



**Mission Assurance & Security Services (MA&SS):
Office of Safeguards**

Federation of Tax Administrators

2007 Computer Security Officers Conference

- ▶ Presented by:
 - Bennett Hodge, Booz Allen Hamilton



Safeguard and Security Workshop

0



**Publication 1075 (Pub. 1075)
Information Technology Security Changes**

Federation of Tax Administrators

2007 Computer Security Officers Conference

- ▶ Presented by:
 - Bennett Hodge, Booz Allen Hamilton



Safeguard and Security Workshop

1

Table Of Contents

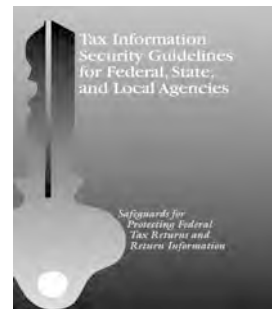
- ▶ Introduction
- ▶ IRS Publication 1075 Defined
- ▶ Pub. 1075 Computer Security Control Updates
- ▶ Pub. 1075 Computer Security Control Requirements
- ▶ PUBLICATION 1075 – GAP ANALYSIS
- ▶ Pub. 1075 Computer Security Control Updates:
Supplementary Information
- ▶ Questions



What is IRS Publication 1075?

IRS Publication 1075 (hereafter called Pub. 1075) provides information security guidelines to agencies that process, store or transmit federal tax information (FTI) under the provisions of Internal Revenue Code Section 6103.

- ▶ To satisfy the current computer system security requirements outlined in the current Pub. 1075, agencies should:
 - Meet the current computer security requirements specified in the current Department of Defense Trusted Computer System Evaluation Criteria (TCSEC).
- ▶ To satisfy the new computer system security requirements outlined in the updated Pub. 1075 (soon to be released) agencies should:
 - Meet the new computer security control requirements specified in the updated Pub. 1075.



Pub. 1075 Computer Security Control Updates

- ▶ The revised computer security framework was primarily developed using applicable guidelines specified in National Institute of Standards & Technology (*NIST Special Publication (SP) 800-30 Risk Management Guide for Information Technology Systems*, (*NIST Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems*).
- ▶ Accordingly, the security controls selected from the *NIST SP 800-53 moderate* impact level were used to identify the common and unique risk elements associated with processing, storing and transmitting Federal tax information in agency computing environments.
- ▶ The sequencing of security controls into **management, operational and technical security categories** achieves the mission of the Safeguards Program Office, fosters consistency with the organizational structure of *NIST SP 800-53* controls, and conforms with the security control classifications promulgated by the Office of Management & Budget (OMB).
- ▶ The control selection and specification process was based on the *NIST SP 800-53* security profile for information protection requirements commensurate with the moderate impact level.



Security Control Organization and Structure

- ▶ The new security controls in the updated Pub. 1075 are organized into *classes* and *families* for ease of use in the control selection and specification process.
- ▶ There are three general classes of security controls:
 - **Management**
 - **Operational**
 - **Technical**
- ▶ Each family contains security controls related to the security function of the family.

CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Security Assessments
Operational	Personnel Security
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection



Pub. 1075 Computer Security Control Requirements

► Management Security Controls

Management security controls focus on managing organizational risk and information system security, and devising sufficient countermeasures or safeguards for mitigating risk to acceptable levels.

Management security control families include:

- Risk Assessment
- Security Planning
- System and Services Acquisition
- Security Assessment



Pub. 1075 Computer Security Control Requirements

► Risk Assessment Defined

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Risk Assessment:

- Risk Assessment Policy & Procedures - develop, document, disseminate and update risk assessment policy and procedures to facilitate implementation of risk assessment controls.
- Risk Assessment - conduct assessments of risk to determine the potential magnitude of harm resulting from unauthorized use, disclosure and destruction of the information system and information.
- Risk Assessment Update - update risk assessments to reflect significant changes in conditions affecting the information system and its facilities.



Pub. 1075 Computer Security Control Requirements

▶ Security Planning Defined

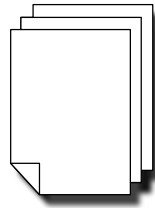
Organizations must develop security requirements for the information system and describe the security controls in place or planned for meeting those requirements.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Security Planning:

- Security Planning Policy & Procedures - develop, document, disseminate and update security planning policy and procedures to facilitate implementation of security planning controls.
- Rules of Behavior - establish and disseminate a set of rules to users of the information system describing their responsibilities and expected behavior with regards to information system use.



Pub. 1075 Computer Security Control Requirements

▶ System and Services Acquisition Defined

Organizations must:

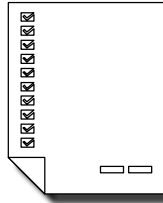
- (i) allocate sufficient resources to adequately protect organizational information systems;
- (ii) employ system development life cycle processes that incorporate information security considerations;
- (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect outsourced organizational information, applications, and/or services.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for System and Services Acquisition:

- System & Services Acquisition Policy & Procedures - develop, document, disseminate and update system and services acquisition policy and procedures to facilitate implementation of system and services acquisition controls.
- Information System Documentation - ensure adequate documentation for the information system is available, protected when required and disseminated to authorized parties.
- Outsourced Information System Services - ensure third-party providers of information system services employ adequate security controls consistent with applicable laws, directives, policies, regulations, standards, guidance and established service level agreements.



Pub. 1075 Computer Security Control Requirements

▶ Security Assessment Defined

Organizations must:

- periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;
- develop and implement plans of action designed to correct deficiencies and eliminate vulnerabilities in organizational information systems;
- authorize the operation of organizational information systems and any associated information system connections; and
- monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Security Assessment:

- Security Assessment Policy & Procedures - develop, document, disseminate and update security assessment policy and procedures to facilitate implementation of security assessment controls.
- Security Assessments - assess security controls (e.g., at least annually) in the information system to determine if controls are implemented correctly and operating as intended.
- Plan of Action & Milestones - develop, document and update plan of action and milestones for the information system to include corrective actions to mitigate or eliminate vulnerabilities identified in the security assessment.
- Continuous Monitoring - perform routine monitoring of security controls in the information system.



Pub. 1075 Computer Security Control Requirements

▶ Operational Security Controls

Operational security controls focus on mechanisms primarily implemented by people as opposed to systems. These controls are established to improve the security of a group, a specific system or group of systems. Operational security controls require technical or specialized expertise and often rely on management and technical security controls.

Operational security control families include:

- **Personnel Security**
- **Contingency Planning**
- **Configuration Management**
- **Maintenance**
- **System and Information Integrity**
- **Incident Response**
- **Awareness and Training**



Pub. 1075 Computer Security Control Requirements

▶ Personnel Security Defined

Organizations must:

(i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions;

(ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and

(iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Personnel Security:

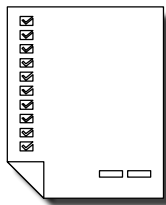
- Personnel Security Policy & Procedures - develop, document, disseminate and update personnel security policy and procedures to facilitate implementation of personnel security controls.
- Position Categorization - assign risk designations to all positions and establish screening criteria for individuals filling those positions.
- Personnel Screening - screen individuals before authorizing access to information systems and information.
- Personnel Security Policy & Procedures - develop, document, disseminate and update personnel security policy and procedures to facilitate implementation of personnel security controls.
- Position Categorization - assign risk designations to all positions and establish screening criteria for individuals filling those positions.
- Personnel Screening - screen individuals before authorizing access to information systems and information.



Pub. 1075 Computer Security Control Requirements

▶ Contingency Planning Defined

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Contingency Planning:

- Contingency Planning Policy & Procedures - develop, document, disseminate and update contingency planning policy and procedures to facilitate implementation of contingency planning security controls.
- Alternate Storage Sites - identify alternate storage site and initiate necessary agreements to permit the storage of information system and information backups.
- Telecommunications Services - identify primary and alternate telecommunications to support the information system and initiate necessary agreements to permit resumption of mission-critical / business functions when the primary telecommunications capabilities are unavailable.
- Information System Backup - conduct backups of user-level and system-level information in the information system and stores backups at a secure location.



Pub. 1075 Computer Security Control Requirements

► Configuration Management Defined

Organizations must:

- (i) establish and maintain baseline configurations and inventories of organizational information systems;
- (ii) establish and enforce security configuration settings for organizational information systems; and
- (iii) monitor and control changes to the baseline configurations and to the constituent components of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.



Pub. 1075 Computer Security Control Requirements

► Key Attributes to Meeting Requirements for Configuration Management:

- Configuration Management Policy & Procedures - develop, document, disseminate and update configuration management policy and procedures to facilitate implementation of configuration management security controls.
- Access Restriction for Change - enforce access restrictions associated with changes to the information system.
- Configuration Settings - configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.
- Least Functionality - configure the information system to provide only essential capabilities and prohibit the use of functions, ports, protocols and services.



Pub. 1075 Computer Security Control Requirements

► Maintenance Defined

Organizations must:

- (i) perform periodic and timely maintenance on organizational information systems; and
- (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.



Pub. 1075 Computer Security Control Requirements

► Key Attributes to Meeting Requirements for Maintenance:

- System Maintenance Policy & Procedures - develop, document, disseminate and update system maintenance policy and procedures to facilitate implementation of system maintenance security controls.
- Maintenance Tools - approve, control and routinely monitor the use of information system maintenance tools.
- Remote Maintenance - approve, control and routinely monitor remotely-executed maintenance and diagnostic activities.



Pub. 1075 Computer Security Control Requirements

▶ System and Information Integrity Defined

Organizations must:

- (i) identify, report, and correct information and information system flaws in a timely manner;
- (ii) provide protection from malicious code at appropriate locations within organizational information systems; and
- (iii) monitor information system security alerts and advisories and take appropriate actions in response.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for System and Information Integrity:

- System & Information Integrity Policy & Procedures - develop, document, disseminate and update system and information integrity policy and procedures to facilitate implementation of system and information integrity security controls.
- Flaw Remediation - identify, report and correct information system flaws.
- Malicious Code Protection - information system implements malicious code protection that includes capability for automatic updates.
- Intrusion Detection Tools & Techniques - employ tools and techniques to monitor events, detect attacks and identify unauthorized use of the information system.
- Information Input Restrictions - restrict input to the information system to authorized personnel only.
- Information Output Handling & Retention - handle and retain output from the information system according to organizational policy and procedures.



Pub. 1075 Computer Security Control Requirements

► Incident Response Defined

Organizations must:

- (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and
- (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.



Pub. 1075 Computer Security Control Requirements

► Key Attributes to Meeting Requirements for Incident Response:

- Incident Response Policy & Procedures - develop, document, disseminate and incident response policy and procedures to facilitate implementation of incident response controls.
- Incident Response Training - train personnel in their incident response roles and responsibilities with respect to the information system.
- Incident Monitoring - routinely track and document information system security incidents.



Pub. 1075 Computer Security Control Requirements

▶ Awareness and Training Defined

Organizations must:

(i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and

(ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Awareness and Training:

- Security Awareness & Training Policy & Procedures - develop, document, disseminate and update security awareness and training policy and procedures to facilitate implementation of security awareness and training controls.
- Security Awareness - ensure all users (including managers and senior executives) are cognizant of, or exposed to, basic information security awareness material before authorizing access to the system.
- Security Training - identify personnel with significant information system security roles and responsibilities, document those roles and responsibilities and provides sufficient information system security training before authorizing access to the system.



Pub. 1075 Computer Security Control Requirements

► Technical Security Controls

Technical security controls focus on the security controls executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system.

Technical security control families include:

- **Identification and Authentication**
- **Access Control**
- **Audit and Accountability**
- **System and Communications Protection**



Pub. 1075 Computer Security Control Requirements

► Identification and Authentication Defined

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Identification and Authentication:

- Identification & Authentication Policy & Procedures - develop, document, disseminate and update identification and authentication policy and procedures to facilitate implementation of identification and authentication controls.
- User Identification & Authentication - information system uniquely identifies and authenticates users (or processes acting on behalf on users).
- Identifier Management - manage user identifiers by uniquely identifying each user, verifying the identity of each user, receiving authorization to issue a user identifier, ensuring user identifier is issued to intended individual, disabling user identifiers timely, and archiving user identifiers.



Pub. 1075 Computer Security Control Requirements

▶ Access Control Defined

Organizations must limit information system access to authorized users, processes acting on behalf of users, or devices (including other information systems) and to the types of transactions and functions that users are permitted to exercise.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Access Control:

- Access Control Policy & Procedures - develop, document, disseminate and access control policy and procedures to facilitate implementation of access control security controls.
- Account Management - manage information system accounts including establishing, activating, changing, reviewing, disabling and removing accounts.
- Access Enforcement - information system enforces assigned authorizations for controlling access to the system.
- Information Flow Enforcement - information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems.
- Separation of Duties - information system enforces separation of duties through assigned access authorizations.
- Least Privileges - information system enforces the most restrictive access capabilities needed by users (or processes acting on behalf of users) to perform specified tasks.
- Unsuccessful Login Attempts - the information system: enforces a limit to the number of consecutive unsuccessful access attempts allowed in a specified period; and automatically performs a specific function (e.g., account lockout, delayed logon) when the maximum number of these attempts is exceeded.
- System Use Notification - information system displays an approved, system usage notification before granting system access informing potential users that: the system contains U.S. Government information, users actions are monitored and audited, and unauthorized use of the system is prohibited and subject to criminal and civil penalties.



Pub. 1075 Computer Security Control Requirements

▶ Audit and Accountability Defined

Organizations must:

- (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and
- (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Audit and Accountability:

- Audit & Accountability Policy & Procedures - develop, document, disseminate and update audit and accountability policy and procedures to facilitate implementation of audit and accountability security controls.
- Auditable Events - information system generates audit records for security-relevant events.
- Content of Audit Records - information system captures sufficient information in audit records to establish what events occurred, sources of events and outcome of events.
- Audit Storage Capacity - allocate sufficient audit record storage capacity and configure auditing to prevent capacity from being exceeded.
- Audit Processing - information system performs specific actions (e.g., shutdown, stop generating audit records, alerts system administrators) in the event of audit failure or audit storage capacity being reached.
- Audit Monitoring, Analysis and Reporting - routinely review / analyze audit records for indications of unusual activities, suspicious activities or suspected violations; reports findings to appropriate officials for resolution.
- Time Stamps - information system provides time stamps for use in audit record generation.
- Protection of Audit Information - information system protects audit information and audit tools from unauthorized access, modification and deletion.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for Audit and Accountability, *continued*:

- Audit Retention - retain audit logs for a predetermined period to support after-the-fact investigations of security incidents and comply with regulatory and organizational requirements.
- Audit Processing - information system performs specific actions (e.g., shutdown, stop generating audit records, alerts system administrators) in the event of audit failure or audit storage capacity being reached.
- Audit Monitoring, Analysis and Reporting - routinely review / analyze audit records for indications of unusual activities, suspicious activities or suspected violations; reports findings to appropriate officials for resolution.
- Time Stamps - information system provides time stamps for use in audit record generation.
- Protection of Audit Information - information system protects audit information and audit tools from unauthorized access, modification and deletion.
- Audit Retention - retain audit logs for a predetermined period to support after-the-fact investigations of security incidents and comply with regulatory and organizational requirements.



Pub. 1075 Computer Security Control Requirements

▶ System and Communications Protection Defined

Organizations must:

- (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and
- (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.



Pub. 1075 Computer Security Control Requirements

▶ Key Attributes to Meeting Requirements for System and Communications Protection:

- System & Communications Protection Policy & Procedures - develop, document, disseminate and update system and communications protection policy and procedures to facilitate implementation of system and communications protection controls.
- Information Remnants - information system prevents unauthorized and unintended information transfer via shared resources.
- Transmission Confidentiality - information system protects the confidentiality of transmitted information.
- Use of Validated Cryptography - when cryptography is employed within the information system, the system performs all cryptographic operations using FIPS 140-2 validated cryptographic modules with approved modes of operation.



Pub. 1075 Computer Security Control Updates: Supplementary Information

- ▶ Technical security controls focus on the security controls executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system. Technical security control families include identification and authentication, access control, audit and accountability, and system and communications protection.
- ▶ The following exhibits included in the new Pub. 1075 contain information that is intended to clarify the new technical controls:

Exhibit 8, Security Controls Catalog – reference guide to the selected specific controls for management, operational and technical family framework.

Exhibit 9, Password Management Guidelines – non-platform specific password security guidelines.

Exhibit 10, System Audit Management Guidelines – non-platform specific audit security guidelines.



PUBLICATION 1075 – GAP ANALYSIS

No	NIST 800-53 Family	NIST 800-53 Control	TCSEC C2 Cat 1	TCSEC C2 Cat 2
Management Control Class				
1	Risk Assessment	Risk Assessment Policy & Procedures	GAP	GAP
2	Risk Assessment	Risk Assessment	Life Cycle Assurance (P)	Security Testing (P)
3	Risk Assessment	Risk Assessment Update	GAP	GAP
4	Security Planning	Security Planning Policy & Procedures	GAP	GAP
5	Security Planning	Rules of Behavior	GAP	GAP
6	System & Services Acquisition	System & Services Acquisition Policy & Procedures	GAP	GAP
7	System & Services Acquisition	Information System Documentation	Documentation	Security Features User Guide Trusted Facility Manual Design Documentation
8	System & Services Acquisition	Outsourced Information System Services	GAP	GAP
9	Security Assessments	Security Assessment Policy & Procedures	GAP	GAP
10	Security Assessments	Security Assessment Policy & Procedures	GAP	GAP
11	Security Assessments	Security Assessments	Life Cycle Assurance Documentation	Security Testing Test Documentation
12	Security Assessments	Plan of Action & Milestones	GAP	GAP
13	Security Assessments	Continuous Monitoring	GAP	GAP

LEGEND:

GAP – Denotes security category associated with new 800-53 based framework was not covered under old C2 framework.
(P) – Denotes security category associated with new 800-53 based framework is partially covered under old C2 framework.



PUBLICATION 1075 – GAP ANALYSIS *Continued*

No	NIST 800-53 Family	NIST 800-53 Control	TCSEC C2 Cat 1	TCSEC C2 Cat 2
Operational Control Class				
1	Personnel Security	Personnel Security Policy & Procedures	GAP	GAP
2	Personnel Security	Position Categorization	GAP	GAP
3	Personnel Security	Personnel Screening	GAP	GAP
4	Personnel Security	Personnel Termination	GAP	GAP
5	Personnel Security	Personnel Transfer	GAP	GAP
6	Personnel Security	Access Agreements	GAP	GAP
7	Contingency Planning	Contingency Planning Policy & Procedures	GAP	GAP
8	Contingency Planning	Alternate Storage Sites	GAP	GAP
9	Contingency Planning	Telecommunications Services	GAP	GAP
10	Contingency Planning	Information Backup	GAP	GAP
11	Configuration Management	Configuration Management Policy & Procedures	GAP	GAP
12	Configuration Management	Access Restrictions for Change	GAP	GAP
13	Configuration Management	Configuration Settings	Security Policy Accountability Accountability	Discretionary Access Control Audit Identification & Authentication
14	Configuration Management	Least Functionality	Security Policy	Discretionary Access Control
15	System Maintenance	System Maintenance Policy & Procedures	GAP	GAP

LEGEND:

GAP – Denotes security category associated with new 800-53 based framework was not covered under old C2 framework.
(P) – Denotes security category associated with new 800-53 based framework is partially covered under old C2 framework.



PUBLICATION 1075 – GAP ANALYSIS *Continued*

No	NIST 800-53 Family	NIST 800-53 Control	TCSEC C2 Cat 1	TCSEC C2 Cat 2
Operational Control Class <i>Continued</i>				
16	System Maintenance	Maintenance Tools	GAP	GAP
17	System Maintenance	Remote Maintenance	GAP	GAP
18	System & Information Integrity	System & Information Integrity Policy & Procedures	GAP	GAP
19	System & Information Integrity	Flaw Remediation	Operational Assurance (P) Operational Assurance (P)	System Architecture (P) System Integrity (P)
20	System & Information Integrity	Malicious Code Protection	Operational Assurance (P) Operational Assurance (P)	System Architecture (P) System Integrity (P)
21	System & Information Integrity	Intrusion Detection Tools & Techniques	GAP	GAP
22	System & Information Integrity	Information Input Restrictions	GAP	GAP
23	System & Information Integrity	Information Output Handling & Retention	GAP	GAP
24	Incident Response	Incident Response Policy & Procedures	GAP	GAP
25	Incident Response	Incident Response Training	GAP	GAP
26	Incident Response	Incident Monitoring	GAP	GAP
27	Security Awareness & Training	Security Awareness & Training Policy & Procedures	GAP	GAP
28	Security Awareness & Training	Security Awareness	GAP	GAP
29	Security Awareness & Training	Security Training	GAP	GAP

LEGEND:

GAP – Denotes security category associated with new 800-53 based framework was not covered under old C2 framework.
(P) – Denotes security category associated with new 800-53 based framework is partially covered under old C2 framework.



PUBLICATION 1075 – GAP ANALYSIS *Continued*

No	NIST 800-53 Family	NIST 800-53 Control	TCSEC C2 Cat 1	TCSEC C2 Cat 2
Technical Control Class				
1	Identification & Authentication	Identification & Authentication Policy & Procedures	Accountability (P)	Identification & Authentication (P)
2	Identification & Authentication	User Identification & Authentication	Accountability	Identification & Authentication
3	Identification & Authentication	Identifier Management	Accountability	Identification & Authentication
4	Access Control	Access Control Policy & Procedures	Security Policy (P)	Discretionary Access Control (P)
5	Access Control	Account Management	Security Policy	Discretionary Access Control
6	Access Control	Access Enforcement	Security Policy	Discretionary Access Control
7	Access Control	Information Flow Enforcement	Security Policy (P)	Discretionary Access Control (P)
8	Access Control	Separation of Duties	Security Policy	Discretionary Access Control
9	Access Control	Least Privilege	Security Policy	Discretionary Access Control
10	Access Control	Unsuccessful Login Attempts	Security Policy	Discretionary Access Control
11	Access Control	System Notification Use	Security Policy	Discretionary Access Control
12	Access Control	Session Lock	Security Policy	Discretionary Access Control
13	Access Control	Session Termination	Security Policy	Discretionary Access Control
14	Access Control	Remote Access	Security Policy	Discretionary Access Control
15	Audit & Accountability	Audit & Accountability Policy & Procedures	Accountability	Audit

LEGEND:

GAP – Denotes security category associated with new 800-53 based framework was not covered under old C2 framework.
(P) – Denotes security category associated with new 800-53 based framework is partially covered under old C2 framework.



PUBLICATION 1075 – GAP ANALYSIS *Continued*

No	NIST 800-53 Family	NIST 800-53 Control	TCSEC C2 Cat 1	TCSEC C2 Cat 2
Technical Control Class <i>Continued</i>				
16	Audit & Accountability	Auditable Events	Accountability	Audit
17	Audit & Accountability	Content of Audit Records	Accountability	Audit
18	Audit & Accountability	Audit Storage Capacity	Accountability	Audit
19	Audit & Accountability	Audit Processing	Accountability	Audit
20	Audit & Accountability	Audit Monitoring, Analysis & Reporting	Accountability (P)	Audit (P)
21	Audit & Accountability	Time Stamps	Accountability	Audit
22	Audit & Accountability	Protection of Audit Information	Accountability	Audit
23	Audit & Accountability	Audit Retention	Accountability (P)	Audit (P)
24	System and Communications Protection	System and Communications Protection Policy & Procedures	GAP	GAP
25	System and Communications Protection	Information Remnants	Security Policy	Object Reuse
26	System and Communications Protection	Transmission Confidentiality	Communications Infrastructure	Communications Infrastructure
27	System and Communications Protection	Use of Validated Cryptography	Communications Infrastructure (P)	Communications Infrastructure (P)

LEGEND:

GAP – Denotes security category associated with new 800-53 based framework was not covered under old C2 framework.
(P) – Denotes security category associated with new 800-53 based framework is partially covered under old C2 framework.



Pub. 1075 Transition Period

- ▶ Suggested transition date is March, 2007.
- ▶ To satisfy the current computer system security requirements outlined in the current Pub. 1075, agencies should:
 - Meet the current computer security requirements specified in the current Department of Defense Trusted Computer System Evaluation Criteria (TCSEC).
- ▶ To satisfy the new computer system security requirements outlined in the updated Pub. 1075 (soon to be released) agencies should:
 - Meet the new computer security control requirements specified in the updated Pub. 1075.



Questions

