authorized users. These requirements also prevent or limit interference with time-critical operations and allow the system to maintain an expected level of service during adverse (deliberate or accidental) conditions.

- Configure the system to detect and report all conditions that degrade service below a specified minimum.

- Place limits on the amount of the total disk and/or central processing unit resources an individual or group can use.

3 Other Controls

3.1 Warning Banner

NRC systems shall be configured to display the following warning banner to users upon first accessing NRC automated information resources:

USE OF THIS COMPUTER CONSTITUTES A CONSENT TO MONITORING.

This computer system is for official or authorized use only. Federal computer systems are subject to monitoring for maintenance, to preserve system integrity and security, and for other official purposes. You should not expect privacy, nor protection of privileged communication with your personal attorney, regarding information you create, send, receive, use, or store on this system.

If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any related information, including your identification, may be provided to law

enforcement officials, including the Office of the Inspector General. Anyone who violates security regulations or makes unauthorized use of Federal computer systems is subject to criminal prosecution and/or disciplinary action.

UNAUTHORIZED ACCESS PROHIBITED BY LAW—TITLE 18, *U.S. CODE* SECTION 1030.

Public Law 99-474 provides that anyone who accesses a Federal computer system with or without authorization, and by means of such conduct obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on the computer, shall be subject to fine or imprisonment, or both.

3.2 System Documentation

All documentation providing the technical parameters (e.g., system administrator manuals) of the AIS hardware- and software-based security features should be accounted for and controlled. Sensitive hard copy documents, working papers, microfiche, and photographs should be stored in locked filing cabinets or safes. Access is to be restricted to authorized personnel only.

3.3 Backup of AIS

Backups should always be performed to allow for recovery of information that has been accidentally or maliciously destroyed. **[REDACTED]**

3.4 Encryption Controls for NRC Sensitive Systems

Cryptographic-based security systems may be utilized in various computer and telecommunication applications (e.g., data storage, access control and personal identification, network communications, radio, facsimile, and video) and in various environments (e.g., centralized computer facilities, office environments, and hostile environments). The cryptographic services (e.g., encryption, authentication, digital signature, and key management) provided by a cryptographic module are based on many factors that are specific to the application and environment. Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST). For all NRC sensitive unclassified information (including Safeguards Information [SGI]) that may require cryptographic protection, only products that make use of NIST-approved encryption algorithms shall be used. Example

algorithms that have been approved for use include the Advanced Encryption Standard (AES) (FIPS PUB 197) and the Triple Data Encryption Standard (DES).

The DES standard became effective July 1977. It was reaffirmed in 1983, 1988, 1993, and 1999. It is anticipated that the Triple DES and the AES will coexist as FIPS-approved algorithms allowing for a gradual transition to AES. The DES standard was revised in 1999 to include the Triple DES. The Triple DES, as specified in American National Standards Institute (ANSI) X9.52, is recognized as a FIPS-approved algorithm. The Triple DES will be the FIPS-approved symmetric encryption algorithm of choice. The Single DES (i.e., DES) will be permitted for legacy systems only. New procurements to support legacy systems shall, where feasible, use Triple DES products running in the Single DES configuration.

Implementations of the encryption algorithms that are tested by a NIST-accredited laboratory and validated will be considered as complying with NIST standards. Since cryptographic security depends on many factors besides the correct implementation of an encryption algorithm, system developers should also refer to NIST Special Publication 800-21, "Guideline for Implementing Cryptography in the Federal Government," for additional information and guidance. (NIST SP 800-21 is available at http://csrc.nist.gov.)

Modules are no longer to be tested against the FIPS 140-1 requirements. All previous validations against FIPS 140-1 are still recognized. However, for all Federal agencies, the use of encryption products and modules that conform to FIPS PUB 140-2 is now mandatory for the protection of sensitive unclassified information when the agency determines that cryptographic protection is required. Agencies are required to use the standard in designing, acquiring, and implementing cryptographic-based security systems within computer and telecommunications systems (including voice systems).

3.5 Encryption Controls for NRC Systems Processing Classified Information

The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems. The NSTISSC has been recently renamed the Committee on National Security Systems (CNSS).

For all NRC systems that are processing classified information, only encryption products that have been approved by the National Security Agency (NSA) shall be used for the protection of classified data. Contact OCIO Computer Security Staff and the Information Security Section (INFOSEC) in the Office of Nuclear Security and Incident Response (NSIR) for assistance with any classified system processing security requirements.

NSTISSP #11 is a national security community policy governing the acquisition of information assurance (IA) and IA-enabled IT products. The policy was issued by the Chairman of NSTISSC in February 2000. The policy mandates, effective July 1, 2002, that departments and agencies (including the NRC) shall acquire, for use on national security systems, only those COTS products or crypto-modules that have been validated in accordance with the International Common Criteria for Information Technology Security Evaluation, National Information Assurance Partnership's (NIAP's) Common Criteria Evaluation and Validation Scheme (CCEVS), or by the NIST FIPS Crypto-module Validation Program (CMVP). Additionally, subject to policy and guidance for non-national security systems, NSTISSP # 11 notes that departments and agencies may wish to consider the acquisition of validated COTS products for use in information systems that may be associated with the operation of critical infrastructures as defined in the Presidential Decision Directive on Critical Infrastructure Protection (PDD-63).

In addition to the specific requirements to use only validated COTS security products in classified information systems, NRC shall also give preference to the use of validated COTS security products for all other NRC AISs.

4 Automated Information System Physical Security Controls

Management Directive 12.1, "NRC Facility Security Program," contains policies, guidelines, and procedures for the overall NRC Facility Security Program, including the approval of facilities for the handling and storage of classified and sensitive unclassified information. This appendix describes additional guidance pertaining to physical security controls that shall be implemented to specifically protect NRC AISs. Physical and environmental security controls are implemented to protect the NRC buildings, facilities, and related supporting infrastructures that are housing essential AIS resources, such as data centers, server rooms, the rooms that contain telecommunications equipment, wiring closets, and other AIS equipment rooms. Physical and environmental security controls are implemented to protect against potential threats to NRC's AIS physical environment and are intended to help prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft. NIST has published a manual that provides guidance for performing

AIS security program reviews and system security self-assessments, that is, NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems." Appendix A in the NIST publication contains a listing of physical security measures that are checked as part of the system's security self-assessment process. The NRC AIS physical security guidelines are based on the NIST guidance.

4.1 Computer Room and AIS Equipment Room Physical Security Controls

The implementation of the following minimum construction requirements for NRC computer and AIS equipment rooms will reduce the exposure of NRC assets to identified risks. The objective of these requirements is to provide all NRC computer and AIS equipment rooms with a means to screen entrants, deny access to unauthorized personnel, and control the flow of materials in and out of the room. The security measures stipulated in this section apply mainly to primary computer rooms and, to a lesser degree, are applicable to equipment rooms. These requirements shall be implemented by the facility sponsor; however, a risk management process shall be used to validate the appropriateness and cost-effectiveness of security controls. Sponsors and regional administrators are authorized to tailor the implementation of security controls to appropriately counter the potential risks associated with each environment.

Rooms adjacent to NRC computer and AIS equipment rooms shall be free of potential physical and environmental threats. Where practical, computer and equipment rooms shall be surrounded by a hallway to prevent environmental threats from being shared and to facilitate monitoring of adjacent areas for unauthorized access attempts.

On the basis of the level of risk, computer and equipment rooms shall have an automated keycard system to control access for NRC employees having authorized access to the room. The system shall record all entries to the room and shall be capable of producing printed audit trails. **[REDACTED]**

4.1.1 Windows and Doors

For NRC rooms that are housing data centers, server rooms, or other essential computer equipment, it is recommended that there be no windows that open to the exterior of the building. If windows already exist, a risk assessment can be conducted to determine the feasibility of closing off the windows to counter any potential threats.

For rooms with lowered ceilings and raised floors, computer and equipment room walls shall extend from true floor to true ceiling. This requirement can be waived by the AIS

system sponsors or regional administrators if a cost-effective, risk management determination is made that indicates that the threats to the computer systems or computer assets in the room are minimal, and if the threats can countered by other security mechanisms, processes, or procedures.

Computer and equipment room doors should be installed with hinge pins on the inside. The doors should be of sufficient strength to prevent unauthorized entry.

4.1.2 Intrusion Detection System

If a computer or equipment room contains a significant portion of the location's AIS equipment assets and is not staffed 24 hours a day, 7 days a week, an intrusion detection system shall be installed in the room. Decisions not to install intrusion detection systems should be supported by risk analyses results showing the detection system not to be cost-effective. The system shall—

- Detect unauthorized entry attempts, as well as motion or sound within the room.

- Be programmed to activate an alarm at a security monitoring center that is staffed 24 hours a day. (Provide the security center with a listing of NRC personnel to be contacted in the event the alarm is activated.)

4.2 Network Physical Security Controls

NRC facility managers shall implement physical security procedures, based on risk, to ensure that the confidentiality, integrity, and availability of NRC networks are sufficient to ensure secured operation.

The following controls for network routers, bridges, gateways, and servers shall be implemented to protect the physical security of network assets.

- Place all network equipment in secured computer or equipment rooms. If this measure is not possible, secure the equipment in locked rooms, such as the telephone or wiring closets.

- Keep telephone and wiring closets that house network cabling or equipment locked at all times. Restrict access to the telephone and wiring closets to a limited number of accountable personnel.

- Keep network consoles logged off or locked out when not attended. If the server does not provide for console protection, physically or logically lock keyboards and consoles at all times.

- Limit access to the computer and AIS equipment rooms in which network equipment resides to those personnel who must access the rooms to perform their duties, such as network and system administrators and telecommunications technicians.

Network physical security safeguards shall be integrated into network design configurations and modifications.

4.3 Key and Combination Control Procedures

It is essential for the protection of all NRC AIS assets that the sponsoring office establish, document, implement, and enforce effective key and combination control procedures.

The NRC sponsoring office should create a comprehensive inventory of all keys and combinations related to the security of office areas, systems equipment, and sensitive materials under their control. The inventory should include the room number, the number of keys, the names of individual(s) issued to, and the date issued. The inventory itself should be appropriately secured (e.g., provided protection at the level of the information being protected by the key or combination).

All individuals should sign for their key(s). Master keys should only be assigned to a select number of personnel.

Individuals signing for keys should be cautioned not to duplicate the key.

All unassigned keys should be properly secured.

Semiannual inventories of all keys should be conducted and recorded. Maintain the inventories as official records for 1 year after they are no longer current.

Include the Division of Facilities and Security (DFS), Office of Administration, as a control point in agency exit procedures to ensure that individuals departing the agency turn in all assigned keys. The Division of Resource Management and Administration (DRMA) is the control point at the regional offices.

Immediately report lost or stolen keys to DFS (or regional DRMAs).

When individuals no longer have a need for access, ensure that combinations are changed immediately.

DFS and regional DRMAs should have any lock(s) rekeyed for which the key(s) are missing and issue new keys to authorized personnel.

4.4 Environmental Security

The facility sponsoring office shall incorporate cost-effective controls to mitigate environmental threats (e.g., fire, water) to AISs and operations. For many types of computer equipment, strict environmental conditions shall be maintained. Manufacturers' specifications should be observed for temperature, humidity, and electrical power requirements. The facility sponsoring office shall ensure that appropriate environmental controls are properly installed, implemented, and maintained to protect NRC AIS resources.

4.4.1 Fire Protection

A fire detection system provides early warning that smoke and/or fire has been discovered and a response action needs to be taken immediately. Fire protection will normally be supplied by the building fire protection system. Class A and C portable fire extinguishers shall be available and located so that an extinguisher is readily available, in accordance with local fire department codes. A sign should be located adjacent to each portable extinguisher and should plainly indicate the type of fire for which the extinguisher is intended.

4.4.2 Protection From Water Damage

To prevent damage from falling or blowing water, facility sponsors shall consider obtaining plastic coverings for all AIS equipment located in computer or equipment rooms. Such coverings should be readily available in the vicinity of computer equipment to allow rapid employment in the event of a water emergency (i.e., sprinkler activation, broken window).

4.4.3 Power Protection

NRC facility sponsors shall ensure that all AIS equipment is protected with surge protection, and if warranted because of its criticality, equipment should be supported by an uninterruptible power supply system.

4.5 Visitor Controls

To safeguard sensitive data from disclosure to unauthorized or uncleared personnel, NRC offices shall ensure that procedures for controlling visitors are established and enforced. Visitors shall not be allowed into areas in which sensitive, SGI, or classified data are being processed, stored, or transmitted unless accompanied by an escort. NRC personnel who are responsible for escorting visitors shall be made aware of the importance of their duties. A means of recording entries and exits of visitors shall be implemented for either the facility or the specified area in which sensitive information is processed or stored, and specifically for any area in which classified processing is being performed. For any specific NRC work space or office in which classified processing is being performed, NRC shall fully comply with the additional physical security guidelines specified by other agencies such as the Department of Defense. (Contact ADM/DFS and OCIO computer security staff for assistance with the physical security requirements for classified processing.) System users shall be instructed to challenge persons they do not recognize in areas in which sensitive processing is being conducted.

In emergency situations, if the need for emergency maintenance personnel arises and the personnel have not been screened or vetted through Security, they require escort by an NRC employee. The escort shall be knowledgeable of the functions being performed by the maintenance personnel.

Appendix B
Information Systems Security
Incident Response Procedures

Approved: February 1, 1999
(Revised: September 12, 2003)

Contents

Appendix B
Information Systems Security
Incident Response Procedures*

A. Overview

With the advent of the Internet and escalating hacker activity worldwide, the threat of compromise or damage to computer systems has grown exponentially over the last few years. The NRC network infrastructure is essential to timely delivery of critical NRC services. Thus, the agency strives to prevent any compromise or damage to its systems, whether through inadvertent disclosure or through modification or loss of information.

This appendix formalizes the procedures for monitoring, detecting, reporting, and responding to information systems security incidents associated with internal NRC computer networks and automated information systems (AISs). These procedures apply primarily to the NRC AISs that are processing unclassified information, such as the unclassified NRC local- and wide-area network, but also to any NRC AISs and standalone computers that may be processing sensitive information, unclassified Safeguards Information (SGI), and classified information. A formal information systems security incident response capability can better respond to all incidents and ensure that the broad range of issues that arise are fully coordinated. It also ensures that NRC executives receive a comprehensive assessment of incident impact on the NRC as quickly as possible. Any information systems security incident that impacts, or has the potential to impact, NRC's ability to successfully perform its mission must be reported to NRC senior management in a timely manner. (See Section C of this appendix for definition of an information systems security incident).

NRC's physical security program protects personnel and facilities, materials, equipment, and information against threats other than military action. The Office of Administration (ADM), Division of Facilities and Security (DFS), is responsible for the agency's Physical and Protective Security Programs. NRC Management Directive (MD) 12.1,

*Note: Because of the dynamic nature of network operations and new threats to information systems, network security procedures are subject to frequent updates. The most current version of the incident response procedures are maintained on the internal Web site (http://csb.nrc.gov/security/security.asp).

"NRC Facility Security Program," contains the policies for these programs and procedures for reporting incidents involving physical or facility security.

The Office of Nuclear Security and Incident Response (NSIR) has primary responsibility for coordinating the agency response to incidents involving licensed nuclear facilities, activities, and material. NSIR is also responsible for NRC information security, specifically information security programs dealing with classification, declassification, and handling of sensitive, SGI, and classified information.

The Office of the Chief Information Officer (OCIO) has also developed separate procedures and processes (posted on the internal OCIO Information Technology (IT) Customer Support Web site) to detect and notify staff when operational service interruptions occur involving internal NRC AISs and networks. These operational service interruptions may include events such as interruption of Internet services, failure of an application, or failure of any other network component or service. However, if it is determined that these events are security related, the processes and procedures for handling information systems security incidents contained in this appendix will apply.

The details of information systems security incidents and related reports are considered "official use only," and shall not be discussed with, given to, or shown to the public by NRC. Information systems security incident details are distributed and released only to those who have a need-to-know to conduct official business. Release of any security incident related information to the public shall not be made without prior approval as specified in MD 3.4, "Release of Information to the Public," and as specified in MD 12.6, "NRC Sensitive Unclassified Information Security Program."

B. Responsibilities

This section summarizes the roles and responsibilities for reporting and responding to information systems security incidents. See Attachment A for a table that lists all the contact information for the following positions.

NRC OCIO

OCIO has overall responsibility for NRC's Automated Information Systems Security Program.

NRC Senior Information Technology Security Officer (SITSO)

The Senior Information Technology Security Officer (SITSO) reports to the NRC CIO. The SITSO provides oversight and guidance for the information systems security incident response procedures and processes. The SITSO also serves as the primary

point of contact between the various security officials throughout NRC, and also with NRC management, including the CIO and the Office of the Executive Director for Operations (OEDO). The SITSO will approve and authorize the reporting of information systems security incidents to the Federal Computer Incident Response Center (FedCIRC), and to other external organizations. For any routine periodic (monthly) report to FedCIRC, the SITSO will forward a summary of that report to the CIO, and the summary will be included with other existing OCIO status reports that are provided to OEDO. For all other nonroutine (emergent) reports that are made to FedCIRC, the SITSO will escalate the internal NRC reporting to include providing details of the incident report to the CIO and OEDO.

The SITSO will also ensure that copies of all reports are provided to the NRC NSIR Operations Center staff, which has primary responsibility for responding to external events involving nuclear security. The SITSO will provide copies of information systems security incident reports, along with understandable technical details, to the Office of Public Affairs (OPA) should it become necessary for the NRC OPA to disseminate appropriate information to the public. The SITSO will also provide copies of these reports to the Office of the Inspector General (OIG) and will coordinate with OIG, or the Office of Investigations (OI), as appropriate, for any incidents that OIG determines requires investigative action. The SITSO will also coordinate the activities of the OCIO Computer Security Staff in responding to, handling, and reporting information systems security incidents involving any computers that are processing sensitive, SGI, or classified information. The SITSO will coordinate with the NSIR Information Security Section to ensure that NRC also files reports for information systems security incidents involving classified information, as required by national security policies, and in accordance with the processes and procedures specified by agencies such as the National Security Agency (NSA). This specifically includes any communications security (COMSEC) incidents. In the absence of the SITSO, the duties and functions listed for the SITSO shall be performed by the Director, Information Technology Infrastructure Division, OCIO.

NRC OCIO Computer Security Staff

The NRC OCIO Computer Security Staff (CSS) is composed of Government employees and contractors in OCIO who possess the appropriate clearance levels required to respond to incidents involving NRC systems that are processing sensitive information, SGI, and classified information. For information systems security incidents in those systems, the CSS will report to, and coordinate with, the SITSO. The OCIO CSS staff will coordinate their information systems security incident response activities with, and

seek assistance as required from, the Office of Administration, Division of Facilities and Security, and with the information security staff in NSIR.

NRC Information Systems Security Officer (ISSO) for the NRC Local- and Wide-Area Network (LAN/WAN)

The NRC LAN/WAN Information Systems Security Officer (ISSO) serves as the security operations specialist within the OCIO, Information Technology Infrastructure Division (ITID), Information Technology Customer Services Branch (IT CSB). The LAN/WAN ISSO is the lead of the NRC Computer Security Incident Response Capability (CSIRC). The LAN/WAN ISSO will inform NRC management when an information systems security incident is confirmed, or when other suspicious activity is observed in NRC's computer information systems and networks. The LAN/WAN ISSO is responsible for forwarding to NRC management the daily, weekly, and monthly summary reports of information systems security incidents involving NRC unclassified computer information systems and networks. The LAN/WAN ISSO will forward reports of incidents in NRC systems that are processing sensitive information, SGI, and classified information to the SITSO and the OCIO CSS. The LAN/WAN ISSO and the SITSO will also provide copies of all information systems security incident reports to the NSIR Operations Center. The SITSO will coordinate with OIG to ensure that digital evidence is preserved through mutually agreeable means. The LAN/WAN ISSO will also forward all information systems security incident reports to the OIG and will coordinate with the OIG about whether investigative action may be required. The ISSO will work with the Customer Support Center and the OCIO Network Operations Center to verify that reported incidents are in fact information systems security incidents, and not other system service interruptions related events such as failure of a network application, failure of a single workstation, or a network printer jam.

NRC Computer Security Incident Response Capability (CSIRC)

NRC's CSIRC is tasked with responding to incidents involving all NRC unclassified computer systems, Internet and intranet servers, and LANs. The team is composed of senior systems administrators and network engineers who are highly skilled and knowledgeable about NRC computer systems and networks. The team can pull in additional technology experts from the OCIO Network Operations Center (NOC), depending on the systems involved and the nature of the incident. The CSIRC, under the direction of the NRC LAN/WAN ISSO, is also responsible for preparing the reports that will be made by the NRC LAN/WAN ISSO to the FedCIRC on security incidents involving unclassified NRC information systems, as authorized and approved by the

SITSO. The CSIRC may provide assistance to the NRC OCIO CSS for incidents involving automated information systems that are handling sensitive information, SGI, or classified information. The CSIRC will provide expert help in all stages of incident handling, including incident detection, containment of any damage that may be caused by an incident, eradication or isolation of the source that may be causing the damage, and recovery from an incident.

Office of the Inspector General (OIG)

Confirmed or suspected wrongdoing related to NRC computers and data and misconduct by NRC employees and contractors shall immediately be reported to OIG. OIG is responsible for conducting any resulting investigation and for contacting and coordinating the response with other law enforcement officials. OIG is responsible for providing approved procedures for the proper collection and maintenance of data for use in potential criminal investigations and prosecutions. Because of the potential for investigative action, OIG will be consulted before any details about information systems security incidents are released to the public.

OCIO Network Operations Center (NOC)

The OCIO NOC is responsible for monitoring the NRC infrastructure throughout the course of a potential security incident and gathering information that may be useful to the investigation and resolution of the incident. The NOC gathers information about potential security incidents and may implement corrective actions under the direction of the NRC LAN/WAN ISSO. If the NOC personnel receive an incident report, or if they suspect that a security incident may be occurring, they will notify the NRC LAN/WAN ISSO immediately and also the NRC CSIRC. If the incident involves NRC AISs that are processing sensitive information, SGI, or classified information, the NOC shall notify both the LAN/WAN ISSO and the SITSO.

NRC Data Center

The NRC Data Center is responsible for monitoring the NRC Data Center operations throughout the course of a potential security incident and gathering information that may be useful to the investigation and resolution of the incident. The Data Center gathers information about potential security incidents and may implement corrective actions under the direction of the NRC LAN/WAN ISSO. If the Data Center personnel receive an incident report, or if they suspect that a security incident may be occurring, they will notify the NRC LAN/WAN ISSO immediately and also the NRC CSIRC. If the incident

involves NRC AISs that are processing sensitive information, SGI, or classified information, the Data Center shall notify both the LAN/WAN ISSO and the SITSO.

NRC Customer Support Center (CSC)

If the NRC CSC (Help Desk) personnel receive an incident report, or if they suspect that a security incident may be occurring, they will notify the NRC LAN/WAN ISSO immediately, and also the NRC NOC and the Data Center. If the incident involves NRC AISs that are processing sensitive information, SGI, or classified information, the CSC shall notify both the LAN/WAN ISSO and the SITSO.

Managers, Supervisors, and Branch Chiefs

Managers, supervisors, and branch chiefs ensure that their employees are made aware of the reporting procedures and the security policies in place to protect NRC information systems, employees, and NRC property. They are responsible for monitoring responses to security incidents involving their employees and ensuring employee compliance with the policies and procedures.

LAN Administrators

LAN Administrators familiar with NRC systems may often be the first to discover a security incident. They are responsible for immediately reporting these incidents to the OCIO NOC and for notifying their program office Information Technology (IT) Coordinator or other senior managers in the program office. They are also responsible for initiating steps to monitor and preserve records of suspected incidents.

System Users

All employees and other systems users are responsible for reporting security incidents. They must notify the CSC Help Desk or the Regional Help Desk (and the Regional ISSO), as appropriate. Upon notification, the Regional Help Desk should notify the CSC Help Desk.

NOTE: Users should report any unusual activity, such as systems that appear to be running slowly, files with dates last modified that may be inaccurate, or new files they do not recognize.

Federal Computer Incident Response Center (FedCIRC)

FedCIRC provides a central point for incident reporting, handling, prevention, and recognition. Its purpose is to ensure that the Government has critical services available in order to withstand or quickly recover from attacks against its information resources. Each agency should designate at least four points of contact with the FedCIRC at the headquarters level. These contacts (a primary and a secondary) should be chosen from both the OCIO or headquarters administrative level to receive high-level communications, and the ISSO or system administrator level to receive more detailed communications. These individuals are responsible for all routine interaction with FedCIRC, including the monthly reporting of intrusion detection data for the agency. FedCIRC also routinely issues advisories and other useful information related to vulnerabilities in commercial software. The NRC points of contact are on the FedCIRC mailing list and interact with FedCIRC for these matters. However, in the case of an actual report by NRC of an intrusion or incident, the SITSO will become the primary point of contact for incident reporting, as displayed in the tables in Section E of this appendix. See Attachment B for information on the NRC FedCIRC Points of Contact.

C. Security Incidents

The term “incident” refers to an event that violates an explicit or an implied NRC security policy. Security incidents are adverse events in an information system and/or network or the threat of the occurrence of such an event. Security incidents may involve suspected viruses, threats to persons, attempted systems intrusions, unauthorized release of Privacy Act information, theft of Government or personal property, unauthorized use of another user's account, unauthorized use of system privileges, unsolicited e-mail spam, and execution of malicious code that destroys data. (Incidents also include any detected during remote access sessions with NRC information systems.)

[REDACTED]

F. Reporting Requirements for Security Incidents

Reporting Information Systems Security Incidents Within NRC

To inform NRC management and personnel involved with the response to computer security incidents, the NRC LAN/WAN ISSO prepares the following reports that summarize information about security incidents. The LAN/WAN ISSO is the POC for all the reports. The following table describes the security incident reporting requirements within NRC.

Table B-2
Reporting Requirements

Frequency	Report Description	Recipients	Security Content
Daily	Infrastructure Status Report	CSC Help Desk NOC SITSO CIO Deputy CIO Director of ITID OIG	Summary statistics for Level 1 and 2 incidents since the previous report. Text description of Level 3 - 5 incidents. Analysis and assessment of statistical anomalies noted at any level.
Weekly	Summary of Daily Security Incident Statistics	CSC Help Desk NOC SITSO CIO Deputy CIO Director of ITID OIG	Summarization of the previous weeks' daily Infrastructure Status Reports.
Monthly	FedCIRC Report	CSC Help Desk NOC SITSO CIO Deputy CIO Director of ITID OIG	Monthly report provided to FedCIRC as described in Section F of this appendix.

Reporting Information Systems Security Incidents to Outside Agencies

All Federal agencies are required to report on information systems security incidents to FedCIRC. These reports are used by FedCIRC to build a Government-wide picture of attacks against Government cyber resources and to aid in developing Government-wide responses to incidents.

The NRC LAN/WAN ISSO develops a monthly report to FedCIRC on incidents at NRC. All five Security Incident Severity Levels are reported to FedCIRC. For Level 3, 4, and 5 security incidents, NRC immediately notifies FedCIRC during the incident to facilitate FedCIRC's responsibility to coordinate interagency responses.

Additional details on the processes and points of contact for external agency reporting are sensitive information and posted on the NRC internal IT security Web site at http://csb.nrc.gov/security/security.asp.

Attachment A
Points of Contact for Reporting Information Systems Security Incidents

NRC Staff Position Observing Possible Information Systems Security Incident	**Report Potential Information Systems Security Incidents to the Following:**	**Contact Information**
System Users	CSC Help Desk or Regional Help Desk	CSC Help Desk Phone: 301-415-1234 E-mail: csc@nrc.gov
CSC Help Desk	OCIO NOC, Data Center, and LAN/WAN ISSO	NOC Phone: 301-415-8150 E-mail: noc@nrc.gov
OCIO NOC	NRC LAN/WAN ISSO, Data Center, and CSIRC Team	ISSO/CSIRC Team
LAN/WAN ISSO	Levels 3, 4, and 5 to • Chief of ITCSB upon confirmation of a security incident • Director of ITID • SITSO • FedCIRC • OIG	Chief of ITCSB Director of ITID SITSO OIG Duty Agent, Page 888-798-7065; the agent may also be reached through NRC Security
SITSO	CIO/DCIO, OEDO, and NRC senior management, as appropriate	CIO DCIO

Attachment B
NRC FedCIRC Points of Contact
(For working-level coordination)

This section refers to personal contact information (such as home phone numbers) and other information that is subject to frequent changes. The complete listing of personal contact information is posted on the NRC internal IT security Web site at *http://csb.nrc.gov/security/security.asp*.

Attachment C
Computer Security Incident Report

The following form should be completed for each computer security incident to which the CSIRC responds.

Date	**Time**	**Location**
Contact Information for person reporting the incident	Name User Id Title Work Phone Home Phone Cellular/Pager FAX E-mail	Internet Protocol (IP) Address(es) of Affected System(s)
Type of Incident	Unclassified system SGI or classified Intrusion Root Compromise Denial of Service Web Site Defacement Virus/Malicious Code User Account Compromise System Misuse Hoax Social Engineering Network Scanning/Probing Other (Specify)	IP Address(es) of Apparent Source(s)

Attachment C (continued)

Date	**Time**	**Location**
Operating System	AIX NT Solaris Linux Compaq TRU64 SGI IRIX Open VMS HP-UX WinNT Macintosh Novell Win2000 Other (Specify)	Describe function of the host
		Estimated number of hosts affected
CSIRC Team Member		

[REDACTED]

Appendix D
Operating System and System Software Maintenance Procedures

Approved: February 1, 1999
(Revised: September 12, 2003)

Contents

Appendix D
Operating System and System Software Maintenance Procedures*

A. Overview

The operating system and other system software provides the software platform on which other programs run by supporting all application and communication processing on a system. Operating systems perform basic tasks such as recognizing input, sending output, keeping track of files and directories, and controlling peripheral devices. For large systems, the operating system manages the programs and users and is responsible for security, ensuring that unauthorized users are not allowed access. System software includes a set of utilities that perform specific functions such as communications, security, and file management.

The Nuclear Regulatory Commission infrastructure includes multiple types and versions of operating systems. In recognition of the potential vulnerabilities that exist when operating system and other system software is not maintained at the most current version and when vendor patches are not installed, the Operating System and System Software Maintenance Procedures were developed. These procedures are applicable to all operating system and system software that is operating on the unclassified NRC local- and wide-area network infrastructure. In order for these procedures to be successful, it is also critical that existing security configuration settings be maintained after an operating and system upgrade or patch installation. Operating and system software upgrades and patch installations shall not be performed until the existing security configuration settings have been verified. The operating and system software security configuration settings shall also be re-verified after the installation of any upgrades or patches. These procedures also include details about NRC's information systems' vulnerability alert and patch dissemination and tracking process.

The vast majority of computer intrusions occur through well-known vulnerabilities. There are no tasks more important in preventing system intrusions than configuring new systems securely and keeping current with vendor security patches. Critical patches

*Note: Because of the dynamic nature of network operations and new threats to information systems, network security procedures are subject to frequent updates. The most current version of the Operating System and System Software Maintenance Procedures are maintained on the internal NRC Web site (http://csb.nrc.gov/security/security.asp).

need to be accomplished in the shortest possible time frame. Baseline security configuration settings and the most recent security patches need to also be considered during the new system build process. Various Government and commercial organizations issue vulnerability alerts and security patches for operating and system software. NRC's vulnerability alert and patch dissemination and tracking process will be closely coordinated with the vulnerability alert and patch dissemination process managed by the Federal Computer Incident Response Center (FedCIRC). **[REDACTED]**

The procedures do not apply to upgrades, maintenance, or replacement of infrastructure hardware.

B. Responsibilities

Office of the Chief Information Officer (OCIO)

The OCIO has overall responsibility for NRC's Automated Information Systems Security Program.

NRC Senior Information Technology Security Officer (SITSO)

The SITSO reports to the NRC CIO. The SITSO provides oversight and guidance for all security issues associated with the Operating System and System Software Maintenance Procedures and for the associated vulnerability alert and patch dissemination and tracking process. The SITSO also serves as the primary point of contact for information systems security matters between the various security officials throughout NRC and also with NRC management, including the CIO and the Office of the Executive Director for Operations (OEDO).

Information System Security Officer (ISSO) for the local- and wide-area network (LAN/WAN), and the Regional ISSOs

The NRC LAN/WAN ISSO provides consultation related to analysis of the security features available within a new version of software or a vendor-supplied patch. The NRC LAN/WAN ISSO notifies Team Leaders about security advisories or security patches as they become available and provides status reporting to NRC senior management. The NRC LAN/WAN ISSO manages the NRC vulnerability alert and patch dissemination and tracking process from day to day. The Regional ISSOs work

closely with the LAN/WAN ISSO to help coordinate and manage the regional implementation of these procedures.

Information Technology Infrastructure Division (ITID)

ITID is responsible for maintaining an accurate inventory of all NRC system software, including software version, current security configuration settings, and patches that have been installed. ITID will provide a periodic vulnerability patch status report to the SITSO. This report will list all patches and alerts that have been issued and will describe impacts to the NRC system(s). ITID will also track patch installation status and provide periodic summaries verifying which systems have/have not installed the prescribed patch. ITID has overall responsibility for the operation and maintenance of the LAN/WAN infrastructure.

OCIO Network Operations Configuration Control Board (Ops CCB)

The OCIO Network Ops CCB is responsible for reviewing Technical Change Requests (TCRs) for the ITID Information Technology Customer Services Branch (ITCSB). A TCR is initiated for any changes to the NRC unclassified information systems infrastructure, including upgrading, patching, or reconfiguring system software for all network segments. The TCR process includes maintenance activities for the desktop platform and servers that support it. The Ops CCB meets weekly to review and approve TCRs. The Ops CCB provides support to the LAN/WAN ISSO and to ITID senior leadership to assist in the management of the NRC vulnerability alert and patch dissemination and tracking process.

Team Leaders

Team Leaders are responsible for the overall implementation and maintenance of specific systems. Tasks related to operating and system software maintenance include the following:

- Disseminating information about patches, including security patches
- Planning software configuration and integration for software upgrades or new software introduced
- Developing and maintaining baseline configurations for operating and system software

- Reporting inventory and configuration updates for which they are responsible to the Ops CCB and to the NRC LAN/WAN ISSO (and in the regions, to the Regional ISSOs).

System Administrators

The System Administrator is responsible for maintaining servers and the system software running on them. The System Administrator performs several critical tasks related to system software maintenance, including the following:

- Communicating with software vendors and NRC users regarding changes to system software
- Identifying available upgrades
- Identifying changes in the application or hardware environment that may necessitate changes to the underlying system software platform
- Analyzing the features available in new software versions or patches and determining how the features may impact operations
- Testing new software versions or patches
- Scheduling installation of new software versions or patches and submitting the proposed installation to Ops CCB
- Troubleshooting and ongoing oversight for system software
- Maintaining the inventory of system software and hardware
- Confirming receipt of and responding to advisories issued by the NRC LAN/WAN ISSO
- Confirming the most recent security configuration of any operating and system software prior to, and after, any upgrades or patch installations. This action will ensure that systems remain hardened as changes and upgrades occur

- Reporting the successful completion of all operating and system software upgrades and patches (including vulnerability patches) to the Ops CCB and the NRC LAN/WAN ISSO (and in the regions, to the Regional ISSOs)

C. Operating System and System Software Maintenance

- Corrective maintenance includes maintaining control over day-to-day operations to ensure that systems remain available to users

- Adaptive maintenance includes controlling modifications made to either the system software, applications, or hardware

- Preventive maintenance includes activities that mitigate weaknesses or maximize system performance

D. The Operating System and System Software Change Control Process (Change Control Process)

The Change Control Process for all NRC unclassified information systems consists of the following series of steps that are designed to ensure that all appropriate maintenance actions are taken in a safe and timely manner.

1. Inventory all system software and document the following information:

- Software installed and date installed

- Vendor and vendor contact information

- Version and patch installed

- Most recent security configuration (hardening)

- Server(s) or hosts on which software is deployed

- Application or other system software dependencies

- Configuration parameters and standard operating procedures

- Specific software versions installed that are no longer supported by their vendor

Maintaining an accurate listing of installed software, current security configuration, and a description of how the software is integrated with other systems supports the stability of the system. As maintenance actions are undertaken, the inventory should be updated to reflect the changes.

2. Identify the most current version and patch available for each type of system software. The NRC LAN/WAN ISSO issues advisories about new patches to the Team Leaders who evaluate them and distribute as appropriate to System Administrators. However, System Administrators should not rely solely on vendor or ISSO notification to identify when a new version or patch is available for a software product.

3. Analyze the features available in the latest software version or patch to determine if the features correct a flaw in the software, improve security, enhance performance or operability, or alter the functionality of the system. Consultation with the ISSO, the Applications Development Division (ADD), or other specialists may be required to completely develop the full impact of certain features. Analysis should address the two critical aspects of system stability and security.

4. Analyze and prioritize updates that should be made to the operating system or other system software. After the impact analysis is complete, determine which upgrades or updates to the system software are required. If a new version of the software or a patch is determined to have a detrimental impact on the operating environment or to be technically infeasible, prepare a written justification that describes the circumstances that do not allow implementation of a new software version or patch and forward it to the NRC LAN/WAN ISSO (and in the regions, to the Regional ISSOs) for review.

5. For maintenance upgrades that are to be made, install and test the new software version or patch in a test environment, if possible. Once installed, the upgrade should be fully tested with the application(s) that depend(s) on the software to ensure that the functionality is not compromised.

6. Once tested, schedule and obtain approval from Ops CCB to deploy the software upgrade to all servers and update operating procedures and contingency planning procedures as necessary. The hardened security configuration of system software shall always be maintained and verified.

7. Update the software inventory for the deployed software upgrade. Report the successful completion of all operating and system software upgrades and patch

installations to the Ops CCB and the NRC LAN/WAN ISSO (and in the regions, to the Regional ISSOs).

Attachment A
Operating System and System Software Inventory Form

The purpose of this Inventory Form is to document the operating and other system software installed within the NRC technology environment. This Inventory Form should be completed for all operating and system software at least annually, when a vulnerability patch is installed and whenever an update is made to a software system. This form should be completed by the System Administrator responsible for maintaining the system. OCIO/ITID is responsible for maintaining the inventory for all operating system and system software in the NRC infrastructure. If this form is completed in connection with an update or other maintenance activity, it should be submitted to the OCIO Operations Configuration Control Board with the Technical Change Request. If this form is completed as part of the annual inventory of operating and system software, a copy should be forwarded to the NRC local-area network/wide-area network (LAN/WAN) Information System Security Officer (ISSO) (and in the regions, to the Regional ISSOs). This form may also be used to supplement (or as an attachment) to the system inventory update forms specified for use with the NRC systems development and life cycle management methodology (SDLCMM).

Host Name:	
Host Function:	
Internet Protocol (IP) Address(es):	
Internetwork Packet Exchange (IPX) Address(es):	
Software Name:	
Version Number:	
Vendor:	

Attachment A (continued)

Is the latest version of software installed, to include verification of the security configuration re-hardening of the software?	Yes No	
If no, explain:		
If software maintenance activity provide:	Description of activity:	
	Version/patch implemented:	
	Implementation schedule:	
	Date testing completed:	
	Is update serial:	Yes No
	If no, explain:	
	Technical Change Request (TCR) number:	
System Administrator Signature:		

Appendix E
Abbreviations

Approved: February 1, 1999
(Revised: September 12, 2003)

Appendix E
Abbreviations

ACL access control list
ADD Applications Development Division (OCIO)
ADM Office of Administration
ADP automatic data processing
AEA Atomic Energy Act of 1954, as amended
AIS automated information system (used synonymously with information system [IS])

BIA business impact analysis

C&A certification & accreditation
CIO Chief Information Officer
CNSS Committee on National Security Systems
COTS commercial off-the-shelf
CPIC Capital Planning and Investment Control
CPU central processing unit
CSC Customer Service Center
CSIRC Computer Security Incident Response Capability
CSS Computer Security Staff (OCIO)

DAA Designated Accrediting Authority
DAC discretionary access control
DBMS database management system
DC Division of Contracts (ADM)
DES data encryption standard
DFS Division of Facilities and Security (ADM)
DNS domain name server
DOE Department of Energy
DOS disk operating system

Abbreviations (continued)

FedCIRC Federal Computer Incident Response Center
FIPS Federal Information Processing Standard
FTP file transfer protocol

GSA General Services Administration
GSS General Support System

HR Office of Human Resources
HTTP hypertext transfer protocol

I&A identification & authentication
IDS Intrusion Detection System
IP Internet protocol
IS information system
ISDN integrated services digital network
ISP Internet Service Provider
ISSO Information System Security Officer
IT information technology
IT CSB Information Technology Customer Services Branch (OCIO)
ITID Information Technology Infrastructure Division (OCIO)

LAN local-area network

MA Major Application
MD management directive

NFS network file system
NIH National Institutes of Health
NIS network information service
NIST National Institute of Standards and Technology
NISTIR National Institute of Standards and Technology Internal Report
NNTP network news transfer protocol
NOC Network Operations Center
NSA National Security Agency

Abbreviations (continued)

NSIR Office of Nuclear Security and Incident Response
NSTISSC National Security Telecommunications and Information Systems Security Committee

OCIO Office of the Chief Information Officer
OEDO Office of the Executive Director for Operations
OIG Office of the Inspector General
OMB Office of Management and Budget
OPA Office of Public Affairs
OppsCCB Operations Configuration Control Board

PC personal computer
PGP "Pretty Good Privacy"
PIN personal identification number
POC point of contact
PPP point-to-point protocol

RIP routing information protocol
RPC remote procedure call

SCIF Sensitive Compartmented Information Facility
SDLCMM System Development Life Cycle Management Methodology
SGI Safeguards Information
SISS Subcommittee for Information Systems Security
SITSO Senior Information Technology Security Officer
SLIP serial line Internet protocol
SMTP simple mail transfer protocol
SSP System Security Plan

TCP transmission control protocol
TCR Technical Change Request
TFTP trivial file transfer protocol

Abbreviations (continued)

UDP user datagram protocol
User ID user identification
UUCP UNIX-to-UNIX copy program

VPN Virtual Private Network

WAN wide-area network
WWW World Wide Web

Appendix F
Information Technology Security References

Approved: February 1, 1999
(Revised: September 12, 2003)

Appendix F
Information Technology Security References

National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) (available at http://csrc.nist.gov).

FIPS Publication 31, “Guidelines for Automatic Data Processing Physical Security and Risk Management,” June 1974.

FIPS Publication 46-3, "Data Encryption Standard (DES)," October 1999.

FIPS Publication 48, “Guidelines on Evaluation of Techniques for Automated Personal Identification,” April 1977.

FIPS Publication 73, “Guidelines for Security of Computer Applications,” June 1980.

FIPS Publication 74, “Guidelines for Implementing and Using the NBS Data Encryption Standard,” Three parts, April 1981.

FIPS Publication 81, “DES Modes of Operation,” December 1980.

FIPS Publication 83, “Guideline on User Authentication Techniques for Computer Network Access Control,” September 1980.

FIPS Publication 87, "Guidelines for ADP Contingency Planning," March 27, 1981.

FIPS Publication 102, "Guidelines for Computer Security Certification and Accreditation," September 27, 1983.

FIPS Publication 112, "Password Usage," Two parts, May 30, 1985.

FIPS Publication 113, “Computer Data Authentication,” May 1985.

FIPS Publication 140-1, “Security Requirements for Cryptographic Modules,” January 1994.

FIPS Publication 140-2, “Security Requirements for Cryptographic Modules,” June 2001.

Information Technology Security References (continued)

FIPS Publication 171, “Key Management Using ANSI X9.17,” April 1992.

FIPS Publication 180-2, “Secure Hash Standard,” August 2002.

FIPS Publication 181, “Automated Password Generator,” October 1993.

FIPS Publication 185, “Escrowed Encryption Standard,” February 1994.

FIPS Publication 186-2, “Digital Signature Standard (DSS),” January 2000.

FIPS Publication 188, “Standard Security Labels for Information Transfer,” September 1994.

FIPS Publication 190, “Guideline for the Use of Advanced Authentication Technology Alternatives,” September 1994.

FIPS Publication 191, “Guideline for the Analysis of Local Area Network Security,” November 1994.

FIPS Publication 196, “Entity Authentication Using Public Key Cryptography,” February 1997.

FIPS Publication 197, “Advanced Encryption Standard,” November 2001.

FIPS Publication 198, “The Keyed-Hash Message Authentication Code (HMAC),” March 2002.

National Institute of Standards and Technology (NIST), Special Publications (available at http://csrc.nist.gov)

Special Publication 800-2, “Public-Key Cryptography,” April 1991.

Special Publication 800-3, “Establishing a Computer Security Incident Response Capability (CSIRC),” November 1991.

Information Technology Security References (continued)

Special Publication 800-4, "Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials," March 1992.

Special Publication 800-5, “A Guide to the Selection of Anti-Virus Tools and Techniques,” December 1992.

Special Publication 800-6, “Automated Tools for Testing Computer System Vulnerability,” December 1992.

Special Publication 800-7, “Security in Open Systems,” July 1994.

Special Publication 800-8, “Security Issues in the Database Language SQL,” August 1993.

Special Publication 800-9, “Good Security Practices for Electronic Commerce, Including Electronic Data Interchange,” December 1993.

Special Publication 800-10, “Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,” December 1994.

Special Publication 800-11, “The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security,” February 1995.

Special Publication 800-12, “An Introduction to Computer Security: The NIST Handbook,” October 1995.

Special Publication 800-13, “Telecommunications Security Guidelines for Telecommunications Management Network,” October 1995.

Special Publication 800-14, “Generally Accepted Principles and Practices for Securing Information Technology Systems,” September 1996.

Special Publication 800-15, “Minimum Interoperability Specification for PKI Components (MISPC), Version 1,” January 1998.

Information Technology Security References (continued)

Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (supersedes NIST Spec. Pub. 500-172), April 1998.

Special Publication 800-17, "Modes of Operation Validation System (MOVS): Requirements and Procedures," February 1998.

Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," December 1998.

Special Publication 800-19, "Mobile Agent Security," October 1999.

Special Publication 800-20, "Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures," revised April 2000.

Special Publication 800-21, "Guideline for Implementing Cryptography in the Federal Government," November 1999.

Special Publication 800-22, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," October 2000.

Special Publication 800-23, "Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products," August 2000.

Special Publication 800-25, "Federal Agency Use of Public Key Technology for Digital Signatures and Authentication," October 2000.

Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," November 2001.

Special Publication 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," June 2001.

Special Publication 800-28, "Guidelines on Active Content and Mobile Code, October 2001.

Information Technology Security References (continued)

Special Publication 800-29, "A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2," June 2001.

Special Publication 800-30, "Risk Management Guide for Information Technology Systems," January 2002.

Special Publication 800-31, "Intrusion Detection Systems (IDS)," November 2001.

Special Publication 800-32, "Introduction to Public Key Technology and the Federal PKI Infrastructure," February 2001.

Special Publication 800-33, "Underlying Technical Models for Information Technology Security," December 2001.

Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002.

Special Publication 800-37, "Guidelines for the Certification and Accreditation of Federal Information Technology Systems," October 2002 (Draft).

Special Publication 800-38A, "Recommendation for Block Cipher Modes of Operation - Methods and Techniques," December 2001.

Special Publication 800-40, "Procedures for Handling Security Patches," September 2002.

Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy," January 2002.

Special Publication 800-46, "Security for Telecommuting and Broadband Communications," September 2002.

Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems," September 2002.

Information Technology Security References (continued)

Special Publication 800-48, “Wireless Network Security: 802.11, Bluetooth, and Handheld Devices,” November 2002.

Special Publication 800-51, “Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme,” September 2002.

Special Publication 500-120, “Security of Personal Computer Systems - A Management Guide,” January 1985.

Special Publication 500-133, “Technology Assessment: Methods for Measuring the Level of Computer Security,” October 1985.

Special Publication 500-134, “Guide on Selecting ADP Backup Process Alternatives,” November 1985.

Special Publication 500-153, “Guide to Auditing for Controls and Security: A System Development Life Cycle Approach,” April 1988.

Special Publication 500-156, “Message Authentication Code (MAC) Validation System: Requirements and Procedures,” May 1988.

Special Publication 500-157, “Smart Card Technology: New Methods for Computer Access Control,” September 1988.

Special Publication 500-166, “Computer Viruses and Related Threats: A Management Guide,” August 1989.

Special Publication 500-169, “Executive Guide to the Protection of Information Resources,” 1989.

Special Publication 500-170, “Management Guide to the Protection of Information Resources,” 1989.

Special Publication 500-171, “Computer Users' Guide to the Protection of Information Resources,” 1989.

Information Technology Security References (continued)

Special Publication 500-174, “Guide for Selecting Automated Risk Analysis Tools,” October 1989.

Special Publication 500-189, “Security in ISDN,” September 1991.

Appendix G
Glossary

Approved: February 1, 1999
(Revised: September 12, 2003)

Appendix G
Glossary

Acceptable risk. A concern that is acceptable to responsible management due to the cost and magnitude of implementing countermeasures.

Access. The ability and the means necessary to approach, to store or retrieve data, to communicate with, or to make use of any resource of an automatic data processing (ADP) system.

Access control. The process of limiting access to the resources of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks).

Access control list (ACL). A discretionary access control mechanism that implements an access control matrix by representing the columns as lists of users attached to the protected objects.

Access privilege. The particular access permission (i.e., read, write, append, execute, delete, create, modify) granted to a subject in relation to an object.

Accountability. The quality or state that enables violations or attempted violations of ADP system security to be traced to individuals who may then be held responsible.

Accreditation. A formal declaration of the accrediting authority that an automated information system (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the accrediting authority and shows that due care has been taken for security.

Adequate security. Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

Glossary (continued)

Application. The use of information resources (information and information technology) to satisfy a specific set of user requirements.

Application software. A set of computer instructions designed to achieve a specified objective such as payroll, accounting, or management analysis. Application software may consist of operating system instructions or any programming language.

Application system. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures (automated or manual) to achieve a specific objective or function.

Assurance. A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. Adequately met includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass.

Audit trail. A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in the path of a transaction from its inception to the output of final results.

Authentication. (1) The act of identifying or verifying the eligibility of a station, an originator, or an individual to access specific categories of information; (2) a measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, a message, a station, or an originator.

Authenticity. The validity of the identity of an automated information system user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an automated information system.

Authorization. The granting of access rights to users, processes, or programs.

Automated information system (AIS). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Glossary (continued)

Automated information system (AIS) facility. One or more rooms (e.g., Two White Flint Computer Room, local-area network [LAN] equipment rooms), generally contiguous, containing the elements of an AIS.

Automated information system (AIS) security. Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AIS and data. AIS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS.

Availability. A state in which AIS resources are in the place needed by the user at the time the user needs them, and in the form needed by the user.

Backup. (1) A copy of a program or data file that is kept for reference in case the original is lost or destroyed; (2) reserve computing capability available in case of equipment malfunction, destruction, or overload.

Capital Planning and Investment Control (CPIC) Process. A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution and is focused on agency missions and achieving specific program outcomes.

Certification. The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Chief Information Officer (CIO). The NRC management official who is responsible for planning, directing, and overseeing the delivery of centralized information technology infrastructure, applications, and information management services, and the development and implementation of plans, architecture, and policies to support the mission, goals, and priorities of the agency.

Glossary (continued)

Computer security (i.e., network security, information systems security). The "cost-effective protection" of sensitive automated information from unauthorized disclosure, modification, misuse, loss, or denial of service.

Computer Security Staff (CSS) personnel. Computer security personnel are Office of the Chief Information Officer (OCIO) personnel located in the Computer Security Staff (CSS) who are responsible for the security of all AIS at NRC. Their primary responsibility is to enforce the NRC AIS security program.

Confidentiality. The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

Configuration management. The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the development and operational life of the system.

Contingency plan. A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with "Disaster Recovery Plan."

Cost-effective protection. The safeguards for a system are reasonably proportionate to the estimated risks (i.e., the potential harm or loss).

Countermeasure. Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system. Synonymous with "Safeguards."

Criticality. The importance of an asset or system to an organization. The level of criticality is determined by the organization's need for asset/system availability, integrity, and confidentiality. The level of criticality is directly related to the level of security protection required.

Data. Programs, files, or other information stored in, or processed by, a computer system.

Glossary (continued)

Data encryption standard (DES). A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and Government use.

Data integrity. The property that data meet a prior expectation of quality. See also "system Integrity."

Degausser. An electrical device that can generate a magnetic field for the purpose of degaussing magnetic storage media.

Denial of service. Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

Designated accrediting authority (DAA). The senior management official who has the authority to decide on accepting the adequacy of the security safeguards prescribed for an AIS. That official is responsible for issuing an accreditation statement that records the formal management "approval to operate" decision to accept those safeguards based on a reasonable assessment of the risks, and how effectively the safeguards mitigate the risks. The DAA is the senior management official who has the authority to authorize processing (accredit) an AIS (Major Application or General Support System) and accept the risk associated with the system.

Destruction. The physical alteration of ADP system media or ADP system components such that they can no longer be used for storage or retrieval of information.

Dial-up. The service whereby a computer workstation can use the telephone to initiate and effect communication with a computer.

Disaster Recovery Plan. Synonymous with "contingency plan."

Discretionary access control (DAC). A means of restricting access to objects based on the identity and need-to-know of the user, process, and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Glossary (continued)

Domain. The unique context (e.g., access control parameters) in which a program is operating; in effect, the set of objects that a subject has the ability to access.

Electronic signature. A method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message; indicates such person's approval of the information contained in the electronic message (GPEA, Section 1709(1)).

Encryption. The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process.

Enterprise architecture (EA). An EA is the explicit description and documentation of the current and desired relationships among business and management processes and information technology (IT). It describes the “current architecture” and “target architecture,” including the rules and standards and systems life cycle information to optimize and maintain the environment that the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's Capital Planning and Investment Control processes, agency EA planning processes, and agency systems life cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with the Government Paperwork Elimination Act, end user satisfaction, and IT security.

Environment. The aggregate of external procedures, conditions, and objects that affects the development, operation, and maintenance of a system.

General Support System. An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local-area network (LAN), including smart terminals that support a branch office; an agencywide backbone; a communications network; a departmental data processing center, including its operating system and utilities; a tactical radio network; or a shared information processing service organization.

Glossary (continued)

Hard copy. Information that is printed on paper, slides, microfilm, or photographs. Does not involve storage on magnetic media.

Identification. The process that enables recognition of an entity (user or process) by a system, generally by the use of unique machine-readable user names.

Identification and authentication (I&A). The combination of a process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names (identification) and the verification of the identity of a user, a device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system (authentication).

Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information management. The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

Information resources. Includes both Government information and information technology.

Information resources management. The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

Information security. Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (2) confidentiality, which means preserving authorized restrictions on access and disclosure, including the means for protecting personal privacy and proprietary information; and (3) availability, which means ensuring timely and reliable access to and use of information.

Glossary (continued)

Information system. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

Information technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. Equipment is used by an executive agency if it is used directly or is used by a contractor under a contract with the executive agency that (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

Integrity. Sound, unimpaired, or perfect condition. The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data have when they have not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

Label. See "sensitivity label."

Labeling. A piece of information that represents the security level of an object and that describes the sensitivity of the information in the object.

Least privilege. The principle that requires that each subject (i.e., user or process) be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Glossary (continued)

Local-area network (LAN). An interconnected group of office automation systems or system components that are physically located within a small geographic area, such as a building or a campus.

Logon. The procedure used to establish the identity of the user and the levels of authorization and access permitted.

Magnetic media. Any data storage medium and related technology, including diskettes and tapes, in which different patterns of magnetization are used to represent the values of stored bits or bytes.

Major Application. An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Major information system. An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Malicious code. Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose (e.g., Trojan horse).

National security system. Any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to include administrative and business applications (such as payroll, finance, logistics, and personnel management applications).

Glossary (continued)

Need-to-know. The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

Nonrepudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

Object. A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Office Information Technology (IT) Coordinator. The Office IT Coordinator is the individual appointed by the office director to coordinate all aspects of data processing for the respective office with OCIO. The coordinator will usually help the ISSOs to determine computer security requirements for their respective offices and provide other advice. The coordinator should approve users' requests for additional facility access (NRC Form 380) and system upgrades and software. The coordinator may also perform other duties regarding virus checking and computer security awareness.

Optical storage media. Media that uses a source of coherent light—usually a semiconductor laser—to read and write the data, usually to an optical disk.

Password. A protected word or string of characters that identifies or authenticates a user, a specific resource, or an access type.

Permissions. A description of the type of authorized interactions a subnet can have with an object. Examples include read, write, execute, add, modify, and delete.

Personnel security. The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.

Physical security. The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

Glossary (continued)

Privileged instructions. A set of instructions (e.g., interrupt handling or special computer instructions) to control features (such as storage protection features) that are generally executable only when the automated system is operating in the executive state.

Privileges. A set of authorizations/permissions granted by an authorized officer to an AIS user to perform certain operations.

Process. A program in execution.

Read. A fundamental operation that results only in the flow of information from an object to a subject.

Records. All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included (44 U.S.C. 3301).

Records management. The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations (44 U.S.C. 2901(2)).

Reliability. The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions.

Remnants. The residual magnetism that remains on magnetic storage media after degaussing. Can also mean any data remaining on ADP storage media after removal of the power.

Glossary (continued)

Remote access. Sending and receiving data to and from a computer or controlling a computer with workstations or personal computers connected through communications (e.g., telephone line).

Risk. The probability that a particular threat will exploit a particular vulnerability of the system. IT-related risk is the net mission impact considering (1) the probability that a particular threat source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to unauthorized (malicious or accidental) disclosure, modification, or destruction of information; unintentional errors and omissions; IT disruptions due to natural or man-made disasters; and failure to exercise due care and diligence in the implementation and operation of the IT system.

Risk analyses. The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analyses are part of risk management. The two general categories of risk analyses are *quantitative* (estimating risks in terms of dollar losses) and *qualitative* (empirical estimates of risk, e.g., high, medium, low).

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.”

Risk management. The total process of identifying, controlling, and mitigating information system related risks. It includes risk assessment, cost-benefit analysis, and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Safeguards. The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include, but are not necessarily limited to, hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

Glossary (continued)

Security measure. Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications.

Security policy. The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security specifications. A detailed description of the safeguards required to protect a system.

Sensitive application. An application that requires a degree of protection because it processes sensitive data (i.e., administrative, personnel, financial, or national security data) or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation.

Sensitive Compartmented Information Facility (SCIF). An accredited area, room, group of rooms, or installation in which Sensitive Compartmented Information (SCI) may be stored, used, discussed, and/or processed.

Sensitive information. A generic term used to identify information designated as classified, sensitive unclassified, or unclassified Safeguards Information (SGI). Sensitive information also refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information the improper use or disclosure of which could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

Sensitive system. A system or network that stores or processes sensitive information.

Sensitive unclassified information. Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, *United States Code* (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Glossary (continued)

Sensitivity label. The physical representation of the sensitivity level of information.

Sensitivity level. A designation associated with information that indicates (1) the amount of harm that can be caused by the exposure of that information to an unauthorized user, (2) any formal access approvals that should be granted before the granting of access to that information, and (3) any specific handling restrictions placed on that information.

Separation of duties. Assigning to separate individuals key duties such as authorizing, approving, and recording transactions, issuing or receiving assets, making payments, and reviewing or auditing to minimize the risk of loss. Internal control depends largely on the elimination of opportunities to conceal errors or irregularities. This elimination of opportunities, in turn, depends on the assignment of work so that no one individual controls all phases of an activity or transaction thereby creating a situation that permits errors or irregularities to go undetected.

Smart card. A plastic card the size of a credit card containing an embedded integrated circuit or a chip that can generate, store, and/or process data. It can be used to facilitate various authentication technologies also embedded on the same card.

Software security. General purpose (executive, utility, or software development tools) and applications programs or routines that protect data handled by a system.

Subject. An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

System administrator. That person responsible for the installation, operation, maintenance, and performance of a LAN or a WAN.

System Development Life Cycle Management Methodology (SDLCMM). The SDLCMM, as detailed in NRC Management Directive 2.5, “System Development Life Cycle Management Methodology (SDLCMM),” is a structured approach to designing, developing, deploying, maintaining, and decommissioning information systems. It addresses all aspects of an information system’s solution from beginning to end. It allows, and even encourages, flexibility within a clearly defined structure.

Glossary (continued)

System integrity. The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. See also "data integrity."

System Security Plan (SSP). The Office of Management and Budget formatted document that identifies the system components, the sensitivity and risks, and the detailed, cost-effective safeguards to protect the system.

Telecommunications security. The protection that ensures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons information of value that might be derived from the acquisition of telecommunications. Telecommunications security includes crypto-security, transmission security, emission security, and physical security of communications security material and information.

Threat. Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

Trojan horse. A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security, for example, making a "blind copy" of a sensitive file for the creator of the Trojan horse program. See also "malicious code."

Unclassified Safeguards Information (SGI). Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material; or security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

User. A person or process accessing an AIS either by direct connections (i.e., via workstations) or indirect connections (i.e., prepare input data or receive output).

User ID (identifier). A unique symbol or character string that is used by a system to identify a specific user.

Glossary (continued)

Virus. A self-propagating Trojan horse composed of a mission component, a trigger component, and a self-propagating component. See also “malicious code.”

Vulnerability. A weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

Wide-area network (WAN). A collection of computing and communications devices, including local-area networks, connected via a variety of transmission media, including telephone lines and other public networks, across a broad geographic area.