1. INTRODUCTION

1.1 Purpose

The *Risk Assessment Procedures* are intended to provide information to the Department of Education (Department) information technology (IT) security professionals (e.g., computer security officers [CSO], system security officers [SSO], network security officers [NSO]) responsible for the security of the Department's general support systems (GSS) and major applications (MA) and the risk analysis of those GSSs and MAs. These procedures are written with the assumption that the reader has some basic knowledge of IT security and the associated disciplines as described by the National Institute of Standards and Technology (NIST). The procedures outline a systematic, flexible, step-by-step approach that can be implemented consistently across the Department. It establishes the parameters and minimum standards required for a Department risk assessment as in accordance with Office of Management and Budget (OMB) Circular A-130, and NIST Special Publication (SP) 800-30. These procedures may be used by a system owner to: 1) perform risk assessments during all stages of the system's life cycle; 2) provide guidance to contractors responsible for developing a system in preparation for an independent risk assessment; and/or 3) understand the risk assessment reports performed by the independent risk assessor.

1.2 Background

Risk is a measure of the degree to which information resources are exposed based on the exploitation of a *vulnerability* by a potential *threat*[1]. Risk is composed of two elements: 1) the **impact** that an exploited vulnerability would have on the organization's mission or operations; and 2) the **likelihood** that such an exploitation would occur. A *risk assessment* is the process of analyzing and then interpreting risk associated with potential threats and vulnerabilities. The risk assessment acts as a means to help evaluate the effectiveness of various security controls in place for each GSS or MA[2].

The *Department of Education Information Technology Security Risk Assessment Procedures* is written to support the Department's risk management based *Department of Education Information Technology Security Policy*, which states that risk assessments must be performed atleast every three years or whenever a significant change occurs to the GSS or MA.

1.3 Scope

The scope of these procedures includes what a risk assessment is, why a risk assessment is important, how a risk assessment feeds into the certification and accreditation (C&A) process, and the minimal security requirements for conducting a risk assessment. These procedures are based upon the *Department of Education Information Technology Security Policy*, *Departmentof Education Information Technology Security Program Management Plan*, NIST SP 800-30, OMB Circular A-130, and other applicable Federal IT security laws and regulations. The process documented in these procedures will be used in performing risk assessments for all GSSs and MAs throughout the Department[3].

1.4 Structure

These procedures are organized into three major sections.

- Section 1 introduces the risk assessment process.
- Section 2 provides an overview of the major risk assessment concepts as well as how the risk assessment is related to the C&A process.
- Section 3 describes how to conduct a complete and thorough risk assessment (characterize the system, identify threats, identify vulnerabilities, analyze risk,recommend remediation measures, and document results).

Supporting the procedures are nine appendices; these appendices provide useful references (e.g., glossary of terms, acronyms, references, baseline security requirements (BLSRs), points ofcontact, vulnerability questionnaire, system disposal checklist, risk assessment report format, andrisk assessment security action plan letter templates).

2. RISK ASSESSMENT CONCEPTS

2.1 Why Conduct a Risk Assessment?

The *Department of Education Information Technology Security Policy* requires risk assessments be performed on all GSSs and MAs. The purpose of the risk assessment is to quantify the impact of potential threats on a particular vulnerability to a GSS or MA. The benefits of performing a risk assessment include—

- Identifying GSS or MA weaknesses
- Enabling management to make informed decisions regarding implementation of security controls and remediation measures
- Promoting a consistent approach to measuring risk
- Allowing stakeholders to place values on potential losses
- Prioritizing levels of risk based on mission criticality and information sensitivity.

2.2 When Should a Risk Assessment be Conducted?

According to Federal regulations, Principal Officers are required to conduct a risk assessment of all GSSs or MAs at least every 3 years or when there is a major change in the GSS or MA environment, whichever occurs first. Ideally, some form of risk assessment must be performed during each phase of the system development lifecycle (SDLC)[4]. The phase of the SDLC during which the risk assessment is performed determines the level of detail, availability, and sometimes the sources of data. For example, the Baseline Security Requirements, in Appendix D, must be used as a checklist when performing a risk assessment for a GSS or MA in Phase 1 ofthe SDLC. Note that the System Disposal Checklist, in Appendix F must be utilized to ensure necessary steps have been taken to dispose of the GSS or MA. Table 1 describes the Department's SDLC phases and related risk assessment activities.

Table 1. SDLC Phases and Related Risk Assessment Activities

SDLC Phase	Risk Assessment Activity
Phase 1 – Project Initiation	Risks are identified to ensure security controls are being considered and will be built into the GSS or MA. Conduct a high-level risk assessment using the BLSRs in Appendix D as a checklist to ensure security controls are being considered and will be built into the GSS or MA.
Phase 2 – Requirements Specification	The risks identified during this phase are used to support the development of the systems requirements, including security requirements.
Phase 3 – Design	The risks identified during this phase can be used to support the security analyses of the GSS or MA that may lead to architecture and design trade-offs during the design phase. A GSS or MA Inventory submission form must be submitted to the Office of the Chief Information Officer (OCIO) during this phase. This will assess the anticipated mission criticality and information sensitivity of the system.

SDLC Phase	Risk Assessment Activity
Phase 4 – Build	Examination of the requirements specification phase is performed to ensure that the business case, project plan, and risk management plan are followed.
Phase 5 – Test	Decisions regarding risks identified must be made prior to deployment. During this phase, and before the next phase of deployment, an independent risk assessment that meets the minimum standards of this procedures must be performed.
Phase 6 – Deploy	The risk management process supports the assessment of the GSS or MA implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system maintenance.
Phase 7 – Maintain	It is good practice to perform a risk assessment during the maintenance of the GSS or MA—in anticipation of the occurrence of an event or even after the occurrence of an event—to analyze vulnerabilities and recommend remediation measures.
Phase 8 – Disposal	Risk management activities are performed for GSS or MA components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that migration is conducted in a secure and systematic manner.

2.3 How is the Required Level of Effort for a Risk Assessment Determined?

Department automated information resources[5] (GSSs and applications) are categorized into one of five certification tiers (e.g., Tier 0 through Tier 4) as listed in Table 2. The certification tier ofthe GSS or MA determines the level of effort required for conducting risk assessments. Mission criticality and information sensitivity are two attributes used to determine the certification tier[6]. Note: A GSS or MA that is determined to be a Mission-Essential Infrastructure (MEI) Asset through the Critical Infrastructure Protection Survey is automatically considered a Tier 4 system.

For example, a risk assessment for a Tier 4 GSS or MA will consist of a fully documented, formal analysis, using the BLSRs and any additional system specific security requirements. In addition, vulnerability scanning is required as part of the risk assessment for a Tier 4 GSS or MA. However, a risk assessment for a Tier 1 system will consist of using the BLSRs as a checklist and a less detailed, documented analysis.

2.3.1 What if the GSS or Application is Categorized as a Tier 0?

Applications that are categorized as a Tier 0 are not considered MAs and therefore, do not require risk assessments. However, all GSSs are required to undergo a risk assessment, those that are categorized as a Tier 0 will utilize the level of effort associated with a Tier 1 GSS.

Table 2. Required Level of Effort for Risk Assessment

Certification Tier	**Required Level of Effort for Risk Assessment**
0	No risk assessment required
1	Risk assessment (using BLSRs as a checklist)
2	Risk assessment (using BLSRs + additional system specific security requirements)
3	Risk assessment (using BLSRs + additional system specific security requirements + vulnerability scanning recommended)
4	Risk assessment (using BLSRs + additional system specific security requirements + vulnerability scanning)

2.4 How does the Risk Assessment Feed into the C&A Process?

The C&A process is comprised of the following four phases:

- Phase 1: Definition
- Phase 2: Verification
- Phase 3: Validation
- Phase 4: Post Accreditation

Risk assessments are performed as part of Phase 1[7]. The risk assessment is the foundation for developing all other security documents needed for certifying and accrediting the GSS and MA. The System Security Plan (SSP) must adequately address risks identified in the GSS or MA risk assessment report. The Configuration Management Plan (CMP) and the Contingency Plan (CP) further mitigate risks determined during the assessment. The Security Testing and Evaluation (ST&E) procedures will verify that critical risks highlighted in the risk assessment report have been corrected.

The result of the risk assessment yields an overall level of risk for the system. When using a qualitative methodology, risk values are rated as *high*, *medium*, or *low*. These results and other certification documentation are included as part of the C&A documentation provided to the Certifier[8]. Table 3 provides descriptions for each of these values. The risk level descriptions must be used consistently throughout the Department, resulting in a standardized approach to identifying risk levels.

Table 3. Risk Levels

Risk Level	**Description**
High	It is likely that exploitation of a given vulnerability by a threat will severely and adversely impact the Department, resulting in over one million dollars worth of damage and/or leading to legal ramifications (e.g., potential jail sentence). This rating indicates a strong need for corrective measures and actions.

Medium	It is likely that an exploitation of a given vulnerability by a threat will moderately impact the Department, resulting in between 100,000 and one million dollars worth of damage or leading to legal action without the potential of a jail sentence. This rating indicates a strong need for corrective measures and actions.
Low	The given vulnerability may be subject to exploitation by a threat, but the probability of such exploitation is small and/or its impact on the Department's assets and resources would be minor, resulting in less than 100,000 dollars worth of damage or leading to administrative penalties. This rating indicates a need for corrective measures and actions.

2.5 Who is Responsible for Conducting the Risk Assessment?

The Principal Officer is responsible for ensuring that a risk assessment is conducted, for all GSSs and MAs for which he or she is responsible, in accordance with OMB Circular A-130. The risk assessment team must consist of individuals who are experienced in performing risk assessments (e.g., understand and have applied proven risk assessment methodologies). The team must have knowledge of Federal laws and regulations associated with risk assessments and have adequate technical knowledge of systems and networks. Risk assessment team members must be independent thus not having a vested interest in the GSS or MA being assessed. Thus, no individual from the Principal Office (PO) or any individual who supports or maintains the system should perform the risk assessment. The independent risk assessment team must work with the GSS or MA owners and those who administer and support the GSS or MA in order to obtain all the information needed for the assessment.

The primary requirement for the risk assessment team is that at least one member be considered an information security professional. This individual must have a working knowledge of information security controls and must ensure that all information and documentation gathered for the risk assessment is treated appropriately as Department sensitive information.

All of the roles and responsibilities for the risk assessment process are listed in the table below.

Roles	Responsibilities
Chief Information Officer	The Chief Information Officer (CIO) endorses the remediation plan submitted by the Principal Officer following a completed risk assessment.
OCIO Information Assurance Office	The Information Assurance (IA) office within the Office of the Chief Information Officer is responsible for developing Department of Education information technology security risk assessment policy, procedures and guidance. IA is also responsible for incorporating and monitoring completion of remediation actions into the Department of Education's FISMA action plan that is reported to OMB.
Principal Officer	The Principal Officer is responsible for ensuring that a risk assessment is conducted, for all GSSs and MAs for which he or she is responsible, in accordance with OMB Circular A-130. The Principal Officer participates in interviews with the Risk Assessment Team and submits the resulting risk assessment remediation plan to OCIO.

Roles	Responsibilities
Independent Risk Assessment Team	The independent risk assessment team completes the risk analysis of the system and documents the results in the final Risk Assessment Report. This team must work with the GSS or MA owners and those who administer and support the GSS or MA in order to obtain all the information needed for the assessment.
System Manager (SM)[9]	The SM represents the interests of the GSS or MA throughout the SDLC. The SM is responsible for ensuring the GSS or MA is operating in accordance with the security controls outlined in the SSP. The SM participates in interviews with and demonstrations of the system for the Risk Assessment Team. The SM signs off on the resulting risk assessment remediation plan that is submitted to OCIO.
Computer Security Officer (CSO)	The CSO manages the efforts of the C&A activities, including the risk assessment, and acts as the managing official for information security of GSSs or MAs within the PO. The CSO participates in interviews with and demonstrations of the system for the Risk Assessment Team. The CSO signs off on the resulting risk assessment remediation plan that is submitted to OCIO.
System Security Officer (SSO)	The SSO is directly responsible for the information security of a GSS or MA within the PO. The SSO ensures that security is considered at every point in the life-cycle process and manages the integrity of the GSS or MA. The SSO participates in interviews with and demonstrations of the system for the Risk Assessment Team. The SSO prepares the resulting risk assessment remediation plan that is submitted to OCIO.
User Representative	The user representative is responsible for ensuring that the user is able to conduct normal business activities with the particular GSS or MA. The user representative is the spokesperson for the user community representing the operational interests of the user. This representative ensures that user requirements are met during the SDLC allowing the user to perform the tasks defined in their job description. The user representative participates in interviews with and demonstrations of the system for the Risk Assessment Team.

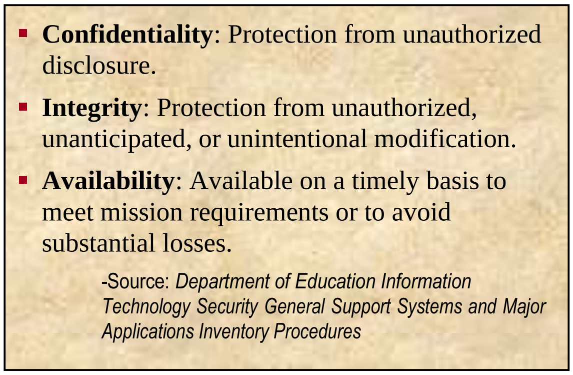
2.6 What is Information Sensitivity and Mission Criticality?

Two very important elements must be considered when performing a risk assessment. *Information sensitivity* and *mission criticality* are key components that will be used to assess risk levels. This section addresses when and how information sensitivity and mission criticality are factored into the risk assessment. The intent of the following two sections is to simply define these two terms. A more thorough discussion of information sensitivity and mission criticality can be found in the *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures*.

[1] The System Manager is also known as the Program Manager.

2.6.1 Information Sensitivity

The criteria used to measure the information sensitivity include: information *confidentiality*, *integrity*, and *availability*. Figure 1 provides a description of each criteria element.



- **Confidentiality**: Protection from unauthorized disclosure.
- **Integrity**: Protection from unauthorized, unanticipated, or unintentional modification.
- **Availability**: Available on a timely basis to meet mission requirements or to avoid substantial losses.

-Source: *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures*

Figure 1. Information Sensitivity Criteria

Information that is labeled “For Official Use Only” is confidential and must be protected from unauthorized disclosure. Unauthorized disclosure of this information may result in a tangible and intangible loss to the agency. Confidential information (i.e., information labeled as “For Official Use Only) is sensitive and may contain any of the following types of data—

- Proprietary business information that may not be released to the public under the Freedom of Information Act or other laws
- Personal data that requires protection under the Privacy Act of 1974.
- Source Selection information for contracts
- Deliberative process materials
- Monetary or budgetary information that would permit circumvention of security measures and internal controls

Refer to the *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures* for additional guidance on assigning levels of high, medium, or low for each information sensitivity criteria. This guidance will assistin determining an overall information sensitivity level for the GSS or MA and the data housed onthat GSS or MA.

When considering the type of data transmitted, stored, or processed (e.g., privacy data) on the GSS or MA, it is important to note that sensitive information includes, but is not limited to—

- Social security numbers
- Personal addresses
- Credit history

2.6.2 Mission Criticality

In accordance with the *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures*, the criterion used to measure mission criticality is closely related to how integral the system is to supporting the mission of the Department.

Mission criticality may be measured as being either: *mission critical*, *mission important*, or *mission supportive.* Figure 2 provides a brief definition of these mission criticality types.

- **Mission Critical**: Automated information resources whose failure would preclude the Department from accomplishing its core business operations.
- **Mission Important**: Automated information resources whose failure would not preclude the Department from accomplishing core business processes in the short term, but would cause failure in the mid- to long-term (three days to one month).
- **Mission Supportive**: Automated information resources whose failure would not preclude the Department from accomplishing core business operations in the short- to long-term (more than one month), but would have an impact on the effectiveness or efficiency of day-to-day operations.

-Source: *Department of Education Information Technology Security General Support Systems and Major Applications Inventory Procedures*

Figure 2. Mission Criticality Criteria

2.7 How are Threat and Vulnerability Defined?

2.7.1 Threat

A *threat* is defined as any circumstance, event, or act that could cause harm to the Department by destroying, disclosing, modifying, or denying service to automated information resources. There are three threat categories: natural, environmental, and human. Table 4 provides examples of threats found in each category.

Table 4. Threat Categories

Natural Disaster			
• Storm damage (e.g., flood, snow, hurricane)	• Fire	• Lightning strikes	• Earthquakes
Environmental Control Failures			
• Long-term power failure	• Chemicals	• Liquid leakage	• Pollution
Human			
• Assault on an employee	• Arson		• Blackmail
• Bomb or terrorism	• Browsing of Privacy Act and proprietary information		• Civil disorder
• Computer abuse	• Corrupted data input		• Falsified data input
• Fraud	• Hacking		• Impersonation
• Interception	• Labor dispute or Strike		• Malicious code
• Negligence or Human error	• Unauthorized disclosure of sensitive information		• Password guessing (e.g., dictionary attack)
• Replay	• Sabotage or Vandalism		• Social engineering
• Spoofing	• System tampering		• Theft

Natural disasters are caused by extreme weather or earthquake, and environmental controlfailures are caused by utility failures; a threat agent, someone who exploits systemvulnerabilities, is the cause of human threats. Examples of human *threat agents* include the following—

- **Insiders**: Disgruntled employees, dishonest employees, and Department system users, both those with general system access and those with increased, privileged access.
- **Contractors and subcontractors**: Cleaning crew, developers, technical support personnel, and computer and telephone service repairmen
- **Former employees**: Employees who retired, resigned, or were fired
- **Unauthorized users**: Computer criminals, terrorists, and intruders (hackers and crackers) who attempt to access the Department's internal network
- **Authorized users**: Any approved user (e.g., government agency employee, contractor, business partner).

2.7.2 Vulnerability

A vulnerability is a condition that has the potential to be exploited by a threat. BLSRs, located in Appendix D, must be the initial security checklist used to determine vulnerabilities. BLSRs are a set of security requirements the Department views as the minimal security standards to be upheld by all GSSs and MAs. BLSRs must be used to determine vulnerabilities. Therefore, BLSRs that are not met must be flagged as vulnerabilities. Appendix E, Vulnerability Questionnaire is used as a supplement to the BLSRs. The questionnaire is provided to initiate probing. It is recommended that each PO amend the questions to reflect appropriate questions for their GSS or MA.

The following list contains sources to consider when identifying vulnerabilities to the GSS and/or MA—

- Previous risk assessments
- Security audits
- Bulletins [Computer Emergency Response Team (CERT), Federal Computer Incident Response Capability (FedCIRC), and Department of Energy's Computer Incident Advisory Capability (CIAC)]
- Vendor advisories
- System development test procedures
- System test results
- System audit logs

Proactive methods that can be used to collect vulnerability information include—

- Automated vulnerability scan
- Network mapping
- Security test and evaluation (ST&E)
- Penetration testing

Figure 3. Vulnerability Sources

Vulnerabilities are identified from information collected from each PO, its GSS or MA, and the environment. This information is collected during site surveys, interviews, network scanning, and documentation. Available industry sources must be used to identify vulnerabilities that may be applicable to specific systems (see Figure 3 for a list of sources). The specific sources of vulnerabilities and the methodology that must be used to identify them vary depending on whether the GSS or MA is in the design phase or has already been implemented.

If the GSS or MA has been neither designed nor implemented, vulnerabilities can be derived by understanding the weaknesses of the network components and operating systems being considered or proposed. If the GSS or MA is in the process of being designed and implemented, the vulnerability identification must be expanded to include more specific information. In this instance, automated tools and databases of known vulnerabilities may be used to identify appropriate GSS or MA security configurations. However, if the GSS or MA is operational, then the vulnerability identification must include an analysis of whether the security controls implemented were determined to be correct and effective.

2.7.3 Relationship Between Threat and Vulnerability

A vulnerability cannot be exploited unless there is a potential threat and associated threat agent. The threat agent must have the means, opportunity, and motivation to exploit a potential vulnerability. Based on this description, it is evident that threats and vulnerabilities are closely aligned when assessing risk. What might constitute a minor threat has the potential to become a greater threat, or a more frequent threat, because of a vulnerability.

2.8 Which Security Domains Should be Assessed?

Table 5. Security Domains

Security Domain	Security Criteria
Management Controls **Procedures and management controls established for use of and access to the GSS or MA and its resources*	▪ Assignment of responsibilities ▪ Risk Management ▪ Authorize Processing ▪ Security Controls Review ▪ Privacy Act ▪ Rules of Behavior ▪ System Security Plan
Operational Controls **Procedures and operational controls established that focus on mechanisms implemented and that are executed by people*	▪ Configuration Management ▪ Contingency Planning ▪ Personnel Security ▪ Security Awareness and Training ▪ Physical Security ▪ Environmental Security ▪ Production Input/Output Controls ▪ Information Sharing ▪ Public Access Control ▪ Data integrity ▪ Incident Handling
Technical Controls **Procedures and technical controls established for securing processing, storage, and transmission of information*	▪ Identification and Authentication ▪ Logical Access Controls ▪ Auditing

2.9 What Information Gathering Techniques Should be Used When Conducting a Risk Assessment?

2.9.1 Questionnaire

To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management, operational, and technical controls planned or used for the GSS or MA. This questionnaire must be distributed to the appropriate technical and nontechnical management personnel who are designing or supporting the GSS or MA. The questionnaire must be used during site visits and interviews.

2.9.2 Interviews

Interviews with the Department’s IT security professionals (e.g., CSO, NSO, SSO) and management personnel enable the risk assessment team to collect pertinent information about the system. Site visits enable the risk assessment team to observe and gather information about the physical, environmental, operational, and technical security of the GSS or MA.

2.9.3 Documentation Review

Risk assessments vary in scope and level of effort. Therefore, documentation used during the risk assessment may vary as well. The following documents must be used to assist in the preparation of the risk assessment—

- Mission statements
- GSS and MA Inventory Submission Form
- NIST SP 800-26, Security Self-Assessment Procedures for Information Technology Systems
- Organization and site-specific security policies and procedures
- Organization charts
- System functional requirements
- System and architecture design, including—
  - Lists of system components and applications
  - Diagrams and descriptions of the system architecture
  - Printouts of system component configurations (e.g., firewall and router policies, server and workstation configuration files)
  - System security controls documentation.
- Site operations manuals (facility specific)
- Standard operating procedures (SOP)
- Reports from prior risk analyses
- Physical security plans
- Configuration management plans and procedures
- Disaster recovery plans
- Site floor maps
- User manuals for specific systems under assessment.

2.9.4 Scanning Tools

Proactive technical methods can be used to collect system information efficiently. An example of this is the use of network mapping tools. These tools can provide a rapid profile of the GSS or MA being assessed.

While the Department does not advocate a particular scanning tool, the following tools are examples of products that have been used across the industry—

- **Network Mapper** (nmap) is a utility for scanning large networks using a variety of techniques to increase speed and minimize detection. It does not build a network topology, but identifies the services that are running on a large group of hosts by scanning networks for the open transport control protocol (TCP) and user datagram protocol (UDP) ports on each host. Usually, nmap is used for initial scans because it provides a quick way to build individual profiles of the target systems.

- **CyberCop Scanner** is a commercial network security vulnerability detection product that scans an entire network or individual hosts to verify and report network and system security issues. It tests for a comprehensive set of known security vulnerabilities, but does not provide details on how to exploit them. Since CyberCop takes some time to complete a scan, this tool is normally applied after narrowing the targets down to a focus group.

- **Nessus** is a free, powerful, and easy-to-use security scanner that remotely audits a given network in order to determine whether crackers may break into it, or misuse itin some way. Taking nothing for granted, Nessus does not consider that a given service is running on a fixed port.

- **Security Auditor's Research Assistant (SARA)** is a third-generation, Unix-based security analysis tool that is based on the SATAN (Security Administrator Tool for Analyzing Networks) model. SARA is adapted to interface with other community products. For example, SARA interfaces with the nmap package for superior "operating system fingerprinting." Additionally, SARA provides a transparent interface to Samba (an open source suite that provides seamless file and print servicesto SMB[10]/CIFS[11]) for security analysis.

- **Internet Security Systems (ISS) Database Scanner** is a commercial tool that automatically scans databases for vulnerabilities from a single-user interface anddisplays scan results and fixes information in clear reports that allow users to respond quickly to critical vulnerabilities. Specifically, the Database Scanner penetration testing feature automatically probes a database through default accounts and password cracking, finding vulnerabilities that a knowledgeable attacker would exploit to gain access to database servers and an organization’s critical data or network.

- **Security Administrator’s Integrated Network Tool (SAINT)** is a tool that gathers information about remote hosts and networks by examining services such as finger, network file system (NFS), Network Information System (NIS), file transfer protocol (ftp), trivial file transfer protocol (tftp), and Remote Execution Daemon (rexd). Based on initial data collection and a user-configurable rule set, SAINT examines the avenues of trust and dependency and iterates further data collection runs over secondary hosts. This allows the user to analyze the network or hosts, as well as examine the real implications inherent in network trust and services.