



Requirements For Computer Security

FTA/IRS Safeguards Symposium
&
FTA/IRS Computer Security Conference
April 2, 2008
St. Louis

1



Agenda

- Security Framework
- Safeguards IT Security Review Process
- Preparing For A Safeguards Review
- Assessment Tools
- Safeguards Review Report Overview
- Safeguards POA&M Process
- Safeguards Procedures Report
- Questions
- Supplemental Technical Slides

2



Laws & Regulations

Laws, Regulations, and Standards directly applicable to Safeguards Program

- Title 26. Internal Revenue Code (IRC) 6103 – Confidentiality and disclosure of returns and return information
- Publication 1075 - Tax Information Security Guidelines For Federal, State, And Local Agencies/Entities
- Federal Information Security Management Act (FISMA) of 2002, Title III – Information Security, P.L. 107-347: A security plan must be developed and practiced throughout all life cycles of the agency's information systems

NIST Standards and Guidelines applicable to Safeguards Program

- Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems:
 - Defines standards for the security categorization information and information systems



Laws & Regulations (continued)

- Federal Information Processing Standards (FIPS) Publication (PUB) 200, Minimum Security Requirements for Federal Information and Information Systems:
 - Contains information regarding specifications of minimum security control requirements for Federal information and information systems
- NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories:
 - Provides guidance for implementing FIPS 199
- NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems:
 - Contains a list of security controls that are to be implemented into Federal information systems based on their FIPS 199 categorization
 - Required by FIPS 200
- NIST Special Publication (SP) 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, draft
 - Provides guidance for testing the implementation of 800-53 controls

NIST Control Families Relevant To Publication 1075

Computer Security Requirements are divided into 17 different control families
Sections 5.6.1 - 5.6.17 in the Pub 1075

Technical Control Family
Identification and Authentication (IA)
Access (AC)
Audit and Accountability (AU)
System and Communications Protection (SC)

Management Control Family
Risk Assessment (RA)
Planning (PL)
System and Services Acquisition (SA)
Certification and Accreditation (CA)



Operational Control Family
Personnel Security (PS)
Physical and Environmental Protection (PE)
Contingency Planning (CP)
Configuration Management (CM)
Maintenance (MA)
System Integrity (SI)
Media Protection (MP)
Incident Response (IR)
Security Awareness Training (AT)

Facts About NIST SP 800-53 Controls and Pub 1075

- Not all of the security controls documented in the 17 NIST SP 800-53 control families were included in the revised Publication 1075
 - Selection was made keeping Confidentiality as the prime security objective
 - Requirements not applicable to Safeguards are marked with an asterisk
 - A strong security program should address all security controls documented by NIST
- Physical and Environmental protection control family from NIST SP 800-53 is included as part of the Physical and Disclosure review as opposed to IT Security Safeguards Review
- New computer security requirements are introduced in Publication 1075 (Exhibit 4) based on NIST SP 800-53
 - Configuration Management
 - System Maintenance
 - Incident Response
 - Awareness Training





Security Objectives

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]
- **Integrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]
- **Availability:** Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]
- Safeguards Primary Objective:
 - Ensuring **Confidentiality** and protecting against **Unauthorized Disclosure** of Federal Taxpayer Information (FTI)

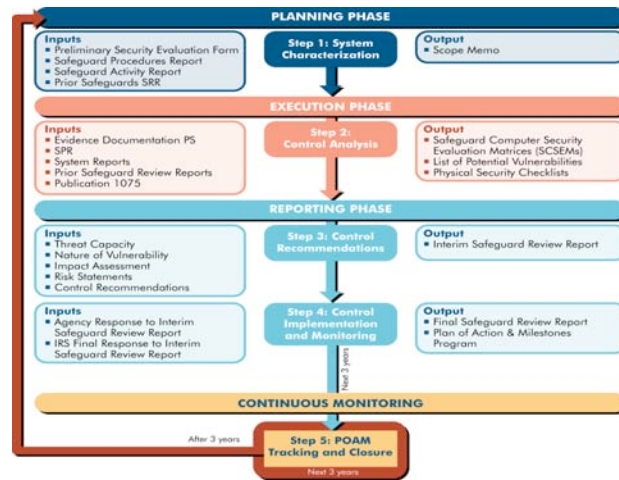
Examples Of Relevant Security Controls	Strong Security Controls Not In Scope of Safeguards
AC-3 ACCESS ENFORCEMENT	*CP-3 CONTINGENCY TRAINING
AT-3 SECURITY TRAINING	*CP-9 INFORMATION SYSTEM BACKUP
AU-2 AUDITABLE EVENTS	*MA-6 TIMELY MAINTENANCE
CM-6 CONFIGURATION SETTINGS	*PE-10 EMERGENCY SHUTOFF
IA-2 USER IDENTIFICATION AND AUTHENTICATION	*PL-5 PRIVACY IMPACT ASSESSMENT
IR-4 INCIDENT HANDLING	*SC-14 PUBLIC ACCESS PROTECTIONS
PS-3 PERSONNEL SCREENING	*SI-8 SPAM PROTECTION



Security Categorization and Tax Management Information Type

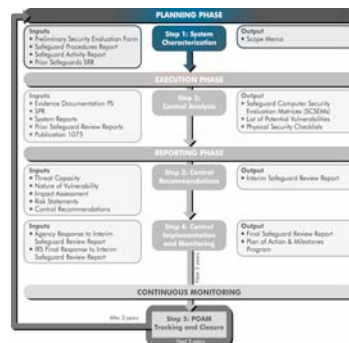
- NIST categorizes information systems according to the information they store, process, or transmit
- FIPS 200 and SP 800-60 provides impact levels in terms of CIA for various information types processed by the Federal Government
- Taxation Management Information type is categorized as
 - Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}
- Taxation Management Information type is Defined as
 - Taxation Management includes activities associated with the implementation of the Internal Revenue Code and the collection of taxes in the United States and abroad
- Special Factor - Taxation Management Information type could have **HIGH** impact on Confidentiality *"in cases where unauthorized disclosure of taxation information can impede anti-terrorism or other homeland security activities or endanger the lives of agents or informants"*

IRS Safeguards IT Security Review Process



4 Ways Agencies Can Prepare For A Safeguards Review

- Timely identification of agency IT POC
 - Timeline: as early as possible
- Identify a mutually convenient time to hold the Preliminary Security Evaluation (PSE) call after initial contact by the IRS
 - Timeline: 60 days before the on-site review
- Collect documents to support Management, Operational, and Technical (MOT) controls
 - Timeline: 2 - 4 weeks prior to on-site review
- Conduct a "dry run" of the applicable SCSEMs to obtain familiarity with the assessment procedures and expected results
 - Timeline: 2 - 4 weeks prior to on-site review





1. Timely Identification of Agency IT Point of Contact

- Critical to a well coordinated Safeguards IT Security Review
- Key activity performed in the planning phase
- IT POC responsibilities:
 - Coordinate with the Agency Safeguards Review POC
 - Provide to the IRS the date and time for the PSE call at least 60 days prior to the on-site review
 - Ensure appropriate resources are available for the PSE call
 - System Administrator (SA) for the Mainframe, Unix, Windows, and Network devices
 - Information System Security Officer (ISSO)
 - System Owner
- Database Administrators (DBA) and Application Developers might not be needed for the PSE call or for the on-site Review at this time

11



2. Timely System Characterization

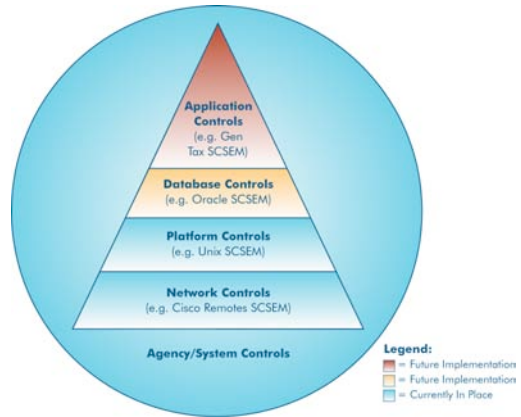
- Critical to finalizing the scope of the Safeguards Review
- Timely scheduling of PSE call during the Planning Phase
- Agency POC is responsible for completing the PSE form provided to the agency after the initial contact by the IRS
- PSE call usually lasts 1 hour and involves the following stakeholders
 - Agency Safeguards POC and IT POC
 - System Administrator(s), Network Administrator(s), System Programmer(s)
 - IRS Office of Safeguards and supporting contractor
 - Small Business/Self-Employed (SBSE) Government Liaison
- System information is collected during the PSE call without any prior knowledge and assumptions
- Output of the PSE call defines the scope of the Safeguards review through Scope Memo

12



IRS Safeguards IT Security Review Scope

- Currently the Safeguards IT review addresses Agency/System, Network and Platform controls.
- Scope of Safeguards IT Security review is projected to include database and application level controls in the future
- Scope continues to evolve over time addressing latest security trends and vulnerabilities while increasing comprehensiveness



13



3. Timely Collection of Evidence to Support MOT SCSEM

- Critical to successful execution of MOT SCSEM
- MOT SCSEM evaluates:
 - System, program, and agency level security controls
 - Through examination of documentation for evidence
 - Through interview of related personnel e.g. ISSO
- MOT Document Request List specifies documentation required for MOT SCSEM
- Completing MOT SCSEM during the on-site Safeguards Review ensures:
 - Unnecessary findings are NOT generated due to lack of evidence
 - Additional coordination between Agency and IRS is not needed after onsite review

14



MOT Document Request List

- MOT Document Request List specifies:
 - Security Requirement control number
 - Security Requirement Objective
 - Evidence requested to support assessment

MOT Document Request List Sample

Item #	Security Requirement	Security Requirement Objective	Evidence Requested
Risk Assessment (RA) Controls			
1	RA-1	Risk Assessment Policy & Procedures	Risk Assessment Policy & Procedures
2	RA-2	Security Categorization	No evidence needed. All agency systems are categorized as Moderate due to the presence of federal tax information
3	RA-3	Risk Assessment	The most recent system risk assessment
4	RA-4	Risk Assessment Update	(see RA-3)
5	RA-5	Vulnerability Scanning	Test plans and test results for Vulnerability Scanning. Provide plan & results for last 4 quarters
97	PB1075-5.6.17.4b	Web Application: FTI Access Through an Intranet Portal/Interface Is Controlled	Inquiry: Does agency have portal/interface application and is FTI accessible through the portal/interface application? System-generated list of who has access to FTI through the portal/interface application
98	PB1075-7.4.5a	Contractors Have Authorized FTI Access	Risk Assessment for the application (See RA-3) Inquiry: Does the agency use contractors to process FTI? System-generated list of all user IDs and associated user name descriptions to determine if the agency employs any contractors
99	MP-2	Media Protection: Supplemental Media is not created or secured if created after FTI is loaded from tapes or through	Inquiry: Is media created after FTI is initially loaded onto the system?



4. Completing a Dry Run of Technical SCSEMs

- Dry run of Technical SCSEMs prepares the agency for the Safeguards review
- Familiarizes the agency with the SCSEMs format and content
- Increases the efficiency of the review, reducing the burden on Agency staff time
- SCSEMs should be shared with the System Administrators and Information Security Officer in advance of the Safeguards Review Team on-site visit
- Provides an opportunity to fix weakness prior to the on-site review

Note: All SCSEMs are available from the www.IRS.Gov Safeguards portal



Safeguards Computer Security Evaluations

- IRS Safeguards Review Team leverages two primary means to evaluate Computer Security during on-site review:
 - Safeguards Computer Security Matrix for each technology and MOT
 - Security Content Automation Protocol (SCAP) based automated compliance COTS software - Planned
- A SCSEM based evaluation:
 - Is manually performed with the help of system personnel
 - Requires more on-site support time from the system administrators
- SCAP based tools :
 - Are automated
 - Requires minimal support from the system administrators
 - Are more comprehensive
- IRS Office of Safeguards is planning to leverage more automated SCAP tools as they become available

17



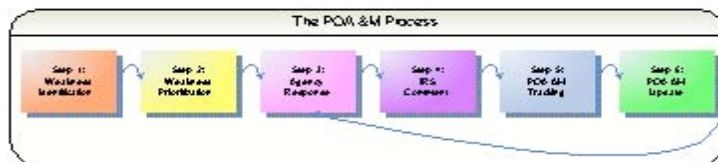
Key Facts About Safeguards Review Report Section H

- Safeguards IT Security findings are reported in section H of the Safeguards Review Report (SRR)
- Section H has two main sub-sections:
 - Technology Specific Findings (e.g. Windows, HP-UX) - Rolled up for each technology
 - MOT Specific Findings (e.g. Incident Response) – Rolled up for each control family
- Each Finding has the following key areas:
 - Finding Statement
 - Finding Description
 - Risk Description (Not a Risk Level)
 - Recommendation
- Agencies with common computer systems are encouraged to collectively resolve IT Security Findings while reporting resolution in their individual reports

18

IRS Office of Safeguards POA&M Process

- IRS POA&M process will clearly identify, track, report and ultimately remediate weaknesses generated from the Safeguards IT/Disclosure Enforcement reviews
- Agencies will be responsible for providing:
 - A resolution plan as part of the Interim SRR response
 - Closure within 1, 3, 6, and 12 months as prescribed in the recommendation within SRR
- POA&M item resolution time frame is specified in the recommendation for each finding (within SRR)




19

SPR Security Requirements

- Latest Publication 1075 (Oct. 2007 version) requires agencies to submit SPR every 6 years or when a significant change occurs
- SPR template has been revised to account for the latest computer security requirements contained in Pub 1075
- Agencies are encouraged to comprehensively document FTI Safeguarding procedures. Agencies will benefit by:
 - Satisfying IRS SPR reporting requirements
 - Satisfying two of the Pub 1075 computer security requirements (PL-2 and PL-3) for developing and updating a System Security Plan (SSP)
 - Avoiding a potential finding that may arise from insufficient information in the SPR observed by the on-site Safeguards review team

Note: Copy of the latest SPR template is included in the presentation package

20



Questions?

21



Supplemental Technical Slides

22



Safeguards Computer Security Evaluation Matrix

- A Safeguards Computer Security Evaluation Matrix (SCSEM) is comprised of the minimum computer security requirements compiled from multiple sources:
 - Applicable Federal Regulations, such as those furnished by the Office of Management and Budget (OMB)
 - National Institute of Standards and Technology (NIST)
 - Department of Treasury and IRS Regulations
 - Industry practices
- One SCSEM exists for each technology within Scope of a Safeguards IT Security Review
- All Safeguards SCSEMs were revised to address any changes, additions, and deletions of security requirements in the revised Publication 1075 (Oct. 2007)
 - A new Management, Operational, and Technical controls SCSEM was drafted to address system wide controls
 - SCSEMs were converted from Word to Excel format

23



Safeguards Inventory of SCSEMs

- | | |
|---|--|
| <ul style="list-style-type: none">■ Mainframe<ul style="list-style-type: none">■ RACF■ ACF2■ CA Top Secret■ Unisys (with SIMAN)■ Network<ul style="list-style-type: none">■ Cisco IOS■ Others<ul style="list-style-type: none">■ MOT (System Wide) | <ul style="list-style-type: none">■ Tier II (Servers)<ul style="list-style-type: none">■ Unix/Linux (Solaris, AIX, RedHat, HP-UX11)■ Windows (NT, 2000, 2003)■ OpenVMS■ SCO Unix■ Tru64■ Novell■ Special<ul style="list-style-type: none">■ GenTax (Planned) |
|---|--|

24



Safeguards Computer Security Evaluation Matrix Sample

Test ID	NIST ID	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments/Supporting Evidence
UNIX-LINUX-7	IA-2, IA-5	Checks to see if passwords contain information such as names, telephone numbers, account names, dictionary words, etc.	Interview the SA or ISSO and ask if passwords are allowed that might contain information such as names, telephone numbers, account names, dictionary words, etc.	Passwords do not contain information such as names, telephone numbers, account names, dictionary words,			
UNIX-LINUX-8	IA-2, IA-5	No automated passwords exist	Interview the ISSO or SA and ask if passwords can be automated through function keys, scripts, or other methods where passwords may be stored on the system.	No automated password methods are used.			
UNIX-LINUX-9	IA-6	Check to see if the feedback from the information system provides information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.	Interview ISSO or SA and ask if any applications or services display the user or service account password during input or after authentication.	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.			

25



Automated Tools Used During Safeguards IT Security Review

- The following tools are available to assist in execution of the Safeguards IT Security Review:
 - NIST SCAP based Windows XP and Vista compliance COTS products
 - Cisco Security Analyzer
- Leveraging SCAP based tools positions the agency and IRS to proactively address present and upcoming Federal Requirements (e.g. FDCC)
- The tools are non-intrusive to the target computing environment
 - They DO NOT change system configuration
 - They are NOT penetration testing tools
- The results from these tools are used only to evaluate and substantiate the evidence for some of the computer security requirements reported in the SRR

26



Security Content Automation Protocol (SCAP)

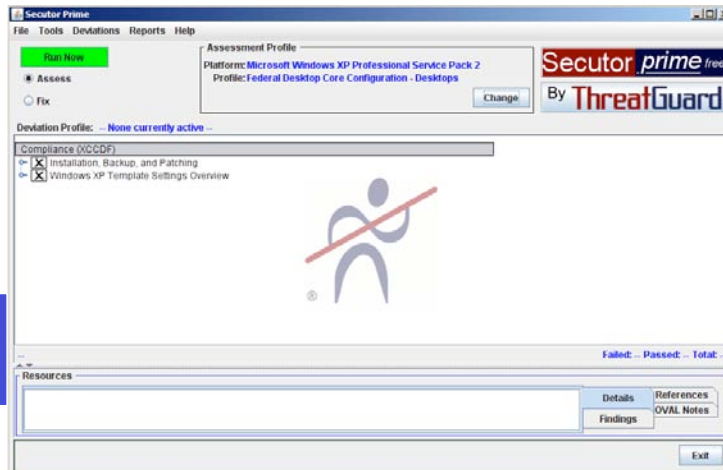
- SCAP is a capability created by the Information Security Automation Program (ISAP) that allows standards based automation of security checking and remediation
- Built through partnership between Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST)
- SCAP tools are based on SCAP content developed for each technology e.g. Windows XP, Windows Vista, Windows 2003 Server – Beta Version, Red Hat Linux – Beta Version, Solaris 10 – Beta Version
- SCAP is more than a standard for compliance based software tools. It brings:
 - Security Measurement
 - Secure Configurations Baseline and Maintenance
 - Technical Controls Compliance Automation
 - Customization of recommended secure configurations
 - Standardization in communication involving security vulnerabilities

27



Sample SCAP Windows XP Tool

Screen shot of the SCAP Windows XP Tool by ThreatGuard



28



Additional Pub 1075 IT Security Requirements

- Transmitting FTI
 - Highlight: All FTI data in transit must be encrypted when moving across a Wide Area Network (WAN). Generally, FTI transmitted within the Local Area Network (LAN) should be encrypted. If encryption is not used, the agency must use other compensating mechanisms, e.g. switched vLAN technology, fiber optic medium, etc., to ensure that FTI is not accessible to unauthorized users
- Remote Access
 - Highlight: Accessing databases containing FTI from a remote location, i.e., a location not directly connected to the Local Area Network (LAN), will require adequate Safeguards to prevent unauthorized entry
- Electronic Mail
 - Highlight: Generally, FTI shall not be transmitted or used on E-mail systems
- Internet/Web Sites
 - Highlight: Perform risk analysis on computer system before they are connected to the internet

29



Facsimile Machines Controls

- **Facsimile Machines:** Protecting facsimile machines is an additional requirement in Publication 1075 section 5.6.17. It requires
 - Having a trusted staff member at both the sending and receiving fax machines
 - Accurately maintaining broadcast lists and other preset numbers of frequent recipients of FTI
 - Placing fax machines in a secured area
 - Including a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes:
 - A notification of the sensitivity of the data and the need for protection and
 - A notice to unintended recipients to telephone the sender—collect if necessary—to report the disclosure and confirm destruction of the information

30



Tumbleweed

- Tumbleweed is a COTS software package (part of SDT) that encrypts FTI while transmitted from IRS to the Agency
- As of October 2007, IRS requires all agencies to receive FTI through Tumbleweed vs. conventional tape delivery
- IRS recommends to install the Tumbleweed client software on a designated Tumbleweed workstation or server
- MOT SCSEM (Test IDs 93 – 95) specifies Tumbleweed client secure configuration required
- Agencies are encouraged to leverage the Tumbleweed security standards specified in the MOT SCSEM when implementing or maintaining the system

31



Identification & Authentication Defined

- **Risk:** Authorized and unauthorized activities performed on the system can be uniquely attributed to a single user.
- **Identification:** Requires identification of each system user—often accomplished with a user ID. A user ID must be unique and auditable.
- **Authentication:** Requires proof of identification before accessing the system – often accomplished with providing a password and/or biometrics e.g. fingerprint scan. Authentication must be an auditable function.
- **Example:** A unique user ID and password is assigned to all the privileged users of the Operating System e.g. System Administrator, Database Administrator, and Security Officer. Shared accounts are not used on the system unless it is a system account e.g. in case of Oracle Database a system account is created for the database to interact with the OS. User IDs are created with a defined pattern e.g. user's first and last initial, department id, and location code. Passwords comply with the complexity requirements e.g. 8 characters in a combination of alpha and numeric or special characters and do not contain dictionary words.

32



Access Control Defined

- **Risk:** Excessive or unauthorized access to system and FTI might be possible.
- **Access Control:** Logical access controls are Safeguards incorporated in computer hardware, operations or applications software, and related devices to protect critical IT resources against vulnerabilities and threats from both internal and external sources. Ensures users only have the minimum privileges necessary to perform job duties. ("Need to Know").
- **Example:** Roles based access control is in place at the operating system level. Access privileges are granted based on the user groups that a user is a member of. Management approval is granted to authorize user access to system resources.

33



Audit & Accountability Defined

- **Risk:** Detection and resolution of unauthorized system activities might not be possible.
- **Audit:** A reliable, systemic trail of accesses to data on the computer system. At a minimum, an audit trail must record login attempts, password changes, and FTI file creation/modification/deletion. To maintain integrity, users should be prohibited from changing the audit records of the computer system.
- **Example:** Audit events are generated in accordance with the Publication 1075 requirements including successful and unsuccessful attempts to FTI data files stored on the system. Audit events contain the necessary information e.g. user ID, date and time stamp, type of event, object name, etc. Audit records are archived off the system to a central server before reaching the storage limit. Reporting tools are used to generate audit reports that are reviewed periodically by Security Personnel (e.g. ISSO) to detect unauthorized access to system and/or FTI data.

34



Personnel Security Defined

- **Risk:** Employees/Contractors with inappropriate background might be authorized to access the system and FTI.
- **Personnel Security:** Personnel security measures are used to ensure that only authorized personnel are physically accessing the system and FTI stored on the system in accordance with their position categorization after going through a background screening process.
- **Example:** Personnel with physical access to the facilities and system containing FTI have gone through an appropriate level of background investigation process with the agency that commensurate with their access to the system and the facility. Policies also exist within the agency to control third-party access to the system and FTI.

35



Media Access Protection Defined

- **Risk:** Unauthorized disclosure of FTI might be possible through improper handling of the media.
- **Media Access Protection:** Media access protects FTI from unauthorized disclosure by controlling access to the media and encrypting the data on the media as well as sanitizing before reusing the media.
- **Example:** Media containing FTI is restricted to a limited number of agency personnel who are authorized to receive and handle the media e.g. computing center staff. Once the media is received by the agency, it is protected in a restricted area. When the media is transported out of a controlled area e.g. computer room, the agency protects the media by restricting the activities associated with transport of such media to authorized personnel only.

36



Supplemental Documentation

- SPR Template
- SAR Template
- MOT SCSEM Release IV
- MOT Document Request List
- Technical SCSEMs Release IV
- Pub1075 October 2007 Release
- Pub 1075 Revision FAQs
- Pub 1075 Revision Drop-in articles
- FTA TAG Ten Security Commandments
- Full Security Contact List
- WinZip Instructions