FEDERAL AUDIT
EXECUTIVE COUNCIL COMMITTEE
"AUDITING IN A PAPERLESS ENVIRONMENT"

AUDITING INFORMATION SYSTEM SECURITY

SEPTEMBER 1999

FEDERAL AUDIT
EXECUTIVE COUNCIL COMMITTEE

"AUDITING IN A PAPERLESS ENVIRONMENT"

AUDITING INFORMATION SYSTEM SECURITY

By

Arnold J. Pettis (AFAA)
LeRoy Stewart (AFAA)
Jim Rothwell (EPA)
Bill Coker (DoDIG)
Tony Broadnax (DLA)
Jim Raube (AFAA)

Compiled and Edited by
Jim Raube (AFAA)

TABLE OF CONTENTS

INTRODUCTION

Information system security for unclassified computer systems is one of the top issues government organizations face today. This developed as government migrated from a closed architecture, limited-access, mainframe environment to a web-based, client/server architecture where literally the world may access government systems. The U.S. General Accounting Office (GAO) confirmed this reality in a series of reports to the Congress. For example, in February 1997, GAO designated information system security as a "new government-wide, high-risk area." Also, the GAO March 31, 1998 report on the federal government's consolidated financial statements reported that "widespread and serious computer control weaknesses affect virtually all federal agencies and significantly contribute to many material deficiencies in federal financial management."

Internal audit can assist management by identifying areas to strengthen in the information system security area. Accordingly, the Federal Audit Executive Council committee, Auditing in a Paperless Environment, established a subcommittee to (1) define the information system security problem and (2) provide potential approaches, including software tools, to assist in auditing information system security. The subcommittee consisted of members from the Air Force Audit Agency, Defense Logistics Agency, Environmental Protection Agency, and Office of Inspector General, Department of Defense. Appendix XI provides biographies of subcommittee members.

To define the information system security problem within the government, the subcommittee focused on a recent report issued by the GAO entitled *INFORMATION SECURITY—Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92), dated September 1998. This report concluded that "important operations at every major federal agency are at some type of risk due to weak information system security controls." To support that conclusion, this report summarized significant information system security weaknesses within 24 federal agencies as identified in audit reports issued from March 1996 through August 1998. The report also provided management practices federal agencies can adopt to improve their security programs.

The GAO report categorized information system security problems into six basic areas: security program planning and management, access control, application program change control, segregation of duties, operating systems security, and service continuity. Our committee considered these categories as the defined problem and compiled audit procedures to assist internal audit organizations in reviewing each area (Appendices I through VI). Also, our report includes a compendium of information system security criteria (Appendix VII), a sampling of information system security training available (Appendix VIII), a table of information system security internet addresses (Appendix IX), and an Information System Security Directive Matrix (Appendix X) cross-referenced to information system application and general control criteria.

INFORMATION SYSTEM SECURITY CONTROL WEAKNESSES

The following excerpts from the GAO report list and describe the six deficient information system security areas referred to in our Introduction. The referenced appendices provide recommended methodologies for auditing these areas.

Entity-Wide Security Program Planning. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, requires all federal organizations to develop an information system security plan. In addition to this regulatory requirement, a complete and effective information system technology security plan is an essential management control and the cornerstone for any successful information system security program. Without an effective security plan, organizations will very likely overlook key security controls and face a very real possibility of intrusion. As such, the auditor's first step in any information system security audit should be to review the adequacy of the information system security plan. Of 17 agencies where this aspect of security was reviewed, the GAO review found that all had deficiencies. Many agencies had not developed security plans for major systems based on risk, had not formally documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on. Appendix I provides guidance to evaluate this area.

Access Controls. These limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protection, such as gates and guards, and logical controls built into the software. Logical controls include (1) requiring users to authenticate themselves through the use of secret passwords or other identifiers and (2) limiting the files and other resources that an authenticated user can access and the actions that he or she can execute. Access control weaknesses were reported for all 23 of the agencies for which this area of controls was evaluated. Appendix II provides guidance to evaluate this area.

Application Software Development and Change Controls. These controls prevent unauthorized software programs or modification to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved before implementation, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and ensure that different versions are not misidentified. Weaknesses in software program change controls were identified for 14 of the 18 agencies where such controls were evaluated. Appendix III provides guidance to evaluate this area.

Segregation of Duties. This refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and, thereby, conduct unauthorized actions or gain unauthorized access to assets or records without detection. Weaknesses were identified at 16 of the 17 agencies where this control was evaluated. Appendix IV provides guidance to evaluate this area.

System Software Controls. These controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on the system. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information system programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Weaknesses were identified at all nine agencies where this control was evaluated. Appendix V provides guidance to evaluate this area.

Service Continuity Controls. These controls ensure that, when unexpected events occur, critical operations continue without undue interruption and critical and sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information system resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. Weaknesses were identified at all 20 agencies where this control was evaluated. Appendix VI provides guidance to evaluate this area.

PERSPECTIVE

In developing this audit guide, our committee researched the wide body of knowledge already available to assist auditors in evaluating information system security. Our report refers the reader to those sources identified. We also developed audit steps to supplement those areas that we could not locate relevant audit guidance.

We generally avoided audit guidance related to auditing "closed architecture" systems (e.g., computer mainframes secured in locked computer facilities "hard-wired" to each other and to computer terminals also located in relatively secure areas). This type of service environment is rapidly disappearing and constitutes a much lower security risk than a web-based, multi-platform, networked client/server system (hereinafter referred to as a web-based system).

Our audit guidance focuses on web-based systems generally consisting of computers inter-connected by telecommunication lines and also connected to the internet for maximum communications flexibility. From a security perspective, however, this same flexibility creates unlimited opportunities to illegally access government systems, thereby enabling intruders to extract information and create havoc within those systems.

This publication cites numerous web site addresses that were current as of July 1, 1999. Because these addresses frequently change, we can not guarantee the accuracy of all web site addresses provided. However, the information can often be found at a different location on the same web site.

APPENDIX I

ENTITY-WIDE SECURITY PROGRAM PLANNING

National Institute of Standards and Technology (NIST) Guidance. The Federal Computer Security Program Managers' Forum, an organization sponsored by NIST, established a working group to develop a guideline for developing security plans for all federal information systems. This guideline is provided in NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998. The 102-page document provides comprehensive guidelines for security plans and could be used as an audit tool for evaluating security plans as well as a guide for developing the plan. NIST also issued an Information Technology Laboratory (ITL) Bulletin in April 1999 to summarize the purpose, responsibilities, format, and development of an effective security plan. Guides can be obtained from the Government Printing Office or downloaded from the NIST web site (http://csrc.nist.gov/nistpubs/).

GAO Guidance. Chapter 3.1 of the GAO *Federal Information System Controls Audit Manual (FISCAM)*, GAO/AIMD-12.19.6, January 1999, provides guidance for evaluating and testing security program planning. Obtain FISCAM copies from the GAO or from its web site (http://www.gao.gov).

APPENDIX II

ACCESS CONTROLS

Background. Access controls should provide reasonable assurance that the information processed, stored, and transiting the network maintains its confidentiality, availability, integrity, and accountability. When implementing security, control, and audit policies, balance access control requirements and the use of security features against user needs, application requirements, and overall system performance. Chapter 3.2 of the GAO FISCAM provides guidance for auditing access controls. The information that follows supplements that guidance.

Network Configuration. The typical network consists of the backbone and organizational local area networks (LANs). The backbone provides customers with the information resources needed to achieve their operational objectives. This backbone normally consists of communications media, routers, gateways, and other types of communications equipment. Through the use of network management systems, firewalls, and intrusion detection and vulnerability assessment tools, the network manager performs network management and problem resolution for the backbone. Organizational LANs connect to the backbone for intranet and internet connectivity. These LANs provide office automation services for the unit and are frequently managed by system administrators assigned to that unit. Organizational LANs normally consist of servers (file, mail, and web), networking devices (routers, bridges, etc.), media, user workstations, and printers.

Security Event Log. This log records security events, thereby helping the administrator to track changes to the security system and identify possible security breaches. Audit policy determines which events the operating system will track in the security event log. As a minimum, the security event log should record log-on and log-off; file and object access; user and group management; security policy changes; and restart, shutdown, and system boot. Auditors should review the logs periodically to ensure security policies are enforced, monitor sensitive activities (such as changes to security), and identify problem areas. For example, the security event log would record if anyone were trying to break into the system through multiple attempts with various password combinations.

Control Activity	Control Technique	Audit Procedure
Auditing	Events to be audited.	**Identification and authentication** (I&A) should be tracked and retained. Audit both successful and unsuccessful log-ons and log-offs. Track all system restarts, unsuccessful attempts to alter file permissions, unsuccessful access attempts to the audit or password files, and remote system accesses. **Automated or Manual Audit Policy**. Use an automated audit log. **Time-out Policy**. Protect normal connections by a password-protected screen saver when the workstation is left unattended. Terminate inactive sessions after 8 hours. **Retention of Audit Records**. Maintain audit records for 90 days. This includes both audit records generated by network servers and workstations. **Audit Review**. The system administrator should review audit logs daily. **Protection of Audit Files**. Protect audit files through file permissions.

Identification and Authentication. User access administration involves both obtaining the appropriate approvals before granting a user access to the system and then setting up the user on the system. User rights authorize a group or user to perform specific actions on the system. The overall system level of security is sensitive to the way rights are assigned and who has them. A responsible person should administer and monitor the user rights policy to ensure adherence to management policy.

Log-on Control. System entrance (log-on) control is essential. This is the initial point of contact a user has with the system. If log-on is not properly set up and protected, unauthorized users may gain entrance into the system. Exit (log-off) control is also essential because if an authorized user has not completely exited the system, an unauthorized user may use the open line for entrance and navigation within the system. The account policy controls passwords and contains the account lockout setting, an important component of log-on control that prevents an intruder from gaining access to the system by guessing a password. The auditor should understand that some systems provide the administrator only with very basic password standards, namely, minimum and maximum length and age, expiration interval, and password history.

Control Activity	Control Technique	Audit Procedure
Identification and Authentication	Identification and authentication mechanism on the network.	**Method of Access Control.** Employ discretionary access control (DAC). DAC provides the ability to control a user's access to information according to the authorization granted the user. It provides the data owner (individual user or groups) a capability to specify permissions (read, write, delete, or execute) to information for each of their files and programs contained in the network. Files do not require internal classification labels. **Password Length**. Passwords must be at least eight characters long and consist of alphanumeric characters with at least one special character. **Password Generation**. Use machine or user-generated passwords. Usually, the base network employs user-generated passwords. The system administrator will assign an initial password the user must change on the first use. Check the strength of passwords by running an approved password cracking program. Note: The need for a password cracking program reduces significantly if the system locks out accounts after three failed log-on attempts (see **Password Lock-outs** below). **Password Protection**. Protect passwords as sensitive For Official Use Only (FOUO). **Changing Passwords**. Change passwords every 90 days. The minimum time for password change is 2 days. Former passwords will not be used for at least 6 months. **Password History**. Enable the "password uniqueness" feature to prevent users from re-using the same password, thereby preventing hackers from logging in to an account using a previously discovered password. **Password Lock-outs**. Lock out accounts after three consecutive failed log-on attempts. System administrators must not reinstate passwords without positive identification of the authorized user. **Password Disclosure**. Users must memorize their passwords. **System Administrator and User Privileges**. Limit system administrator (root) privileges to the least possible number. **Password Manager**. Assign a password manager.

		Dial-in Access. Log and authenticate use of dial-in services, and brief users on the risks associated with dial-in access. Users should sign a statement acknowledging they have been briefed and they understand and accept the responsibility for enforcing security procedures and requirements. Maintain a list of personnel having dial-in access. Dial-in hardware or software will disconnect sessions after 15 minutes of inactivity. The hardware or software may warn the user five minutes prior to disconnection. The host organization should permit access only to those services and data required by the remote users to perform their functions. Do not publicize modem telephone numbers, and provide the numbers only to those with a need-to-know. **Remote Maintenance**. Allow remote software diagnostics or maintenance only if the system audits such activities or if an appropriately cleared individual (capable of identifying unauthorized activity) observes such activities. The system being remotely maintained will authenticate the identity of the maintenance personnel. When suspending maintenance activities, disconnect or disable maintenance access to the system.

Personnel Security. Base your security policy on the rule of "least privilege" (i.e., users have the minimum required amount of privileges and access necessary to perform their jobs). As information becomes more critical to the continued effective operation of an organization and its organizational units, data security has increased importance.

Control Activity	Control Technique	Audit Procedure
Personnel Security.	Personnel security program	**Security Clearances**. Ensure all persons accessing the network have the required security clearances. **Need to Know**. Although users may have the required clearance, restrict access to those who have a need to know.

Network Sustainment. The overall goal of physical security is to protect information systems and the people who operate and maintain them. Physical security helps to protect against human threats by limiting or controlling physical access to the equipment. The auditor should evaluate management policies and practices to ascertain whether the necessary policies exist and determine whether they are properly followed. The auditor should determine whether security provisions for computer hardware, software, data files, data transmission, input and output material, and personnel are adequate. This review should include computer equipment in the central processing facility as well as minicomputers, remote terminals, communications operations, and other peripheral equipment.

Control Activity	Control Technique	Audit Procedure
Network Sustainment.	Information Protection	**Entry Control**. The facility manager must control entry to the network facility. Network users are responsible for the positive identification of individuals attempting to access network assets. **Resource Protection**. The network consists of high value items (both physically and logically) subject to pilferage. Physical resources are the network equipment, physical storage media, and the physical environment (site). Logical resources encompass data and software. **Physical Resource Protection**. Protect network resources from natural threats, physical disasters, human threats, and any other identified physical threat. **Logical Resource Protection**. Back up servers daily, and retain for a minimum of 1 month. Store all removable media in a secure location. An additional removable hard drive may be used as the backup. Mark, store, and handle the backups as Sensitive.

Hardware/Software. To protect against software "bugs" and other design flaws, management should establish sound, practical configuration management procedures based on NCSC-TG-006, A Guide to Understanding Configuration Management in Trusted Systems. Are configuration management procedures documented in writing, possibly in a Configuration Management Plan? Does trusted software have configuration management controls and some form of trusted distribution to ensure its integrity?

Viruses have cost organizations millions of dollars through corrupted data and the personnel time to repair the damage. A virus destroys by attaching itself to a legal procedure and modifying it so that the virus code gains control when the legal procedure is invoked by a legitimate user. Users can bring viruses into the network, unwittingly or deliberately, from external sources, such as games on floppy disks, files from unprotected

home computers, and programs downloaded from infected electronic bulletin boards. To help protect against viruses, users should install a virus detection program, update it regularly, and run it continuously. A combination of effective system features and administrative procedures can effectively eliminate the virus threat.

A Trojan horse is typically designed to mimic a system's standard log-on procedure in order to read (and store away) sensitive data such as the user's log-on name and password. The author of the Trojan horse can later retrieve the hidden name and password and use them to access the system. Systems can effectively eliminate Trojan horses by providing a controlled log-on channel through the disciplined standard procedure system boot sequence. If this is done, rogue procedures cannot execute before the user initiates the log-on sequence; however, the Trojan horse may still fool trusting users into divulging their usernames and passwords by displaying a fake log-on screen. Therefore, users should always use the disciplined standard log-on procedure even if the invitation to log on is already displayed.

Control Activity	Control Technique	Audit Procedure
Hardware/ Software.	Hardware and software security features that provide controlled access protection are not by-passed or disabled.	**Configuration Management**. The network manager conducts configuration management for the backbone. Network managers and/or system administrators conduct configuration management for organizational LANs. Managers or administrators must coordinate significant changes to the network configuration (e.g. additional servers or new operating system) with the local configuration control board (CCB) and subsequently document those changes in the system architecture section of the network accreditation package. **Software Use**. Users must follow the guidelines for software security. Also, restrict access for diagnostic programs and security-critical software to authorized personnel. Limit public domain software for mission accomplishment only and approve usage on a case-by-case basis. **Database Management Systems (DBMS) in a multi-user environment.** The database should complement the operating system audit trail with its own audit trail to protect the data to its lowest identifiable element. **Securing Directories, Files, and Objects**. Examine each shared physical network disk and document each partition on the physical disk, its drive letter (C, D, etc.) and the corresponding file system (NTFS, FAT, or HPFS), and CDROM drives identified as the CDFS file type. **Controlled Access Protection (CAP) Products**. Use

		products listed in the National Security Agency's Evaluated Products List. **Y2K Compliance.** Networks whose lifespans extend beyond 1999 must have countermeasures in place to correct the Year 2000 vulnerability. Test for this vulnerability on all network components. For Y2K vulnerabilities not countered, determine corrective measures, seek approval from the network manager, and document them in the network's accreditation documentation. **Virus Detection Software**. To protect against malicious logic, does the system use anti virus software such as virus scanning programs, anti virus programs which form a protective "wrap" around executable code, or programs using cyclical redundancy checks (CRC) to verify code integrity?

System Maintenance. Computer systems are typically controlled by an operating system that provides data handling and multiprogramming capabilities, file label checking, authorization controls, and general controls over computer processing. System administrators should monitor new versions of the operating system to ascertain their compatibility with application software currently in use, regardless of whether the application software was developed commercially or in house. The auditor should know the operating system controls and ascertain the extent to which they have been implemented as well as how they can be bypassed or overridden. The auditor should also know that personnel who maintain the operating systems, as well as other individuals who are able to modify them, can either intentionally or accidentally cause specific controls within the operating systems to become ineffective.

Control Activity	Control Technique	Audit Procedure
System Maintenance.	In-house maintenance on the network.	**Hardware Maintenance**. Workgroup managers and system administrators perform initial troubleshooting and component replacement. Purge all sensitive information before releasing equipment for contract maintenance. **Software Maintenance.** Remote diagnostics must be restricted (e.g., length of remote session, authorized personnel) and approved by the network manager. The system administrator conducts software maintenance and installs vendor patches.

Incident and Vulnerability. A technical vulnerability is a hardware, software, or network communications weakness or design deficiency that leaves a system open to potential exploitation, either externally or internally. This, in turn, increases risk of compromise of information, alteration or destruction of information, or denial of service.

An administrative vulnerability is a system security weakness caused by incorrect or inadequate implementation of security features by the system administrator, security officer, or users. Correct vulnerabilities by changing the system implementation or by establishing special administrative or security procedures for the system administrators and users. Also, ensure all personnel know how to report any incident of unauthorized entry, or attempted entry, to a system (including browsing, viruses, disruption or denial of service, altered or destroyed input, processing, storage, or output of information).

Incident Reports. Review all reports from the last 12 months. How many reports reference changes to hardware, network communications, or software with or without the user's knowledge, instruction, or intent? Do all the reports ensure the operational instructions provided with both the system hardware and software have been followed, ensure the system is operating as specified, and ensure the problem is not the result of human or mechanical error? Does the security officer initiate formal reporting to the responsible computer security manager? Does the security officer follow the rules to determine the priority of the event and how quickly to report it? If the system processes classified information, are technical vulnerability reports classified only if exploitation of the vulnerability could result in compromise of classified information? (The report originator may classify the vulnerability to the same level as information processed on the system.) As a minimum, are all incident reports affecting unclassified systems marked FOUO? If the system processes classified, are all incident reports classified CONFIDENTIAL or higher?

Control Activity	Control Technique	Audit Procedure
Vulnerabilities and Incidents.	Reporting.	**Proper reporting** of newly discovered vulnerabilities and incidents ensures containment of impact, recovery of network availability, identification of breach and perpetrator, and countermeasure implementation. **Protecting.** All personnel implement security patches as appropriate.

Information Protection Tools. The pace and sophistication of attacks from hackers hunting for a thrill, disgruntled employees, and unethical contractors increases every day. Unless you understand your vulnerabilities, you can not balance potential threats against the reward of availability. The most efficient and effective way to understand your vulnerabilities is to incorporate an information protection tool in your network. Information protection tools provide the capability to secure system access and protect the information in networks, systems, applications, and internet initiatives. Learn more about securing your network and obtaining tools to do by visiting web sites at http://www.nha.com/products.htm and http://www.iss.net/prod/products.php3.

Control Activity	Control Technique	Audit Procedure
Information Protection Tools.	These tools perform numerous security functions including boundary protection, viral detection, configuration inspection, network mapping, remote patching, vulnerability testing, etc.	**Use**. Because of the intrusiveness of some IP tools and the sensitivity of the information that may be observed during IP operations, only designated personnel are authorized to use "intrusive" IP tools. **Training on IP Tools**. All personnel required to use IP tools must be trained on tool usage and the rules of engagement, either through approved courses or on-the-job training. **Types of Vulnerability Checks**. Test the following system functions: file transfer protocol, network device, Email, RPC, NFS, denial of service, password, web server, protocol spoofing, firewall, remote service, domain name service, file system, account, service, registry, security patches, browser, NIS, critical files obtainable, and information gathering.

Barrier Reef. Use the barrier reef policy stance to evaluate your network. Follow the audit procedures below to identify your network weaknesses or vulnerabilities.

Control Activity	Control Technique	Audit Procedure
Barrier Reef.	The Barrier Reef policy stance is "Allow authorized traffic and Deny all else."	**Know Thyself**. Identify and reduce exterior network access points to a manageable number. Conduct traffic analysis to determine the protocols and throughput that currently exist. Gather information on personnel security. **Requirements Determination**. Validate the traffic is mission-required. Gather information on type of hardware and software used by incorporating an information protection tool. **Policy Formation**. Create a network security policy involving all functional areas. Enumerate all allowable services and deny all that is not specifically allowed. Evaluate audit and account policies and configuration management to ensure compliance with regulatory standards. **Filter Packets**. Take advantage of existing router Access Control List (ACL) capabilities. Block as many unsafe services as possible based on Transmission Control Protocol/Internet Protocol (TCP/IP) headers. Validate the existence of firewalls and the use of controlled access protection tools. **Monitor Network**. Integrate network monitoring

		device(s) such as the Automated Security Incident Monitor (ASIM). Monitor outside the boundary protection mechanism to identify all attempted attacks. Include a review of physical and logical resource protection procedures. **Integrate Time Server**. Integrate a Global Positioning System (GPS) receiver to provide a reliable, accurate time source for base systems. Protect base from introduction of false time and compliance with year 2000 issues. **Centralize Dial-in Access**. Aggregate multiple remote log-in or dial-in solutions into one centralized service. Protect access through this service via strong authentication of users. **Proxy World-Wide Web Requests**. Direct all outgoing WWW requests through a WWW proxy device to hide users' identities from Internet eavesdroppers, reduce wide-area network utilization, and improve user response time. Provide positive control over web access to unauthorized sites. **Internet and Intranet Services**. Place the web servers in a "demilitarized" zone to reduce internal network access. Establish a system to keep public data updated and separate from internal web servers. Provide a public "lobby" for e-mail entry and access to data for wide distribution. **Proxy Common and Special Services**. Authenticate outside users before granting access for "dangerous" services (TELNET, FTP). Implement controlled access for specialized services (InfoConnect). **Conceal Network**. Hide internal network address space from public domain. Separate public and private domain name servers (DNS). Encrypt when necessary and increase the cipher strength on internet browsers to 128-bit. **Train, Maintain, and Certify**. Establish continuity for training, system changes, and upgrades. Certify and accredit the boundary protection system and base network. Train personnel on advisories and software maintenance (vendor patches), maintain in-house maintenance on hardware devices, and certify security and contingency plans.

APPENDIX III

APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROLS

Background. Application software development is a longstanding problem in the Federal Government. The GAO and Inspectors General (IGs) have issued numerous reports that identify computer control weaknesses in the federal government. Also, the 1996 President's Council on Integrity and Efficiency (PCIE) report on application software maintenance by the federal government concluded that software maintenance costs were not properly accounted for or identified; software maintenance contracts and oversight were inadequate; and organizations were not adequately managing software change control processes to ensure software integrity. Chapter 3.3 of the GAO FISCAM provides guidance for auditing application software development and change controls. The information that follows supplements that guidance.

Computer Mainframe Software Systems Development. During the 1970s and 1980s, government and industry used complex, batch process, custom, and centralized applications that ran on large mainframes. Major systems took 3 to 5 years to develop and had a life cycle of 10 to 15 years. Management made all decisions to build and replaced the software based on a systems life cycle concept of building custom software. Management decisions to upgrade or replace the software were driven primarily by operations and by cost-benefit studies. As the system software become more complex, inefficient and costly to maintain, it was replaced. Security was not as big a concern because most systems ran on a mainframe in a closed environment.

Current Software Life Cycle. In today's environment, the systems development life cycle has shortened significantly. Current software life cycle for major systems typically is an off-the-shelf software with a life as low as 5 years, and current software life cycle for software upgrades is about 18 months. Enterprise resource and planning uses a shortened system development life cycle to adapt off-the-shelf software and re-engineer practices. Management first identifies its requirements (including security) and then evaluates available software to determine the best fit. Implementation of the off-the-shelf software is the baseline for the software configuration management. Change control primarily consists of upgrades provided by the software vendor or emergency fixes. Usually, systems use a complex, de-centralized environment including Internet access, multiple platforms (mainframe, local server, and personal computers) linked by local area networks. Security controls are in both the operating systems and application software. Custom application software serves as a supplement for off-the-shelf software to satisfy unique users needs.

Configuration Management. Controlling the modification of application software programs helps to ensure only authorized programs and modifications are put

into operations. Policies and procedures are used to make sure all application programs are authorized, tested, and approved, which becomes the baseline. The two primary security concerns are (1) security features in the baseline software could be turned off or inadvertently (or deliberately) omitted and (2) malicious or unauthorized code could be introduced into the baseline software. Configuration management is critical to maintaining system integrity.

Requirements. Several policy documents published by the Office of Management and Budget (OMB) address information systems and the need for specific controls. OMB Circular A-130, Management of Federal Information Resources, February 1996, establishes a minimum set of controls for Federal information system security programs. This circular implemented the Computer Security Act of 1987 and also required NIST to publish additional guidance. OMB Circular A-109, Major Systems Acquisition, April 1976, established the basic process for acquiring major systems. OMB Circular A-127 , Financial management Systems, July 1993, established policies and procedures for financial management systems. OMB Circular A-123, Management Accountability and Control, June 1995, addresses policies for establishing management accountability, control standards and reporting.

Additional Directive Guidance. Appendix VII provides a compendium of federal guidance on security and software development. Also, each organization has its own security and system development policies and procedures. For example, The Department of Defense DOD STD-2167A, Defense System Software Development (1988), establishes uniform requirements for system development and maintenance.

Audit Subject Areas. Audit review during system design and development is crucial for management to reasonably assure that systems under development have the necessary controls to include security as an integral part of the systems development and change control process. Software development audits should evaluate the contractor's processes, plans, and procedures to include system architecture, software engineering, software configuration management, testing, system integration, risk management, and corrective action. This process provides early notification to audit clients of potential problems that could impact cost, schedule, quality, and technical performance.

Audit Approach. The systems development life cycle should provide a structured approach for identifying and documenting the needed changes to computer software; assessing the costs and benefits of various options including off-the-shelf software; and designing, developing, and testing the software being placed in operation. The exact methodology is dependent on the organization's policies and procedures. In FISCAM Volume I, Chapter 3.3, the GAO provides general audit methodology for auditing software development. Also, NIST SP 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, April 1988, addresses controls and security in the software development life cycle.

Initiation Phase (System or Upgrade). The objective of this phase is to evaluate the alternative functional solutions, whether they be a custom in-house development or an off-the-shelf software program. The need(s) and purpose for a system should be documented in a preliminary security plan. Also, sensitivity of data to be processed should be identified and documented (see NIST PUB 800-18, 3.7, Sensitivity of Information Handled). Further, as part of the cost-benefit analysis, management should evaluate the impact of security, privacy, and internal control requirements under the alternative approaches. For further information on cost benefit analyses, consult a recently issued publication, Federal CIO Council, ROI, and The Value Puzzle, April 1999, at http:\\www.cio.gov. Upon completion of this phase, management selects the alternative to implement.

Development or Acquisition of Software Phase. The objective of this phase is to develop requirements that incorporate user needs, controls, and standards. These requirements should then be used to establish a project plan for developing custom software or a basis for evaluating off-the-shelf programs. Management should develop system security requirements during this phase to be addressed by the operating system software or the application software. (Most systems rely on the operational systems software for part of the security requirements.) When purchasing software off-the-shelf, the acquisition specifications should identify all requirements. It may take several software programs to meet these requirements. If management decides to develop custom software, security requirements must be identified and included in the software design. The systems design process should also identify independent verification, validation, and testing needed to certify the software.

Off-the-Shelf Software. If off-the-shelf software needs little modification, management may decide to go directly to independent verification, validation, and testing before acceptance. If the software needs minor modifications, management may decide to perform systems testing, field test the operations, and finalize a version for production. If the software requires major changes, management may need to establish a full systems development project. Also, the manufacturer should certify sensitive systems for technical adequacy before installation. For example, encryption processes should be certified as compliant with NIST standards.

Custom-Developed Software. Custom-developed software must be coded, tested, and accepted by users and management. This should include unit testing of specific code operation, systems testing to validate operations between the application and users, and integration testing to ensure the code operates in the desired operating environment. At test conclusion, management should independently validate the test results.

Implementation Phase. During system implementation, management should configure the system, enable security controls, and evaluate the effectiveness of security controls. If applying custom software, specific testing should ensure design specifications are functioning properly. Management should also provide an accreditation that the system is operating effectively and identify any restrictions as part of the accreditation.

Operation and Maintenance Phase. An approved security plan should document system security activity for the current system. The plan should address backups, training, cryptographic use, administrative policies and procedures, access controls (roles, passwords and other), security software, personnel controls, audits, and security reviews (see Appendix I). Management should authorize the system to process information based on an original assessment of system operational security controls and an updated assessment at least every 3 years.

Disposal Phase. This is the removal of the information from the application to another system or archive. The information should be sanitized from the media. Retention or destruction is based on the system Federal archiving record documents.

Control Activities. Management should authorize systems application software (custom or off-the-shelf) by using a Systems Development Life Cycle (SDLC) approach for design, development, maintenance, and disposal of software. Also, management should apply a disciplined process for testing and approving custom modifications, upgrading off-the shelf software, and programming emergency software changes. Finally, management should ensure approved software programs are protected from unauthorized changes and destruction. Auditors should review all these areas to ensure management has implemented the necessary controls.

APPENDIX IV

SEGREGATION OF DUTIES

Introduction. Separation of duties is a form of checks and balances where one person checks the work of another or no one person has complete control of a transaction from beginning to end. Conversely, the possibility of processing errors or malicious acts increases with policies and procedures that allow insufficient separation of duties. For instance, a computer programmer usually is not allowed to work in a production environment, and, if allowed to do so, the risk of erroneous or fraudulent acts occurring will increase.

Organization Size. Typically, as the size of an organization increases, a well-defined separation of duties will exist. However, with smaller organizations or distributed computing, the auditor will typically find duties that typically should be separated are assigned to the same person. This, in turn, increases the possible erroneous or fraudulent acts that could occur. As a result, management must recognize the increased risk, agree to an acceptable higher risk level, and compensate for the increased risk through a better review mechanism.

Audit Review. When reviewing separation of duties, an auditor should determine how an entity states it is organized versus how it actually is organized. To accomplish this, the auditor should review applicable organization charts and position descriptions and compare them to physical observation of tasks and interviews with personnel. This comparison could reveal possible insufficient separation of duties and thus, a possible unacceptable level of risk for management. Auditors should also obtain applicable exception reports and management's review of them. Also, the auditor should determine whether management has an acceptable level of risk or if the actual risk is greater than management outlines in its security plan.

Directive Guidance. Chapter 3.5 of the GAO FISCAM (GAO/AIMD-12.19.6, January 1999) provides comprehensive guidance for evaluating separation of duties. Obtain FISCAM copies from the GAO or from its web site (http://www.gao.gov).

APPENDIX V

SYSTEM SOFTWARE CONTROLS

GAO FISCAM. Chapter 3.4 of the GAO FISCAM (GAO/AIMD-12.19.6, January 1999) provides comprehensive guidance for evaluating system software controls. As defined by the FISCAM, system software is a set of programs designed to operate and control the processing activities of computer equipment. According to the FISCAM, system software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system. Some system software can change data and program code on files without leaving an audit trail. Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. Examples of systems software include operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

NIST Special Publication 800-12. This publication, An Introduction to Computer Security: The NIST Handbook, addresses application software development and change controls in Chapter 14 under "Configuration Management."

NIST Special Publication 800-18. This Guide for Developing Security Plans for Information Technology Systems provides further advice about system software maintenance controls (and is linked to application software development and change controls). These controls are used to monitor the installation of, and updates to, operating system software and other software to ensure that only authorized software is installed on the system. Typically system software maintenance controls include products and procedures used in auditing for, or preventing, illegal use of shareware or copyrighted software. Issues and questions suggested by NIST SP 800-18 include:

- Does version control allow association of system components to the appropriate system version?
- Are procedures for system software change identification, approval, and documentation established?
- Are system software changes/modifications subjected to a system acceptance before being placed in operation?
- Does management have procedures for testing and/or approving system components (such as the operating system, other system, utility, applications) before promotion to production?
- Are test data "live" data or made-up data?

- Are test results documented?
- Are system software modifications thoroughly tested to make sure that modifications function properly?
- Does management have procedures for ensuring those contingency plans and other associated documentation are updated to reflect system changes?
- How are emergency fixes handled?
- Does management have procedures to ensure that emergency system software modifications are immediately subjected to a system acceptance?
- Does management have policies against illegal use of copyrighted software and shareware?
- Do the policies contain provisions for individual and management responsibilities and accountability, including penalties?
- Are periodic audits conducted of users' computers to ensure only legal licensed copies of software are installed?
- What products and procedures are used to protect against illegal use of software?
- Are software warranties managed to minimize the cost of upgrades and cost reimbursement or replacement for deficiencies?

APPENDIX VI

SERVICE CONTINUITY CONTROLS

Background and Perspective. As previously noted, service continuity controls ensure that when unexpected events occur, critical operations continue without undue interruption and critical and sensitive data are protected. Service continuity controls should address the entire range of potential disruptions from relatively minor interruptions, such as temporary power failures, to major disasters, such as fires or natural disasters that would require re-establishing operations at a remote location.

NIST further defines and describes service continuity controls as an "event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions." According to NIST, contingency planning involves more than planning for a move offsite after a disaster destroys a data center. The term also addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. NIST Special Publication 800-12 describes a six-step approach to the contingency planning/disaster recovery process.

In the past, contingency planning concentrated on the mainframe environment and on whether the data center was down. Today contingency planning must include the distributed environment and on whether local area networks, minicomputers, workstations, and personal computers are operating.

Applicable Publications. Publications that cover service continuity controls include:

GAO FISCAM, Volume 1, Chapter 3.6. The FISCAM states that service continuity consists of four critical elements—assess the criticality and sensitivity of computerized operations and identify supporting resources, take steps to prevent and minimize potential damage and interruption, develop and document a comprehensive contingency plan, and periodically test the contingency plan and adjust it as appropriate. The four critical elements are further divided into 11 sub critical elements.

NIST Special Publication 800-12. An Introduction to Computer Security: The NIST Handbook addresses and describes service continuity in Chapter 11 under "Preparing for Contingencies and Disasters." This publication describes six steps in the contingency planning process to include (1) identifying the mission or business critical functions, (2) identifying the resources that support the critical functions, (3) anticipating potential contingencies or disasters, (4) selecting contingency planning strategies, (5) implementing the contingency strategies, and (6) testing and revising the strategy. Chapter 14.4 also addresses this subject.

NIST Special Publication 800-18. This Guide for Developing Security Plans for Information Technology Systems (5.GSS.4, 5.MA.4, and Appendix 14C) provides further advice about contingency planning and offers a number of specific questions for examining and testing service continuity controls in both general systems and major applications

NIST Special Publication 800-16, Chapter 3.3.8.

NIST ITL Bulletin "Preparing for Contingencies and Disasters" (September 1995). This bulletin offers a general overview and discussion on contingencies and disasters and is keyed to Chapter 11 of NIST Special Publication 800-12.

Federal Information Processing Standards (FIPS) Publication 87, Guidelines For ADP Contingency Planning (March 1981) describes what should be considered when developing a contingency plan for an ADP facility. The document provides a suggested structure and format, which may be used as a starting point from which to design a plan to fit each specific operation.

FIPS Publication 191, Guideline For The Analysis Of Local Area Network Security (November 1994) can be used as a tool to help improve the security of a local area network (LAN). The publication describes a LAN security architecture that discusses threats and vulnerabilities to examine as well as security services and mechanisms to explore.

The CPA's Guide to Information Security, by John Graves and Kim Hill Torrence, (1997 edition) describes and addresses data backup procedures and disaster recovery planning in Chapter 3

Procedures for Testing Service Continuity Controls. To test the service continuity controls, NIST Special Publication 800-18 suggests that auditors address the following:

- Any agreements for backup processing (e.g. hotsite contract with a commercial service provider)?
- Do documented backup procedures include frequency (e. g. daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup)?
- Where are the stored backups located (off site or on-site) and generations of backups?
- How often are contingency, disaster, and emergency plans tested?

- Are formal written emergency operating procedures posted or located to facilitate their use in emergency situations?
- Are tested contingency/disaster recovery plans in place to permit continuity of mission-critical functions in the event of a catastrophic event?
- Are tested contingency/disaster recovery plans in place for all supporting IT systems and networks?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?
- What is the coverage of the backup procedures (e. g. what is being backed up)?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

The GAO FISCAM proposes the following audit procedures for service continuity controls.

- Review the list of critical operations and data.
- Review the documentation supporting critical operations and insure that they include computer hardware, computer software, computer supplies, systems documentation, telecommunications, office facilities and supplies, and human resources.
- Determine whether emergency processing priorities have been established and approved by appropriate program managers and review the supporting documentation.
- Review written policies and procedures for backing up files.
- Determine whether backup files are created and rotated off-site and are sent before prior versions are returned.
- Examine the backup storage site.
- Review the contingency plan and determine whether it reflects current conditions, has been approved by senior management, clearly assigns responsibilities for recovery, includes detailed instructions for restoring operations, identifies the alternate processing facility and backup storage facility, includes procedures to follow when the data or service center is unable to receive or transmit data, identifies critical data files, and includes computer and telecommunications hardware compatible with agencies needs.
- Review policies on testing of the contingency plan.
- Review the test results and ascertain whether the current plan has been tested under conditions that simulate a disaster.

Environmental Security. This area concerns electrical power, temperature and humidity, hazards, and natural disasters. Electrical power problems can include over-voltage or under-voltage conditions, blackouts, harmonic distortions (noise) on the lines, and power fluctuations. For most equipment, temperature and humidity must be within

normal ranges; otherwise, equipment failures will become increasingly apparent. Hazards may overlap with natural disasters and include dust, smoke, static electricity, floods, fires, explosions, vibrations, earthquakes, magnetic fields, food and drink, and insects.

Fault Tolerance. This is the ability of an information system to continue to operate (usually for a limited time and/or at a reduced level) when part of the system fails. A system provides several levels of fault tolerance such as a provision for recovery after failure of disk's boot partition, duplicate copies of vital system information, and automatic detection and replacement of bad disk sectors. Partially or fully fault tolerant systems depend on various levels of redundant hardware components, such as backup electrical power, duplex server processors, and redundant disk drives. Also, systems provide automatic management of fault tolerance through the following features.

Redundant disk arrays. These are based on the standard called RAID, a Redundant Array of Inexpensive Disks that can recover data on the fly.

Uninterruptable power supply (UPS). This feature provides short-term electrical power when the main supply fails so that the system can be shut down smoothly. In addition, systems can communicate with an UPS device to detect and warn of power failures and shutdown conditions.

Symmetrical multiprocessing. The system balances the workload among two or more simultaneous processors. The second and subsequent processors provide additional computing power under normal circumstances and full backup in case of a failure in any processor.

Whatever the level of fault tolerance, tape backup copies are essential to protect against catastrophic failures such as physical destruction (e.g., fire, floods, earthquakes, or tornadoes), or human error. Procedures for evaluating fault tolerance follow.

Control Activity	Control Technique	Audit Procedure
Fault Tolerance	Level of tolerance is appropriate for the organization.	Ascertain whether the administrator determines server tolerance by reviewing the graphical map of the server's disk storage, with mirror sets and stripe sets identified by contrasting colors
	Use of redundant data feature	Determine if the administrator utilizes the redundant data feature.
	Uninterruptable power supply (UPS) service	1. Determine if uninterruptable power supply (UPS) service was installed on the current server or servers. 2. Discuss with the administrator the organization's plan for avoiding system failures due to power fluctuations. .

	Restricted access to boot disks.	1. Determine if the system administrators and senior management restrict access to boot disks. 2. Determine if the administrator owns a "last line of defense" boot disk to be used in case of the failure of a server's disk boot track.
	Duplication of boot disks and storage of boot disk copy offsite.	1.Determine whether the system administrator has created and maintained two system boot disks for each server and that all boot disks are protected like backup tapes. 2. Determine whether these boot disks are stored off site
	Regular fault tolerance testing	Determine the duration and frequency of fault tolerance testing.

Capacity Planning. Capacity planning is the process of monitoring the network to ensure the system has adequate resources, typically disk space, main memory (RAM), and processor power to meet current and future service needs. A rule of thumb is that active resources should normally have at least 20% spare capacity; in other words, maximum utilization should not exceed 80%. If the system's resources are not adequate, the organization risks system failure or loss of data. For example, data loss can occur if the server runs out of disk space and cannot complete process updates. Also, very high utilization of critical resources (over 90%) may indicate that the system is spending excessive processor time on internal tasks such as searching for free disk space. This results in slow response time at the personal computers, leading to user frustration and inefficiency. Systems provide an analytical tool for administrators to monitor system capacity and predict potential bottlenecks before they occur. Proper capacity planning also allows the organization to budget for system upgrades and to predict the likely effects of new systems and workloads. The following matrix provides steps to evaluate capacity planning.

Control Activity	Control Technique	Audit Procedure
Capacity Planning	Existence of organizational procedures for capacity planning and results reported to management	1. Determine if the organization has procedures for capacity planning. 2. Determine if management is regularly informed of the results of capacity planning. 3. Determine whether results of capacity planning are being used to prepare hardware purchases and equipment upgrades.
Capacity Planning	System Performance Monitored Regularly	Determine if the performance of the system is monitored regularly.

Control Activity	Control Technique	Audit Procedure
	Use of Peer Entity Authentication or Data Origin Authentication	Ascertain whether the network uses Peer Entity Authentication or Data Origin Authentication to ensure that a data exchange is established with the addressed entity (and not with an entity masquerading or replaying a previous exchange).
	Equipment Failure or Actions by Persons or Processes not authorized to alter data.	To counter equipment failure, or actions by persons or processes not authorized to alter data, determine if the network ensures that information is accurately transmitted from source to destination.
	Automated Testing, Detecting, and Error Reporting	1. Determine whether the network has an automated monitoring tool to monitor for capacity. 2. Ascertain whether the automated network monitoring includes the ability to test, detect, and report errors exceeding a threshold to counter jamming, spoofing, line or node outages, hardware or software failures, or active wiretapping.
	Positive Techniques or Audit Trail of Proof of Shipment/Receipt of Data	To prevent senders from disavowing legitimate messages, or recipients from denying receipt, ascertain if the e-network has a positive technique or audit trail to provide proof of shipment and/or receipt of data?
	Active or passive network replacement, or other forms of redundancy	1. Interview the manager. 2. Determine if the network uses active or passive replacement, or other forms of redundancy. 3. If so, describe the redundancies.
	Contingency Planning.	Develop continuity of operations plans or emergency action plans to enhance system survivability. These plans must be consistent and integrated with disaster recovery plans maintained by the organization. Test contingency plans periodically to ensure currency.

APPENDIX VII

INFORMATION SYSTEM SECURITY DIRECTIVE GUIDANCE

Public Laws

The Federal Managers' Financial Integrity Act (P.L. 97-255). The Federal Managers' Financial Integrity Act (also referred to as FMFIA) establishes specific requirements with regard to agency management controls. Under FMFIA, each agency head establishes controls that reasonably ensure (1) obligations and costs comply with applicable law; (2) assets are safeguarded against waste, loss, unauthorized use or misappropriation; and (3) revenues and expenditures are properly recorded and accounted for to enable Federal agencies to prepare reliable financial and statistical reports and maintain asset accountability. Also, each agency head annually evaluates and reports on the control and financial systems that protect the integrity of Federal programs. FMFIA text is at http://www.disa.mil/comptrol/DC4/mgtcontr/FMFIA.html.

Privacy Act of 1974 (P.L 93-579). The Privacy Act of 1974 defines the privacy of an individual as directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies. The Act states that increasing use of computers and sophisticated information technology has greatly magnified the harm to individual privacy and, therefore, requires Federal agencies to safeguard personal data. Verification of compliance to this Act is part of the audit function. Further, the Privacy Act provides ways for citizens to find out what information is being retained on them and allows for correction of inaccurate information. Finally, the Privacy Act does not give individuals control over information, but only constrains what recordkeepers can do. Refer to http://www.ljextra.com/cgi-bin/f_cat?/ljextra/data/practice/texts/941119.001 for full text of the Privacy Act.

Computer Security Act of 1987 (P. L. 100-235). The Computer Security Act of 1987 expands the definition of computer security, increases the awareness of computer security as an issue, and serves as a federal data policy. The Computer Security Act establishes standards and guidelines for improving security and privacy of sensitive information in the Federal government, provides for the establishment of Federal computer system security awareness training, provides for the establishment of security plans, provides for the establishment of standards for information privacy and security, and assigns to the National Bureau of Standards (within the Department of Commerce) certain roles and responsibilities for standards and guidelines in the computer security area. The text for the Computer Security Act can be accessed at the Computer Security Resource Clearinghouse web site, http://csrc.nist.gov/secplcy/csa87.txt.

Chief Financial Officers Act (P. L. 101-576). The Chief Financial Officers (CFO) Act establishes a leadership structure, provides for long-range planning, requires audited financial statements, and strengthens accountability reporting. The act creates chief financial officer positions in 23 major agencies. The agency CFO is responsible for developing and maintaining integrated accounting and financial management systems; directing, managing, and providing policy guidance and oversight of all agency financial management personnel, activities, and operations; approving and managing financial management systems design and enhancement projects; implementing agency asset management systems, including systems for cash management, credit management, debt collection, and property and inventory management and control; and monitoring the financial execution of the agency budget in relation to actual expenditures. The act further requires the OMB to prepare and submit to the Congress a government-wide financial management plan that includes planned OMB and agency activities for the next 5 years. Also, the act requires the preparation and audit of financial statements for 23 Federal agencies and requires auditors to report on internal controls and compliance with laws and regulations. Access text for the Chief Financial Officer Act at the Capitol Hill web site, http://thomas.loc.gov/cgi-bin/query/z?c101:H.R.5687.ENR:

Clinger-Cohen Act (P. L. 103-356). Under the Clinger -Cohen Act, the head of each executive agency establishes goals for improving the efficiency and effectiveness of agency operations and the delivery of services through the effective use of information technology, prepares an annual report to Congress on achieving these goals, and ensures that performance measures for information technology are developed and used to measure results. In addition, the Chief Information Officer (CIO) of each executive agency advises and assists on information technology purchases and information resource management; promotes improvements in agency work processes; develops, implements and maintains sound and integrated IT architecture; and promotes effective design and operation of all major IT resource management processes. Further, each agency head will submit to OMB and to the Congress a strategic plan and a performance plan. Under the Act, the Secretary of Commerce, through the National Bureau of Standards, establishes standards and guidelines covering the security and privacy of Federal computer systems. Access text for this act at http://cio.gov/s1124_en.htm

Federal Financial Management Improvement Act of 1996 (FFMIA). This was enacted into law to provide for consistency of accounting by an agency from one fiscal year to the next; provide uniform accounting standards throughout the Federal Government; require Federal financial management systems to support full disclosure of Federal financial data so that programs and activities can be considered based on their full costs and merits; increase the accountability and credibility of federal financial management; improve performance, productivity and efficiency of Federal Government financial management; establish financial management systems to support controlling the cost of Federal Government; build upon and complement the Chief Financial Officers Act of 1990 (Public Law 101-576; 104 Stat 2838), Government Performance and Results

Act of 1993 (Public Law 103-62 107 Stat. 285), and Government Management Reform Act of 1994 (Public Law 103-356; 108 Stat. 3410); and to increase the capability of agencies to monitor execution of the budget by more readily permitting reports that compare spending of resources to results of activities. Access this document from the OMB web site, http://www.financenet.gov/financenet/fed/legis/ffmia96.htm.

Paperwork Reduction Act of 1995. The Paperwork Reduction Act of 1995 amendments require that the creation, collection, maintenance, use, dissemination, and disposition of information by the Federal Government is consistent with applicable laws including privacy and confidentiality, security of information, and access to information. Also, each agency shall improve the integrity, quality, and utility of information to all users within and outside the agency, including protections for privacy and security. Further, each agency will implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for each agency. Last, each agency will develop and maintain a strategic information resource management plan. The text for the Paperwork Reduction Act and amendments can be assessed and downloaded electronically from the congressional web site. Access the full text of this act at http://thomas.loc.gov/cgi-bin/query/C?c104:./temp/~c104o4G40q.

OMB Circulars

OMB Circular No. A-123. Revised on June 21, 1995, OMB Circular No. A-123, "Internal Control Systems", provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls. This OMB circular links to the Federal Managers' Financial Integrity Act discussed below. Access the circular from the Federal Register Online via GPO Access (wais. Access.gpo.gov) or from the Department of Commerce's FedWorld Network under the OMB Library of Files at http://www.fedworld.gov/ftp.htm#omb.

OMB Circular No. A-127. Revised on July 23, 1993, OMB Circular No. A-127, "Financial Management Systems," describes government-wide requirements for financial systems. The circular prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The circular defines information and financial system. Access this document at the Department of Commerce's FedWorld Network under the OMB Library of Files at http://www.fedworld.gov/ftp.htm#omb.

OMB Circular No. A-130. OMB Circular No. A-130, "Management of Federal Information Resources," describes government-wide requirements for information resource management and incorporates requirements of the Computer Security Act of 1987. Appendix III, "Security of Federal Automated Information Resources," specifically describes and establishes a minimum set of controls to be included in Federal automated information security programs for general support systems and for major applications. The circular also assigns specific responsibilities for security of automated information to the Department of Commerce, Department of Defense, Department of Justice, General Services Administration, and Office of Personnel Management. This OMB circular also links individual agency and departmental automated information security programs to agency management control systems established by OMB Circular No. A-123. The circular drives responsibilities down to the users and managers of computer systems and information. Access this OMB circular at the OMB web site, http://www.whitehouse.gov/WH/EOP/OMB/html/circulars/a130/a130.html.

NIST Special Publications and the GAO FISCAM

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook. This 200-page handbook provides a broad overview of computer security to help readers understand computer security requirements and develop a sound approach to select appropriate security controls. The handbook also provides a broad overview of computer security and is an excellent primer for anyone interested in computer security. The document explains important concepts, cost considerations, and interrelationships of security controls. The purpose of this handbook is not to specify requirements but, rather, to discuss the benefits of various computer security controls and situations in which their application may be appropriate. The handbook provides the "why to" and served as the template for deriving the practices in NIST Special Publication 800-14. Access the text for this NIST Special Publication at the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/nistpubs/800-12.

NIST Special Publication 800-13, Telecommunications Security Guidelines for Telecommunications Management Network. This 44-page NIST document focuses on the Telecommunications Management Network and the security features needed to protect the operations, administration, maintenance, and provisioning of these components. The guidelines address security threats and concerns, sources of threats, threat categories, and requirements framework. In addition, the document covers identification, authentication, system access control, resource access control, data and system integrity, audit, security administration, and data confidentiality. Finally, the document covers development life cycle requirements during the various phases of the life cycle. Access the text for this NIST Special Publication at the Computer Security Resource Clearinghouse web site, **http://csrc.nist.gov/nistpubs**/800-13.

NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems. This 56-page NIST document provides a baseline that organizations can use to establish and review their information technology (IT) security programs. It presents a foundation of generally accepted system security principles, gives common practices used in securing IT systems, and provides the "what to do" in securing IT resources. The principle section contains intrinsic expectations whether the system is small, large, or owned by a government agency or by a private corporation. The practice section shows what should be done to enhance or measure an existing information system security program or to aid in the development of a new program. The guideline assists internal auditors and security professionals to gain an understanding of basic security requirements. Access the text for this publication at the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/nistpubs/800-14.

NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance Based Model. This 170-page NIST

document implements OMB Circular A-130, as revised in 1996, and presents a new conceptual framework for providing IT security training. This document emphasizes training criteria or standards rather than fixed content of specific courses and audiences. This framework includes the IT security training requirements appropriate for today's distributed computing environment and provides flexibility for extension to accommodate future technologies and the related risk management decisions. Also, this document focuses on roles and responsibilities specific to individuals (not job titles); delineates the differences among awareness, training, and education; provides an integrated planning tool to identify training needs throughout the workforce; provides a course development tool; and provides a structure for evaluating learning effectiveness. The emphasis on roles and results gives the training requirements flexibility, adaptability, and longevity. Access the text for this NIST Special Publication at the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/nistpubs/800-16

NIST Special Publication 800-18, Guideline for Developing Security Plans for Information Technology Systems. This NIST handbook addresses the development of security plans that document the management, technical, and operational controls for federal automated information systems. The guide explains important concepts, cost considerations, and interrelationships of security controls. It provides a broad overview of information system security and provides the "why" to many security-related issues. The handbook serves as the template for deriving the practices recommended in the NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems. Access this NIST Special Publication at the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/nistpubs/800-18.

NIST Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach. This 175-page NIST handbook addresses the six-phase system development life cycle (SDLC) phases—initiation, definition, system design, programming and training, evaluation and acceptance, and installation and operation. The handbook describes a process for an automated information system to ensure that controls and security are designed and built into the system. The guide is designed to provide audit/review programs for each of the six major phases of the SDLC. This document is not available electronically from the Computer Security Resource clearinghouse web server; instead, the document must be special ordered (ordering number PB88-217450) at $55 per copy.

NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability. This 39-page NIST handbook covers the steps and issues involved in setting up a Computer Security Incident Reporting Capability (CSIRC) to respond to computer security threats. A CSIRC is a proactive approach to computer security, one that combines reactive capabilities with active steps to prevent future incidents. Issues include structure, management support, funding, and staffing of the organization; alert and hotline mechanisms; activity and incident logs; agency

notification, confidentiality procedures, law enforcement and investigative agency coordination, evidence gathering, and press relations. Access this document at the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/nistpubs/800-3.

NIST Special Publication 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials. This 60-page NIST handbook provides guidance for federal procurement initiators, contracting officers, and information system security officials on how to include information system security requirements in federal information processing procurements. The document covers general information system security, control of hardware and software, control of information/data, security documentation, information system security training and awareness, personal security, physical security, and information system security features in systems. Access this document at the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/nistpubs/800-4.

FIPS Pub 73, Guidelines for Security of Computer Applications. The 55-page FIPS publication describes the technical and managerial decisions necessary to assure that adequate controls are included in new and existing computer applications to protect them from natural and human-made hazards and to assure that critical functions are performed correctly and with no harmful side effects. Fundamental security controls such as data validation, user identification verification, authorization, journalizing, variance detection, and encryption are discussed as well as security-related decisions that should be made at each stage in the life cycle of a computer application. This document is available electronically from the Computer Security Resource clearinghouse web server, http://csrc.nist.gov/nistpubs/fips/fips73.pdf. You may also special order this document in hardcopy from the National Technical Information Service (NTIS) in Springfield, Virginia. Ordering Number is FIPSPUB 73. Cost is presently $27 per copy.

GAO Federal Information System Controls Audit Manual (FISCAM), Volume I. This GAO audit manual describes the computer-related controls that auditors should consider when assessing the integrity, confidentiality, and availability of computer data. GAO applies this guide primarily in financial statement audits, and the guide is available for use by other government auditors. The manual lists specific control techniques and related suggested audit procedures. However, the audit procedures provided are stated at a high level and assume some expertise about the subject to be effectively performed. More detailed audit steps should be developed by the IS auditor based on the specific software and control techniques employed by the auditee after consulting with the financial auditor about audit objectives and significant accounts. The GAO Distribution Center in Washington DC provides one free copy, and additional copies are $2 each.

Additional Legislation, Executive Orders, Presidential Decision Directive, OMB Memoranda and Federal CIO Council Study

National Information Infrastructure Protection Act of 1996. In 1996, the National Information Infrastructure Protection Act was signed into law amending the Computer Fraud and Abuse Act. The law made it a crime to obtain information from any department or agency of the United States, obtain information from any protected computer, intentionally access a protected computer without authorization and cause damage, or to transmit program information, code or command and intentionally cause damage.

Executive Order 13011 of July 16, 1996, "Federal Information Technology. This executive order directs executive agencies to (1) improve management of their information systems, (2) refocus information technology management to directly support their strategic missions, (3) implement an investment review process, and (4) create agency Chief Information Officers to (among other things) monitor and evaluate performance of their information systems. Further, the head of each executive agency shall establish agency-wide management structures and processes for managing, selecting, controlling and evaluating investments in information systems and shall ensure that information security policies, procedures and practices of the agency are adequate. This executive order can be accessed and downloaded from the GSA IT policy web site at http://www.itpolicy.gsa.gov/mks/reg-rleg/exo13011.htm.

Executive Order 13010 of July 15, 1996, "Critical Infrastructure Protection". This executive Order notes that the national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. The order defines "critical infrastructures" to include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. The order provides for the creation of a Presidential Commission on Critical Infrastructure Protection. The mission of the Commission shall include (1) assessing the scope and nature of the vulnerabilities of, and threats to, critical infrastructures; (2) determining what legal and policy issues are raised by efforts to protect critical infrastructures and assess how these issues should be addressed; (3) recommending a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation; (4) proposing any statutory or regulatory changes; and (5) producing reports and recommendations. Access this executive order from the White House web site at http://www.pub.whitehouse.gov/white-house-publications/1996/07/. Scroll down to item # 75 and click.

White Paper/Presidential Decision Directive (PDD) 63 of May 22, 1998. This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. According to the White Paper, no later than the year 2000, the United States shall have achieved an initial operating capability and no later than 5 years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of: the Federal Government to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services; the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. Further, PDD 63 provides for the preparation of sectoral National Infrastructure Assurance Plans by Government departments and corporations. Each sectoral National Infrastructure Assurance Plan will assess the vulnerabilities of the sector to cyber or physical attacks; recommend a plan to eliminate significant vulnerabilities; propose a system for identifying and preventing attempted major attacks; develop a plan for alerting, containing and rebuffing an attack in progress; and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack. Access this white paper and presidential decision directive at item # 241 on the White House web site, http://www.pub.whitehouse.gov/white-house-publications/1998/05/.

Executive Order 13130 of July 14, 1999 "National Infrastructure Assurance Council". This executive order establishes a 30-member National Infrastructure Assurance Council (NIAC). The members of the NIAC shall be selected from the private sector, including private sector entities representing the critical infrastructures identified in Executive Order 13010, and from State and local government. The members of the NIAC shall have expertise relevant to the functions of the NIAC and shall not be full-time officials or employees of the executive branch of the Federal Government. The NIAC will meet periodically to: (1) enhance the partnership of the public and private sectors in protecting our critical infrastructure and provide reports on this issue to the President as appropriate; (2) propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems; and (3) monitor the development of Private Sector Information Sharing and Analysis Centers (PSISACs) and provide recommendations to the National Coordinator and the National Economic Council on how these organizations can best foster improved cooperation among the PSISACs, the National Infrastructure Protection Center (NIPC), and other Federal Government entities. Access this executive order from the CIO web site at http://www.cio.gov/exo13130.htm/.

OMB MEMORANDUM M-99-20, June 23, 1999. OMB recently issued a new memorandum on computer security. According to OMB, a number of agencies have recently experienced the intentional disruption of their Internet website operations,

ranging from minor nuisance to significant service interruption. Memorandum M-99-20 reminds agencies that, consistent with the principles embodied in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," they must continually assess the risk to their computer systems and maintain adequate security commensurate with that risk. Accordingly, agencies will conduct a review of their security practices to ensure they have in place a process that permits program officials and security managers to understand the risk to agency systems and act to mitigate it. This process should include specific procedures to ensure the timely implementation of security patches for known vulnerabilities, especially for those systems accessible via the Internet. Installing such patches is a proven way of avoiding disruptions to systems. Within 90 days, each agency must report its process along with the name of the official responsible for its implementation. Access this OMB memorandum at the CIO web site, http://www.cio.gov/itl-3.html.

Additional Useful NIST Publications, FIPS Publications, and ITL Bulletins

NIST has also published some additional special publications, FIPS publications, and ITL bulletins that may prove useful to auditors. Many of the special publications and ITL bulletins are available electronically from the Computer Security Resource Clearinghouse (CSRC) web server site. Most FIPS pubs are unavailable electronically and must be special ordered from the NTIS at 5285 Port Royal Road, Springfield, Va 22161 or on-line from the NTIS web site at http://www.fedworld.gov/onnow/.

Internet Security Policy: A Technical Guide (NIST SP 800-XXX) is presently in draft only. This document is intended to help an organization create a coherent Internet-specific information system security policy. It provides a brief overview of the Internet and its constituent protocols. It discusses the primary uses of the Internet, and the associated policy implications. It also provides sample policy statements for low, medium, and high risk/protection environments. An electronic copy of this draft is available from the CSRC web site, http://csrc.nist.gov/isptg.

The 27-page NIST **Guide to the Selection of Anti-Virus Tools and Techniques** (NIST SP 800-5) provides criteria for judging the functionality, practicality, and convenience of anti-virus tools. It furnishes information to use in determining which tools are best suited to target environments, but it does not weigh the merits of special tools. This NIST special publication covers detection, identification and removal tools, general purpose monitors, access control shells, checksums for change detection, knowledge-based virus removal tools, selecting anti-virus techniques, and selecting the right tool. This document is available electronically from the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/nistpubs/800-5.

The 23-page **Automated Tools for Testing Computer Systems Vulnerability** (NIST SP 800-6) discusses automated tools for testing computer system vulnerability. This special publication examines basic requirements for vulnerability testing tools and describes the different functional classes of tools. This document covers vulnerability testing objectives, testing methods, and policy and procedures. Finally, this document offers general recommendations about the selection and distribution of these tools. Obtain this document electronically from the Computer Security Resource Clearinghouse web site, http://csrc.nist.gov/nistpubs/800-6.

Security in Open Systems (NIST SP 800-7) provides information for service designers and programmers involved in the development of telecommunications application software; it focuses on building security into software based on open system platforms. The document is useful in understanding the capabilities and limitations of open systems. The URL for this site and publication is http://csrc.nist.gov/nistpubs/800-7.

The document is downloadable from the site in PostScript (Ps) and HTML formats. The postscript format is 1447678 bytes.

Good Security Practices for Electronic Commerce, including Electronic Data Interchange (NIST SP 800-9) covers security procedures and techniques, including internal controls and checks, that constitute good practice in the design, development, testing, and operation of electronic commerce systems. Security techniques considered include audit trails, contingency planning, use of acknowledgements, electronic document management, activities of support networks, user access controls to systems and networks, and cryptographic techniques for authentication and confidentiality. This document is not available electronically from the Computer Security Resource Clearinghouse web server, but must be special ordered from NTIS at 5285 Port Royal Road, Springfield, Va 22161. Phone call orders may be placed at (703) 605-6000 and fax orders at (703) 321-8547. Ordering Number is PB94-139045. Cost is presently $21.50 per copy.

Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls (NIST SP-800-10) provides an overview of the Internet and security-related problems. It describes firewall components, the reasoning behind firewall usage, several types of network access policies, and resources for more information. This document is available electronically from the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/nistpubs/800-10.

Security of Personal Computer Systems – A Management Guide. (NISP SP 500-120) describes management and technical security considerations associated with the use of personal computer systems. The issues discussed in this document include physical and environmental protection, system and data access control, integrity of software and data, backup and contingency planning, auditability, and communications protection. In addition a general plan of action for the management of personal computer information security is discussed. This document is not available electronically from the Computer Security Resource Clearinghouse web server, but must be special ordered from the NTIS in Springfield, Virginia. Ordering Number is PB85-161040. Cost is presently $27.00 per copy.

The 21-page NIST **Guide for Selecting Automated Risk Analysis Tools** (NIST SP 500-174) recommends a process for selecting automated risk analysis tools, describing important considerations for developing selection criteria for acquiring risk analysis software. The guide covers the certification and accreditation process, contingency planning, how to use risk analysis, and selecting automated risk analysis tools. This document is not available electronically from the Computer Security Resource Clearinghouse web server, but must be special ordered from the NTIS in Springfield, Virginia. Ordering Number is PB90-148784. Cost is presently $24.50 per copy.

The 34-page **Analyzing Electronic Commerce** (NIST SP 500-218) document defines and describes the basics of electronic commerce and electronic data interchange. In addition, the document describes the steps required to set up a typical EDI transaction; outlines 14 common transaction sets, and describes a variety of electronic commerce applications. Finally, the document discusses some security implications of electronic commerce and electronic data interchange. This document is not available electronically from the Computer Security Resource Clearinghouse web server, but must be special ordered from the NTIS in Springfield, Virginia.

Guidelines for Automatic Data Processing Physical Security and Risk Management (FIPS PUB 31), published in 1974, provides a handbook for use by Federal organizations in structuring physical security and risk management programs for their ADP facilities. Written from a mainframe perspective, this publication discusses security analysis, natural disasters, supporting utilities, system reliability, physical protection of ADP facilities, internal controls, security of off-site facilities, contingency plans, security awareness and training, and internal audit of physical security. This document is not available electronically from the Computer Security Resource clearinghouse web server, but must be special ordered from the NTIS in Springfield, Virginia. Ordering Number is FIPSPUB 31. Cost is presently $27 per copy.

Computer Security Guidelines for Implementing the Privacy Act of 1974, (FIPS PUB 41), provides guidance in the selection of technical and related procedural methods for protecting personal data in automated information systems. The document discusses categories of risks and the related safeguards for physical security, information system management practices, and system controls to improve system security. This document is not available electronically from the Computer Security Resource clearinghouse web server, but must be special ordered from the NTIS in Springfield, Virginia. Ordering Number is FIPSPUB 31. Cost is presently $12.50 per copy.

Data Encryption Standard (FIPS Pub 46-2) reaffirms the Data Encryption Algorithm (DEA) until 1998 and allows for implementation of the DEA in software, firmware or hardware. The DEA is a mathematical algorithm for encrypting and decrypting binary-coded information. This document is available electronically from the Computer Security Resource clearinghouse web serve. The URL for this site and publication is http://csrc.nist.gov/fips/fips46-2.txt. This document is also available in hardcopy by special order from the NTIS in Springfield, Virginia. Ordering Number is FIPSPUB 46-2. Cost is presently $22.50 per copy.

The 37-page **Guidelines for ADP Contingency Planning** (FIPS Pub 87) describe what should be considered when developing a contingency plan for an ADP facility. The document provides a suggested structure and format, which may be used as a starting point from which to design a plan to fit each specific operation. The document describes the preliminary planning, preparatory actions, and action plan components of a

contingency plan and also describes the importance of testing in contingency planning. This document is available electronically from the Computer Security Resource clearinghouse web server, http://csrc.nist.gov/fips/fips87.pdf. This document is also available as hardcopy. Ordering Number is FIPSPUB 87. Cost is presently $24.50 per copy.

The 96-page **Guideline for Computer Security Certification and Accreditation** (FIPS Pub 102) describes how to establish and carry out a certification and accreditation program for information system security. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the official management authorization for the operation of the system and is based on the certification process. The document describes the steps in the certification/accreditation process, from planning, data collection, basic evaluation, detailed evaluation, and report of findings to accreditation. This document is available electronically from the Computer Security Resource clearinghouse web server, http://csrc.nist.gov/fips/f102a.pdf. This document is also available in hardcopy from the NTIS in Springfield, Virginia. Ordering Number is FIPSPUB 102, and cost is presently $36.50 per copy.

The **Standard on Password Usage** (FIPS Pub 112) defines ten factors to consider in the design, implementation, and use of access control systems that are based on passwords. It specifies minimum security criteria for such systems and provides guidance for selecting additional security criteria for password systems, which must meet higher security requirements. This document is available electronically from the Computer Security Resource clearinghouse web server, http://csrc.nist.gov/nistpubs/fips/f112-1.ps and http://csrc.nist.gov/fips/f112-1.wp. This document is also available in hard copy from the NTIS in Springfield, Virginia. Ordering Number is FIPSPUB 112, and cost is presently $27 per copy.

The **Guideline for Analysis of Local Area Network Security** (FIPS Pub 191) describes how to improve the security of a local area network (LAN). A LAN security architecture is describes that discusses threats and vulnerabilities that should be examined, as well as security services and mechanisms that should be explored. This document is available electronically from the Computer Security Resource clearinghouse web site, http://csrc.nist.gov/fips/fips191.ps.

The **Guide for Developing Security Plans for Information Technology Systems** (ITL Bulletin -April 1999) summarizes the purpose, responsibilities, format and development of an effective security plan and recaps some of the important concepts outlined in NIST Special Publication 800-18, **Guide for Developing Security Plans for Information Technology Systems**. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

The **Management of Risks in Information Systems: Practices of Successful Organizations** (ITL Bulletin – March 1998) bulletin summarizes the GAO executive guide on **Information Security Management, Learning from Leading Organizations.** The bulletin identifies the five principles of risk management adapted by the organizations studied and the sixteen successful practices common to the organizations studied. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

The **Information Security and the World Wide Web (WWW)** (ITL Bulletin-February 1998) bulletin describes threats and vulnerabilities from using the World Wide Web. The bulletin notes that security policies provide the foundation for implementing security controls to reduce vulnerabilities and reduce risks. Finally, the bulletin describes some low, medium and high-risk situations and some model policy statements for mitigating these three risks. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

What is Year-2000 Compliance (ITL Bulletin – December 1998) describes the year 2000 problem and some currently used definitions of "year 2000 compliance." The bulletin cites definitions used by Institute of Electrical and Electronics Engineers, British Standards Institute, Hewlett Packard, Bethlehem Steel Corporation, and Government of British Columbia. Next, the bulletin identifies the core set of requirements common to all year-2000compliance definitions. Finally, the bulletin concludes by answering five year-2000 compliance questions. This bulletin is available electronically from the NIST web site, http:/www.nist.gov/itl/lab/bulletns/.

The **Internet Electronic Mail** (ITL Bulletin - November 1997) bulletin summarizes a chapter of the draft **Internet Security Policy: A Technical Guide**. The bulletin describes an appropriate organizational e-mail policy, the principle e-mail protocols; potential e-mail problems from accidents, personal use, marketing, e-mail threats dangerous attachments, impersonation, eavesdropping, junk and harassing e-mail; and low, medium, and high levels of e-mail protection. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

The **Security Considerations in Computer Support and Operations** (ITL Bulletin - April 1997) bulletin describes important security considerations and issues within user support, software support, configuration management, backups, media controls, documentation, and maintenance operations. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

Audit Trails (ITL Bulletin - March 1997) bulletin defines audit trails as a series of records of computer events, about an operating system, an application, or user activities. The bulletin also descibes the ways in which audit trails can be used. Finally, this ITL bulletin describes an event-oriented log and a keystroke log and the distinction between a

system level audit trail and an application level audit trail. This bulletin is available electronically from the NIST web site, http:/csrc.nist.gov/nistbul/.

The Security Issues for Telecommuting (ITL Bulletin - January 1997) bulletin defines telecommuting as the use of telecommunications to create an '"office" away from the established (physical) office. Telecommuting can be in an employees home, a hotel room or conference center, an employee's travel site, or a telecommuting center. This bulletin explores some of the potential security risks to an organization in telecommuting and identifies some security issues for protecting internal systems. The bulletin describes three methods--firewalls/secure gateways, robust authentication, port protection devices--for protecting internal systems. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

Generally Accepted System Security Principles (GSSPS): Guidance on Securing Information Technology (IT) Systems (ITL Bulletin - October 1996) bulletin presents a set of generally accepted system security principles (developed by NIST. This document provides an overview of **Generally Accepted Principles and Practices for Securing Information Technology Systems** (NIST Special Publication 800-14) and explains some of the needs, which GSSPs can solve. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

The World Wide Web: Managing Security Risks (CSL - May 1996) bulletin addresses general security issues related to the use of the World Wide Web, concentrating on risk management for Web readers and publishers. The bulletin notes that computer users are finding the Internet and the World Wide Web extremely useful for browsing through information, publishing documents, and exchanging information. Some of the more likely losses and their causes are damage to the system and user information from buggy software, virus-infected executables, Trojan horse programs, embedded macros, and downloadable applets (an applet is a small program that is downloaded and executed on-the-fly by the browser). Web threats stem from shortcuts in the software development process, shortcomings in popular operating systems, deficiencies in the Internet protocols, and the problems inherent in managing the Internet. The bulletin states that web browsers are especially hazardous because they can allow access to untrustworthy systems on the Internet and they often invoke other applications as a side effect of their use. Some may also act as an FTP (file transfer protocol) client, Usenet news (Internet-based discussion groups) client, or an e-mail client. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

Preparing for Contingency and Disasters (CSL- September 1995) bulletin summarizes a chapter on contingency planning from **An Introduction to Computer Security: The NIST Handbook** (NIST Special Publication 800-12). According to the bulletin, contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical

functions operating in the event of disruptions. The bulletin also describes six discrete steps in the contingency planning process as follows: identifying the mission- or business-critical function, identifying the resources that support the critical functions, anticipating potential contingencies or disasters, selecting contingency planning strategies, implementing contingency strategies, and testing and revising the strategy. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

The **Threats to Computer Systems: An Overview** (CSL – March 1994) bulletin provides an overview of today's common computer system threats. Some of the common threats identified by the bulletin include errors and omissions, programming and developing errors, fraud and theft, disgruntled employees, physical and infrastructure loss, malicious hackers, industrial espionage, malicious software, and threats to personal privacy. This bulletin is available electronically from the CSRC NIST web site, http:/csrc.nist.gov/nistbul/.

Security Program Management (CSL Bulletin – August 1993) discusses the establishment and operation of a security program and describes some of the features and issues common to most organizations. The bulletin describes an ideal structure off a security program. Next, it discusses the elements of a central security program and the characteristics of a viable system level security program. This bulletin is available electronically from the NIST web site, http:/csrc.nist.gov/nistbul/.

Proposed Federal Legislation

The United States Congress has several bills in process that, if passed, could impact information systems auditing. Most bills relate to privacy issues which could impact auditors as they audit information systems containing Privacy Act data. A brief summary of these bills follows.

S.187, Financial Information Privacy Act of 1999. This Senate bill would give customers notice and choice about how their financial institutions share or sell their personally identifiable sensitive financial information.

S.573, Medical Information Privacy and Security Act. This Senate bill would provide individuals with access to and the right to inspect and copy health information of which they are a subject, ensure personal privacy with respect to health-care-related information, impose Federal criminal penalties for knowingly and intentionally obtaining or disclosing protected health information, and allow any individual whose rights have been knowingly or negligently violated to bring a civil action to recover compensatory (or specified liquidated) damages, punitive damages (for knowing violations), and attorney's fees.

S.578, Health Care Personal Information Nondisclosure Act of 1999. This Senate bill would ensure confidentiality with respect to medical records and health care-related information.

S.759, Inbox Privacy Act of 1999. This Senate bill would regulate transmission of unsolicited commercial electronic mail on the Internet.

S.809, Online Privacy Protection Act of 1999. This Senate bill would require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about private individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet and to provide greater individual control over the collection and use of that information.

S.854, Electronic Rights for the 21st Century Act. This Senate bill would establish standards and procedures regarding law enforcement access to location information, prohibit U. S agencies from establishing standards regarding decryption keys or key recovery for encrypted communications and stored electronic information, require a Federal order before authorizing the interception of a wire or electronic communication and affirm the rights of Americans to use and sell encryption products as a tool for protecting their on-line privacy.

S.881, Medical Information Protection Act of 1999. This Senate bill would ensure confidentiality regarding medical records and health care-related information.

H.R.367, The Social Security On-line Privacy Protection Act of 1999. This House bill would prohibit interactive computer services from disclosing Social Security account numbers and related personally identifiable information.

H.R.369, Children's Privacy Protection and Parental Empowerment Act of 1999. This House bill would amend Title 18, United States Code, to prohibit the sale of personal information about children without their parents' consent

H.R.514, Wireless Privacy Enhancement Act of 1999. This House bill would amend the Communications Act of 1934 to strengthen and clarify prohibitions on electronic eavesdropping.

H.R.1057, Medical Information Privacy and Security Act. This House bill, similar to S.573, would provide individuals with access to health information of which they are a subject, ensure personal privacy with respect to health-care-related information, impose criminal and civil penalties for unauthorized use of protected health information, provide for the strong enforcement of these rights, and amend the Privacy Act of 1974 to require an agency that receives protected health information to promulgate rules to exempt a system of records within the agency from all but specified provisions of that Act.

H.R.1685, Internet Growth and Development Act of 1999. This House bill, sponsored by Congrssman Rick Boucher, would provide for the recognition of electronic signatures for the conduct of interstate and foreign commerce, restrict the transmission of certain electronic mail advertisements, authorize the Federal Trade Commission to prescribe rules to protect the privacy of users of commercial Internet websites, and promote the rapid deployment of broadband Internet services.

H.R.1929, Banking Privacy Act of 1999. This House bill would control financial institution disclosure of customers' personal financial information.

H.R. 2413, Computer Security Enhancement Act. This House bill amends the National Institute of Standards and Technology Act and the Computer Security Act. It enhances the ability of the National Institute of Science and Technology (NIST) to improve computer security and provides for a more proactive involvement by the NIST in computer security matters. Introduced into and passed by the House of Representatives in 1997, but not passed by the Senate, the Computer Security Enhancement Act was reintroduced in 1999 as HR 2413. The current bill requires NIST to provide technical assistance to Federal agencies and to develop uniform computer security standards and guidelines for cost effective security and privacy of sensitive information in Federal computer systems.

APPENDIX VIII

INFORMATION SYSTEM SECURITY TRAINING COURSE PROVIDERS

Introduction. Government training institutions, commercial training organizations, and professional audit, accounting, and information security organizations all provide training in the areas of information system security and information technology. This appendix provides a sampling of information systems security training course providers. Please note this appendix is not intended to be an all-inclusive or comprehensive document on information system security training and providers. We believe this appendix is a useful starting point for auditors interested in identifying training to improve their knowledge, skill, and ability in the field of information system security. The omission of some providers is unintentional, and the inclusion of certain training course providers should not be construed as an official endorsement of their training courses.

Perspective. In 1997, the GAO identified information technology (IT) as a "new high-risk area that touches virtually every major aspect of government operations" (GAO Report HR#97-30). In its report the GAO further identified people factors such as "insufficient awareness and understanding of information security risks among senior agency officials," "poorly designed and implemented security programs," "a shortage of personnel with the technical expertise needed to manage controls," and "limited oversight of agency practices." The key to addressing these people factors is awareness training and education.

Information system security specialists designed NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, to (1) provide guidance on awareness training and education, (2) satisfy the mandatory periodic training awareness requirement of the Computer Security Act of 1987 (PL 100-235), and (3) satisfy the requirement of OMB Circular A-130, as revised in 1996, to update the old NIST training standards spelled out in NIST Special Publication 500-172. According to NIST, Special Publication 800-16 was designed as a "living handbook" and included the following elements:

1. Terminology that is most consistent across Federal agencies and broadest in scope,
2. An extensive set of knowledges, skills, and abilities (known as KSAs) linked to knowledge, topics, and concepts categories, and
3. Emphasis on training criteria or standards, rather than on specific curricula or content, with training criteria established according to trainees' roles within their organizations.

The framework outlined in NIST Special Publication 800-16 includes the security training requirement appropriate for today's distributed computing environment and provides flexibility for extension to accommodate future technologies. The approach presented in NIST SP 800-16 is designed to facilitate results-based learning.

GOVERNMENT INFORMATION SYSTEM SECURITY TRAINING COURSE PROVIDERS

The United States Department of Agriculture Graduate School's Government Auditor Training Institute, Washington DC, offers three courses related to information system auditing. They are Introduction to Information Systems Auditing (TAUDT778), Assessing the Reliability of Computer-Processed Data (TAUDT728), and Auditing and Control of Computer Networks (TAUDT894). Additional information on these three courses, their frequency, and costs is provided at the USDA Grad School web site, http://grad.usda.gov/auditing/infosys.html.

The Inspectors General Auditor Training Institute (IGATI) at Ft. Belvoir VA offers four courses related to information systems auditing. They are Introductory Information Systems Auditing, Intermediate Information Systems Auditing, Advanced Information Systems Auditing, and Control Objectives for Information and related Technology (CobiT). Dates and times of current courses and course costs are provided at the IGATI web site, http://www.igati.org/99catalo.html.

The National Defense University's Information Resource Management College at Ft. McNair in Washington, D. C offers two information system security courses—Managing Information Security in a Networked Environment (SEC) and Managing Information Security – Advanced topics (SAT). Courses are free for Department of Defense employees and cost $500 for non-DOD Federal Employees. Managing Information Security in a Networked Environment (SEC) is also offered as a non-residence, distance education course for those unable to attend the resident course. Specific information on course schedule, enrollment procedures, and costs are available from the NDU/IRMC web site, http://www.ndu.edu/ndu/irmc/intensive-courses.html. Information on the distance education course is available from http://www.ndu.edu/ndu/irmc/distance.html.

The Federal Law Enforcement Training Center's Financial Fraud Institute at Glynco GA offers information system security courses from an investigator's perspective. The Institute offers 16 courses covering the field of financial fraud. Four courses—Computer Network Investigators Training Program, Fraud and Financial Investigations Training Program, Telecommunications Fraud Training Program, and White Collar Crime Training Program---may benefit auditors interested in information system security. Complete course offerings and a detailed description of each course are provided at their web site, http://www.ustreas.gov.fletc/ffi/training.html.

PROFESSIONAL AUDIT, ACCOUNTING, AND INFORMATION SECURITY ORGANIZATIONS THAT PROVIDE TRAINING.

Professional audit, accounting, and information system security associations are another source of information systems security training. The national office and local chapters of the Institute of Internal Auditors (IIA), Information Systems Audit and Control Association (ISACA), Association of Government Accountants (AGA), Information Systems Security Association (ISSA), and Computer Security Institute (CSI) provide professional development and education seminars on information systems and computer security.

For further information on the Institute of Internal Auditors (IIA), visit the IIA website at http://www.theiia.org/chapters/iiaregon.htm. Information on seminars is also available at http://www.theiia.org/seminars/seminars.htm. An IIA web site dedicated to Information Technology can be accessed at http://www.itaudit.org/. The IIA web site dedicated to Information Technology (IT) includes a Forum, IT articles, a reference section, technology products, and "departments" that cover audit and control, business continuity, business systems, emerging issues, internet, network management, risk management, software, technology, e-commerce, information management, security, standards, and year 2000 from the Information Technology perspective. The web site for the Washington, D. C Chapter of IIA is at http://www.dciia.org/.

For further information on the Information Systems Audit and Control Association (ISACA), their 160 chapters worldwide, or their professional development and education seminars, visit the ISACA web site at http://www.isaca.org. The web site for the National Capital Area Chapter of ISACA is at http://isaca-washdc.org.

For further information on the Association of Government Accountants, a chapter in your area, or professional development and education seminars, visits their web site at http://www.agacgfm.org/education.

The Information Systems Security Association (ISSA) and its local chapters sponsor information system security professional education and development courses. For further information on the ISSA, its local chapters, or its professional development seminars, visit its web site at http://www.uh.edu/~bmw/issa/chapter.html.

The Computer Security Institute (CSI) sponsors professional development courses to train the information, computer, and network security professional. CSI sponsors two conferences and exhibitions each year and information system security seminars in Atlanta, Chicago, Phoenix, San Antonio, Gaithersburg, Md., San Francisco, St. Louis, and Washington, D. C. Course offerings include Advanced UNIX and Internet Security, Advanced Windows NT Security, Annual Computer Security Conference and Windows NT Security, Comprehensive Intrusion Management, Effective Deployment of

Encryption and Certificate Authorities, Essential Network Security for IT Professionals, Firewalls and Internet Security, How to Become a More Effective Information Security Professional, How to Build Winning Security Architecture, How to Form an Incident Response Team, How to Conduct a Network Vulnerability Assessment, How to Develop and Sell Information Security Policies and Procedures, Introduction to Computer Security, Intrusion Techniques and Countermeasures, Multidimensional Security, Practical Application of Risk Analysis, Rapid Roll-out of an Information Security Awareness Program, and Windows NT Security. For additional information, consult the CSI web site at http://www.gocsi.com/..

COMMERCIAL INFORMATION SYSTEM SECURITY TRAINING COURSE PROVIDERS.

The MIS Training Institute offers a variety of information security courses throughout the country at sites in Atlanta, Boston, Chicago, Las Vegas, Minneapolis, New York, Orlando, San Francisco and Washington, D. C. Specific courses are offered in: Introduction to Computer Security, Introduction to Network Security, Introduction to Internet Security and Audit, Introduction to Audit and Security of Data Communications, Audit and Security of Windows NT Server, Audit and Security of UNIX-based Systems, Audit and Security of Oracle client server Databases, Audit and Security of PeopleSoft Applications, Windows NT and Internet Security, Auditing Your Web Site, and Network Firewall Security. Current course offerings, locations and costs may be found by accessing the MIS Training Institute web site at http://www.misti.com.

Learning Tree International offers information system security courses at training sites in Atlanta, Boston, Chicago, Los Angeles, New York, and Washington DC. Courses are offered in: Introduction to Internet and Intranet Security, UNIX System and Network Security, Internet and Intranet Firewalls, and Implementing Web Security. Current course offerings and costs may be found by accessing the Learning Tree International web site at http://www.learningtree.com.

APPENDIX IX

INFORMATION SYSTEM SECURITY-RELATED WEBSITES

The following websites are provided to assist auditors in identifying helpful sources for accomplishing information system security audits. These website addresses were updated July 1, 1999, but because website addresses periodically change, we do not guarantee the accuracy of this listing.

CRITERIA	WEB ADDRESSES
OMB Circular A-130, Revised	csrc.nist.gov/secplcy/a130.txt
Appendix III to OMB Circular A-130 – Security of Federal Automated Information Resources	csrc.nist.gov/secplcy/a130app3.txt
Executive Order 13010 Critical Infrastructures	www.fas.org/irp/offdocs/ep13010.htm
Computer Security Act of 1987	csrc.nist.gov/secplcy/csa_87.txt
Computer Security Training Policy	csrc.nist.gov/secplcy/opm_plcy.txt
Computer Security Enhancement Act of 1997 (H.R. 1903) (Pending Legislation)	thomas.loc.gov/cgi-bin/query/z?c105:H.R.1903
Electronic Communications Privacy Act of 1986	www.hr.doe.gov/ucsp/ecpa.htm
Computer Fraud and Abuse Act of 1986	www.hr.doe.gov/ucsp/cfa.htm
Privacy Act of 1974	www.hr.doe.gov/ucsp/pa.htm
Information Technology Management Reform Act	www.hr.doe.gov/ucsp/itmra.htm
Draft Version of Special Publication 800-XXX Internet Security Policy: A Technical Guide	csrc.nist.gov/isptg/html
U.S. Customs AIS Security Policy Manual CIS HB 1400-05	csrc.nist.gov/secplcy/ais_plcy.wp6
U.S. Customs Security Policy	www.customs.ustreas.gov/about/ais-doc.htm
Department of Commerce's Software Copyright Policy	csrc.nist.gov/secplcy/doc-copy.txt
Department of Commerce's Chapter 10 of the DOC "Information Technology Security Manual"	csrc.nist.gov/secplcy/doc-poli.txt
Green Book on Security Information Systems	nsi.org/Library/Compsec/greenbk.txt
DoD Computer Security Requirements	nsi.org/Library/Compsec/yellowbo.txt

(Yellow Book)	
DoD Password Management Guide (Green Book)	nsi.org/Library/Compsec/greenboo.txt
DoD Trusted Computer Systems Evaluation Criteria (Orange Book)	nsi.org/Library/Compsec/orangebo.txt
European Orange Book	nsi.org/Library/Compsec/eurooran.txt
Technical Rationale Behind the Yellow Book	nsi.org/Library/Compsec/yellowb2.txt
NII Security: The Federal Role	nsi.org/Library/Compsec/nii.txt
NII Advisory Council's Comments on "NII Security: The Federal Role"	nsi.org/Library/Compsec/niiacsec.txt
Multilevel Security in the Department of Defense: The Basics	nsi.org/Library/Compsec/secO.html
Computer Security Roles of NIST and NSA	nsi.org/Library/Compsec/nistnsa.txt
National Computer System Security and Privacy Board's 1994 Annual Report	nsi.org/Library/Compsec/94-rpt.txt
National Computer System Security and Privacy Board's Charter	nsi.org/Library/Compsec/csschart.txt
National Computer System Security and Privacy Board's FAQ	nsi.org/Library/Compsec/ncssfaq.txt
Federal Internet Security – A Framework for Action	www.fnc.gov/fisp_sec_contents.html
A Guide to Understanding Audit in Trusted Systems (Tan Book)	www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
Computer Security Subsystem Interpretation of the TCSEC (Venice Blue Book)	www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-009.html
A Guide to Understanding Security Testing and Test Documentation in Trusted Systems (Bright Orange Book)	www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-023.pdf
Technical Report, Computer Viruses: Prevention, Detection, and Treatment	www.radium.ncsc.mil/tpep/library/rainbow/C1-TR-001.html
The Design and Evaluation of INFOSEC Systems: The Computer Security Contribution to the Composition Discussion	www.radium.ncsc.mil/tpep/library/rainbow/C-TR-32-92.html
Auditing Issues In Secure Database Management Systems	www.radium.ncsc.mil/tpep/library/rainbow/ NCSC-TR-005-4.pdf
Guidelines For Computer Security Certification and Accreditation (FIPS Pub 102)	csrc.nist.gov/fips/f102a.pdf
Guidelines for the Analysis of Local Area Network Security (FIPS Pub 191)	csrc.nist.gov/fips/fips191.ps
Telecommunications & Computer Security (NSDD145)	www.fas.org/irp/offdocs/nsdd145.htm

National Policy for the Security of National Security Telecom and Info Systems (U) NSD 42	snyside.sunnyside.com/cpsr/privacy/computer-security/nsd-42.txt
National Security Information (PRD/NSC-29)	www.fas.org/irp/offdocs/prd29.htm
Protecting America's Critical Infrastructures	www.fas.org/irp/offdocs/pdd-63.htm
Critical Infrastructures (E.O. 13010)	www.fas.org/irp/offdocs/eo13010.htm
DoD Information Security Program (DoDD5200.1)	web7.whs.osd.mil/dodiss/directives/direct7.htm
Information Security Program (DoDD 5200.1-R)	web7.whs.osd.mil/dodiss/publications/pub2.htm
Security Requirements of Automated Information Systems (AISs) (DoD 5200.28)	web7.whs.osd.mil/pdf3/d5200(3-21-88)/d520028.pdf
DoD Information Technology Security Certification & Accreditation Process (DITSCAP) (DoDI 5200.40)	www.p-and-e.com/DITSCAP.pdf
Computer Viruses and Related Treats (SP 500-166)	csrc.nist.gov/nistpubs/sp500166.txt
Management Guide to the Protection of Information Resources (SP 500-170)	csrc.nist.gov/nistpubs/sp500-170.txt
Computer Users' Guide to Protection of Information Resources (SP 500-171)	csrc.nist.gov/nistpubs/sp500-171.txt
Guide for Selecting Automated Risk Analysis Tools (SP 500-174)	csrc.nist.gov/nistpubs/sp174.txt
Computer Security Considerations in Federal Procurements: A Guide for Procurements Initiators, Contracting Officers, and Computer Security Officials (SP 800-4)	csrc.nist.gov/nistpubs/sp800-4.txt
Automated Testing Tools for Testing Computer System Vulnerabilities (SP 800-6)	csrc.nist.gov/nistpubs/800-6.txt
Security in Open Systems (SP 800-7)	csrc.nist.gov/nistpubs/800-7/
An Introduction to Computer Security: The NIST Handbook (SP 800-12)	csrc.nist.gov/nistpubs/800-12/
Telecommunications Security Guidelines for Telecommunications Management Network (SP 800-13)	csrc.nist.gov/nistpubs/800-13.wpd
Generally Accepted Principles and Practices for Securing Information Technology Systems (SP 800-14)	csrc.nist.gov/nistpubs/800-14.pdf
Information Security and the World Wide Web	csrc.nist.gov/nistbul/itl198-02.txt
Security Considerations In Computer	csrc.nist.gov/nistbul/itl197-04.txt

Support and Operations	
Security Issues for Telecommuting	csrc.nist.gov/nistbul/itl197-01.txt
Generally Accepted System Security Principles (GSSPs): Guidance On Securing Information Technology (IT) Systems	csrc.nist.gov/nistbul/cs196-10.txt
Human/Computer Interface Security Issue	csrc.nist.gov/nistbul/cs196-02.txt
Digital Signature Standard	csrc.nist.gov/nistbul/cs194-11.txt
Threats to Computer Systems: An Overview	csrc.nist.gov/nistbul/cs194-03.txt
Computer Security Policy	csrc.nist.gov/nistbul/cs194-01.txt
Computer Security Roles of NIST and NSA	csrc.nist.gov/nistbul/cs191-03.txt
Computer Virus Attacks	csrc.nist.gov/nistbul/cs190-07.txt
Connecting to the Internet: Security Considerations	csrc.nist.gov/nistbul/cs193-07.txt
Security Issues in Public Access Systems	csrc.nist.gov/nistbul/cs193-05.txt
Audit Issues	csrc.nist.gov/nistbul/itl197-03.txt
The World Wide Web: Managing Security Risks	csrc.nist.gov/nistbul/cs196-05.txt
Minimum Security Requirements for Multi-User Operating Systems	csrc.nist.gov/nistir/ir5153.txt
Assessing Federal and Commercial Information Security Needs	csrc.nist.gov/nistir/ir4976.txt
Threat Assessment of Malicious Code and External Attacks	csrc.nist.gov/nistir/ir4939.txt
Information Vulnerability and World Wide Web	www.defenselink.mil/other_info/depsecweb.pdf
Security in Cyberspace (House Subcom. Rept)	www.fas.org/irp/congress/1996_hr/s960605t.htm
Glossary of Information Security –Related Terms	www.isse.gmu.edu:80/~csis/glossary/merged_glossary.html
A Guide to Understanding Data Remanence in Automated Information Systems (NCSC-TG-025)	www.infowar.com/iwftp/sec_text/ITAR.WP
Interpretations of DoD Trusted Computer System Evaluation Criteria (TCSEC) for Trusted Computer/Communications (NCSC-TG-005)	www.infowar.com/iwftp/sec_text/TG005.TXT
Information Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance	www.infowar.com/mil_c4i/joint/joint.html_ssi
Federal Criteria for Information Security (Vol. I)	www.infowar.com/iwftp/sec_text/FCVOL1.TXT
Federal Criteria for Information Security (Vol. II)	www.infowar.com/iwftp/sec_text/FCVOL2.TXT

Executive Guide to the Protection of Information Resources	csrc.nist.gov/nistpubs/sp500169.txt
Security Issues in Database Language SQL	csrc.nist.gov/nistpubs/800-8.txt
Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls	csrc.nist.gov/nistpubs/800-10/
Training for Information Technology Security: Evaluating the Effectiveness of Results-Based Learning	csrc.nist.gov/nistbul/itl98-06.txt
Training Requirements for Information Technology Security: An Introduction to Results-Based Learning	csrc.nist.gov/nistbul/itl98-04.txt
Management of Risks in Information Systems: Practices of Successful Organizations	csrc.nist.gov/nistbul/itl98-03.txt
Internet Electronic Mail	csrc.nist.gov/nistbul/itl97-11.txt
Cryptographic Standards and Supporting Infrastructures: A Status Report	csrc.nist.gov/nistbul/itl97-09.txt
Public Key Infrastructure Technology	csrc.nist.gov/nistbul/itl97-07.txt
Audit Trails	csrc.nist.gov/nistbul/itl97-03.txt
Advanced Encryption Standard	csrc.nist.gov/nistbul/itl97-02.txt
Federal Computer Incident Response Capability (FedCIRC)	csrc.nist.gov/nistbul/csl96-11.txt
Implementation Issues for Cryptography	csrc.nist.gov/nistbul/csl96-08.txt
Cryptology Standards and Infrastructures for the Twenty-first Century	csrc.nist.gov/nistbul/itl98-09.txt
Guidance on the Selection of Low Level Assurance Evaluated Products	csrc.nist.gov/nistbul/csl96-04.txt
An Introduction to Role-Based Access Control	csrc.nist.gov/nistbul/csl95-12.txt
A Framework for Cryptographic Standards	csrc.nist.gov/nistbul/csl95-08.txt
Acquiring and Using Asynchronous Transfer Mode in the Workplace	csrc.nist.gov/nistbul/csl95-03.txt
Data Encryption Standard (FIPS 46-2)	csrc.nist.gov/fips/fips46-2.txt
The Data Encryption Standard: An Update	csrc.nist.gov/nistbul/csl95-02.txt
Reducing the Risks of Internet Connection and Use	csrc.nist.gov/nistbul/csl94-05.txt
Security Program Management	csrc.nist.gov/nistbul/csl93-08.txt
Connecting to the Internet: Security Considerations	csrc.nist.gov/nistbul/csl93-07.txt
Security Issues in Public Access Systems	csrc.nist.gov/nistbul/csl93-05.txt
Sensitivity of Information	csrc.nist.gov/nistbul/csl92-11.txt
Disposition of Sensitive Automated Information	csrc.nist.gov/nistbul/csl92-10.txt
An Introduction to Secure Telephone Terminals	csrc.nist.gov/nistbul/csl92-03.txt

Security Requirements for Cryptographic Modules (FIPS 140-1)	csrc.nist.gov/fips/fips1401.htm
Secure Hash Standard (FIPS 180-1)	csrc.nist.gov/fips/fip180-1.txt
Automated Password Generator (FIPS 181)	csrc.nist.gov/fips/fips181.txt
Escrowed Encryption Standard (FIPS 185)	csrc.nist.gov/fips/fips185.txt
Digital Signature Standard (FIPS 186)	csrc.nist.gov/fips/fips186.txt
Digital Signature Standard (Change 1 Notice)(FIPS 186)	csrc.nist.gov/fips/chnge186.htm
Standard Security Labels (FIPS 188)	csrc.nist.gov/fips/fips188.txt
Guideline for the Use of Advanced Authentication Technology Alternatives (FIPS 190)	csrc.nist.gov/fips/fip190.txt
Guideline for The Analysis Local Area Network Security (FIPS 191)	csrc.nist.gov/fips/fips191.ps
Entity Authentication Using Public Key Cryptography (FIPS 196)	csrc.nist.gov/fips/fips196.wp6
Computer Data Authentication (FIPS 113)	csrc.nist.gov/fips/fips113.wp
Guidelines for Implementing and Using the NBS Data Encryption Standard (FIPS 74) Part 1	csrc.nist.gov/fips/fips74-1.txt
Guidelines for Implementing and Using the NBS Data Encryption Standard (FIPS 74) Part 2	csrc.nist.gov/fips/fips74-2.txt
Guidelines for Implementing and Using the NBS Data Encryption Standard (FIPS 74) Part 3	csrc.nist.gov/fips/fips74-3.txt
DES Modes of Operation (FIPS 81)	csrc.nist.gov/fips/fip81.txt csrc.nist.gov/change81.wp5
Guidelines for Computer Security Certification and Accreditation (FIPS 102)	csrc.nist.gov/fips/f102a.pdf csrc.nist.gov/fips/f102b.pdf csrc.nist.gov/fips/f102c.pdf csrc.nist.gov/fips/f102d.pdf csrc.nist.gov/fips/f102e.pdf csrc.nist.gov/fips/f102f.pdf csrc.nist.gov/fips/f102g.pdf
The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security	csrc.nist.gov/nistpubs/800-11/
Public-Key Cryptography	csrc.nist.gov/nistpubs/800-2.txt
Modes of Operation Validation System (MOVS) Requirements and Procedures	csrc.nist.gov/nistpubs/800-17.txt
Information Technology Security Training Requirements: A Role-and Performance-Based Model	csrc.nist.gov/nistpubs/800-16.pdf csrc.nist.gov/nistpubs/AppendixA-D.pdf csrc.nist.gov/nistpubs/Appendix_E.pdf
National Operations Security Program (NSDD 298)	www.fas.org/irp/offdocs/nsdd298.htm

Advanced Telecommunications and Encryption (PRD/NSC 27)	www.fas.org/irp/offdocs/prd27.htm
Public Encryption Management (PDD/NSC 5)	www.fas.org/irp/offdocs/pdd5.htm
Computer Security Assistance Program (AFI 33-207)	www.p-and-e.com/Documents/AFI%2033-207%20(1%20Sep%2097).pdf
The Computer Security (COMPUSEC) Program (AFSSI 5102)	www.p-and-e.com/Documents/AFI%205102%(23%20Sep%2096).pdf
Viruses and Other Forms of Malicious Logic (AFSSM 5023)	www.p-and-e.com/Documents/AFI%205023%20(1%20Aug%2096).doc
Network Security Policy (AFSSI 5027)	www.p-and-e.com/Documents/AFI%205027%20(27%20Feb%2098).doc
Unclassified Computer Security Program (Draft DOE Policy 200.xx)	www.hr.doe.gov/ucsp/ecpa.htm

APPENDIX X

INFORMATION SYSTEM SECURITY DIRECTIVE MATRIX

The Federal Government has established requirements and issued guidance relating to application and general controls for information systems. Tables 1 and 2 provide applicable references for Federal laws and OMB circulars, and Tables 3 and 4 provide applicable references for NIST publications, FIPS publications, and the GAO FISCAM.

Table 1 – Federal Laws

	FMFIA	Privacy Act	Computer Security Act	CFO Act	Clinger-Cohen Act
Application Controls					
1. Ensure transactions are authorized					
2. Ensure transactions are valid					
3. Ensure information is complete		Sec 552 a(e) (6)		Sec 902 (a) (3) (D) and sec 3512 (a) (3) (B) (iii)	
4. Ensure information is accurate/ reliable		Sec 552 a (e) (6)		Sec 902 (a) (3)(D)	
5. Ensure information is timely		Sec 552 a (e) (6)		Sec 902 (a) (3) (D) and sec 3512 (a) (3) (B) (iii)	
6. Ensure system and data are secure		Sec 552 a (e) (10)			
7. Ensure system is auditable and application security controls are reviewed					
General Controls					
1. Develop and document a system security plan			Sec 2 (b) (3) and sec 6 (b)		Sec 306 (a) to (e)
2. Ensure continuity of support (aka contingency plan/ disaster recovery plan) plan exists					
3. Test the continuity of support plan					
4. Ensure cost/benefit analysis exists					
5. Develop computer standards and guidelines for security and privacy			Sec 3 (b) (3) and sec 4 (d)		

	FMFIA	Privacy Act	Computer Security Act	CFO Act	Clinger-Cohen Act
General Controls					
6. Ensure adequacy of information security policies, procedures and practices of the agency					Sec 5123 (6)
7. Provide reasonable assurance	Sec 2				
8. Prepare annual report on internal controls (IC)	Sec 2 (3)			Sec 902 (a) (6) (D) and sec 3512 (a) (2) (D)	
9. Prepare statement of assurance	Sec 2 and Sec 4				
10. Send annual reports on IC and material weaknesses to OMB, if appropriate, and to President and/or Congress	Sec 2 (3) (A) and (B) (4)			Sec 902 (a) (6) (D) and sec 3512 (a) (2) (D)	
11. Perform risk assessment					
12. Perform reviews (including self-assessments reviews or audits) of security controls					
13. Perform initial certification and accreditation prior to implementation of the system and periodic reaccreditation of the system					
14. Develop 5-year information systems plan/Information Resource Management (IRM) strategic plan				Sec 3512 (a) (3) (A) and sec 3512 (a) (3) (B)	Sec 306 (a) to (e), Title 5 USC
15. Incorporate summary of security plan into IRM strategic plan					
16. Develop Computer Security Incident Response Capability					
17. Ensure that a mandatory computer security awareness training and education program exists to provide mandatory initial training for new users and periodic refresher training and education for current users.			Sec 2 (b) (4) and sec 5 (a)		

	FMFIA	Privacy Act	Computer Security Act	CFO Act	Clinger-Cohen Act
General Controls					
18. Assign organizational responsibility					
19. Assign individual responsibility					

Table 2 – Federal Laws and OMB Circulars

	FFMIA	Paperwork Reduction Act	OMB Circular A-123	OMB Circular A-127	OMB Circular A-130 and Appendix III
Application Controls					
1. Ensure transactions are authorized					
2. Ensure transactions are valid					
3. Ensure information is complete		Ch 35, sec 3506 (b) (1) (C)		Sec 6	Sec 8 b 2 (b)
4. Ensure information is accurate/ reliable		Ch 35, sec 3506 (b) (1) (C)		Sec 6	Sec 8 b 2 (b)
5. Ensure information is timely				Sec 6	
6. Ensure system and data are secure		Ch 35, sec 3506 (b) (1) (C)			Sec 8 b 2 (b)
7. Ensure system is auditable and application security controls are reviewed					Apdx III, Sec A. 3. b 3) Sec B. b. 3)
General Controls					
1. Develop and document a system security plan		Ch 35, sec 3506 (b) (1) (c)		Sec 7. h.	Apdx III, Sec A.3.a. 2) Sec A.3. b 2) and Sec B. A. 2)
2. Ensure continuity of support (aka contingency plan/ disaster recovery plan) plan exists					Apdx III, Sec A.3.b. 2) d) Sec B. a. 2) e) Sec B. b. 2) d)
3. Test the continuity of support plan					Apdx III, Sec A.3.a.2)

	FFMIA	Paperwork Reduction Act	OMB Circular A-123	OMB Circular A-127	OMB Circular A-130 and Appendix III
4. Ensure cost/benefit analysis exists				Sec 8. B	
5. Develop computer standards and guidelines for security and privacy		Ch 35, sec 3504 (g) (1) and sec 3506 (g) (1)			Sec 9. h.. 10
6. Ensure adequacy of information security policies, procedures and practices of the agency		Ch 35, sec 3504 (g) (1) and sec 3506 (g) (1)			
7. Provide reasonable assurance			Sec II. and sec III.		
8. Prepare annual report on internal controls (IC)	Sec 803 (a)		Sec V.	Sec 7 j. and Sec 9. a. 3.	Apdx 111, Sec A.5. and Sec B. 5.
9. Prepare statement of assurance	Sec 803 (a)		Sec V		
10. Send annual reports on IC and material weaknesses to OMB, if appropriate, and to President and/or Congress	Sec 803 (a)		Sec III para 5 and sec V.		Apdx III, Sec B. 5
11. Perform risk assessment		Ch 35, sec 3504 (g) (3) and sec 3506 (g) (3)			
12. Perform reviews (including self-assessments reviews or audits) of security controls			Sec III para 2	Sec 9. a. 3.	Apdx III, Sec A. 3. a. 3), Sec B. a. 3), and Sec B. b. 3)
13. Perform initial certification and accreditation prior to implementation of the system and periodic reaccreditation of the system					Apdx III, Sec A. 3.a. 4 Sec B. a. 4) and B. b. 4)

	FFMIA	Paperwork Reduction Act	OMB Circular A-123	OMB Circular A-127	OMB Circular A-130 and Appendix III
General Controls					
14. Develop 5-year information systems plan/Information Resource Management (IRM) strategic plan		Ch 35, sec 3506 (b) (2)		Sec 9. a 2.	Sec 8. b. 2. (a)
15. Incorporate summary of security plan into IRM strategic plan					Sec 8. b. 2. (c) (iv), Apdx III, Sec A. 3. a. 2) and Apdx III, Sec A. 5.
16. Develop Computer Security Incident Response Capability					Apdx III, Sec A. 2. 3. a. 2 .d and Sec B. a. 2) d)
17. Ensure that a mandatory computer security awareness training and education program exists to provide mandatory initial training for new users and periodic refresher training and education for current users.					Apdx III, Sec B. a. 2) b)
18. Assign organizational responsibility					Apdx III, Sec A. 3. b.. and Sec B. b. 1)
19. Assign individual responsibility					Sec 8. B. 3. (c) Apdx III, Sec A. 3. a. 1), Sec A. 3. b. 1) Sec A. 3. b. 2) a) Sec A. 3. b. 2) c) Sec B. a. 1)

Table 3 – NIST Publications

	NIST SP 800-12	**NIST SP 800-13**	**NIST SP 800-14**	**NIST SP 800-16**	**NIST SP 800-18**
Application Controls					
1. Ensure transactions are authorized					
2. Ensure transactions are valid					Ch 5.MA.6 and Apdx C, pg 6C
3. Ensure information is complete					Ch 5.MA.6
4. Ensure information is accurate/reliable					Ch 5.MA.6
5. Ensure information is timely					Ch 5.MA.6
6. Ensure system and data are secure					
7. Ensure system is auditable and application controls are reviewed					Ch 6.MA.4 and Apdx C, pg 8C to 9C
General Controls					
1. Develop and document a system security plan					Ch 1.6, 1.9, 3.1 to 3.7.
2. Ensure continuity of support (aka contingency plan/ disaster recovery plan) plan exists	Ch 11		Ch 3.6	Ch 3.3.8	Ch 5.GSS.4 and Apdx C, pg 14C
3. Test the continuity of support plan	Ch 11.6		Ch 3.6.5		
4. Ensure Cost/benefit analysis exists	Ch 8.6				
5. Determine adequacy of security requirements	Ch 8.4.2.2			Ch 4.2 Cell 3.2B to Cell 3.3E	
6. Develop computer standards and guidelines for automated information system security and privacy (and computer support and operations)	Ch 14.6			Ch 3.3.6	Ch 5.GSS.7 and Apdx C, pg 15C

	NIST SP 800-12	NIST SP 800-13	NIST SP 800-14	NIST SP 800-16	NIST SP 800-18
General Controls					
7. Ensure adequacy of information security policies, procedures and practices of the agency				Ch 3.3.6	Ch 5.GSS.7 and Apdx C, pg 15C
8. Provide reasonable assurance					
9. Ensure that a formal configuration management control process exists for managing system change and keeps track of changes/modifications to the system and that changes/modifications to the system program modifications are properly authorized.	Ch 14.2 and Ch 14.3		Ch 3.9		Ch 5.GSS.5 and Apdx C, pg 14C-15C
10. Ensure that physical and environmental security controls exist	Ch 15			Ch 3.3.8	Ch 5.GSS.2 and Apdx C, pg 13C
11. Ensure that identification and authentication controls exist	Ch 16	Ch 3.2, S1 and S2 and Ch 4.1 R1 to R6 and Ch 4.2 R7 to R17	Ch 3.11	Ch 3.3.9	Ch 6.GSS.1 and Apdx C, pg 16C
12. Ensure that logical access controls exist	Ch 17		Ch 3.12	Ch 3.3.9	Ch 6.GSS.2 and Apdx C, pg 16C
13. Perform risk assessment	Ch 7		Ch 3.3	Ch 3.2 and Ch 3.3.5	
14. Ensure that life cycle requirements incorporate security concerns and issues	Ch 8.4	Ch 5.0 R85 to R145	Ch 3.4	Ch 3.2, Ch 3.3.7 and Ch 4.2 Cell 3.1A to-Cell 3.6E	
15. Ensure that system level audit trails and audit logs exist to assign individual responsiblility and to identify and reconstruct events	Ch 18	Ch 3.2, S6 and Ch 4.6 R53 to 65	Ch 3.13	Ch 3.3.9	6.GSS.3 and Apdx C, pg 18C

	NIST SP 800-12	NIST SP 800-13	NIST SP 800-14	NIST SP 800-16	NIST SP 800-18
General Controls					
16. Perform reviews (including self-assessments reviews or audits) of security controls periodically					Ch 4.2
17. Perform system certifications and accreditations prior to implementation and periodic reaccreditations of the system	Ch 8.4.3.2, 8.4.3.3, 8.4.4.4 and 9.1				Ch 4.5 and Apdx C, pg 13C
18. Develop Information Resource (IRM) strategic plan					Entire document
19. Incorporate security plans into IRM strategic plan					Entire document
20. Develop Computer Security Incident Response Capability	Ch 12		Ch 3.7		Ch 5.GSS.9 and Apdx C, pg 16C
21. Ensure that a mandatory computer security awareness, training and education program exists and that it provides periodic follow-up COMPUSEC training	Ch 13.3, Ch 13.4. And Ch 13.5			Entire document and Ch 4.2.2 Cell 2.1A to Cell 2.2E	Ch 5.GSS.8 and Apdx C, pg 15C-16C
22. Ensure equipment and media are sanitized before disposal or object reuse					
23. Assign organizational responsibility					Ch 3.2.2
24. Assign individual responsibilities				Ch 3.3.6	Ch 3.2.4

Table 4 –NIST, FIPS, and GAO Publications

	NIST SP 500-153	NIST SP 800-3	NIST SP 800-4	FIPS PUB 73	GAO FISCAM Vol I
Application Controls					
1. Ensure transactions are authorized				Ch 3.3	Ch 4.1 AN-1 of draft
2. Ensure transactions are valid				Ch 3.1	
3. Ensure information is complete			Ch II. Sec B. 1. b.	Ch 4.3	Ch 4.2 AN-1 of draft
4. Ensure information is accurate/reliable	Ch 4.1.2.4		Ch II. Sec B. 1. b.	Ch 4.3	Ch 4.3 AN-1 of draft
5. Ensure information is timely				Ch 4.3	
6. Ensure system and data are secure			Ch II. Sec B. 1. b.	Ch 4.3 and Ch 7.1	
7. Ensure system is auditable and application controls are reviewed	Ch 4.1.2.4			Ch 4.3	
General Controls					
1. Develop and document a system security plan			Ch II. Sec A. 2.		Ch 3.1 SP-2
2. Ensure continuity of support (aka contingency plan/ disaster recovery plan) plan exists			Ch II. Sec A. 2. and Ch IV. Sec B.	Ch 6.2.6 and Ch 7.6	Ch 3.6 SC-2.1 and SC-3.1
3. Test the continuity of support plan			Ch II. Sec A. 2. and Ch IV. Sec B.		Ch 3.6 SC-4
4. Ensure Cost/benefit analysis exists	Ch 4.3.5.3 and Ch 4.4.3.1		Ch II. Sec B. 1. c		
5. Determine adequacy of security requirements	Ch 4.2.2.1 Ch 4.5.2.2 and Ch 4.5.5.3		Ch II. Sec B. 1. b	Ch 6.1	
6. Develop computer standards and guidelines for automated information system security and privacy (and computer support and operations)					

	NIST SP 500-153	NIST SP 800-3	NIST SP 800-4	FIPS PUB 73	GAO FISCAM Vol 1
General Controls					
7. Ensure adequacy of information security policies, procedures and practices of the agency					
8. Provide reasonable assurance	Ch 4.1.2.3				
9. Ensure that a formal configuration management control process exists for managing system change and keeps track of changes/modifications to the system and that changes/modifications to the system program modifications are properly authorized.					Ch 3.4 SS-3
10. Ensure that physical and environmental security controls exist			Ch IV. Sec I		Ch 3.4 SS-3
11. Ensure that identification and authentication controls exist			Ch IV Sec J. 1.	Ch 3.2	
12. Ensure that logical access controls exist			Ch IV Sec J. 1.		Ch 3.2 AC-3.2
13. Perform risk assessment			Ch II. Sec A. 2. Ch II Sec B. 1. B and Apdx C		Ch 3.1 SP-1
14. Ensure that life cycle requirements incorporate security concerns and issues	Entire document		Ch II. Sec A. 1. and Ch II Sec A.2.	Ch 4.3	
15. Ensure that system level audit trails and audit logs exist to assign individual responsiblility and to identify and reconstruct events			Ch IV Sec J. 3	Ch 3.4 and ch 4.3	Ch 3.2 AC-4.1
16. Perform reviews (including self-assessments reviews or audits) of security controls periodically			Ch IV Sec J. 3	Ch 4.3	
17. Perform system certifications and accreditations prior to implementation and periodic reaccreditations of the system			Ch II. Sec A. 2. Ch II Sec B. 1. B and Apdx C.		

	NIST SP 500-153	NIST SP 800-3	NIST SP 800-4	FIPS PUB 73	GAO FISCAM Vol 1
General Controls					
18. Develop Information Resource (IRM) strategic plan					
19. Incorporate security plans into IRM strategic plan					
20. Develop Computer Security Incident Response Capability		Entire document	Ch II. Sec A. 2.		Ch 3.1 SP-2 and SP-3.4 and Ch 3.2 AC-4
21. Ensure that a mandatory computer security awareness, training and education program exists and that it provides periodic follow-up COMPUSEC training			Ch II. Sec A. 2.	Ch 7.3.2	Ch 3.2 SP-4.2
22. Ensure equipment and media are sanitized before disposal or object reuse			Ch IV. Sec J. 5.		Ch 3.2 AC-3.4
23. Assign organizational responsibility					
24. Assign individual responsibilities					Ch 3.1, SP-3.2

APPENDIX XI

BIOGRAPHIES OF COMMITTEE MEMBERS

Arnold J. Pettis

Arnold Pettis is a systems auditor in AFAA's audit office located at Patrick Air Force Base (AFB), Florida. Arnie assisted AFAA personnel in planning audits covering broadly related and highly complex functions of a large multi-mission activity and developed and wrote system-related technical segments of the audit guide for highly complex agency-wide audits. Because of his ability to program in 12 languages and decode 12 database schematics, he has continuous access to 12 Air Force computer systems used in complex agency-wide audits.

Mr. Pettis has been with the AFAA for 6 years, the first 3 as an internal auditor and the last 3 as a Systems Auditor at Patrick AFB, Florida. Also, Arnie spent 9 years with the Defense Finance and Accounting Service (DFAS) Office at Langley AFB, Virginia. He worked the first 4 years as an operating accountant in charge of processing disbursement and reimbursement transactions for two appropriations. During the last 5 years with DFAS, he worked as a systems accountant responsible for security, operation, programming, maintenance, and administration of DFAS automated systems. Mr. Pettis received AFAA performance awards for applying technological advancements to several audit areas. Also, DFAS recognized him with special achievement awards for designing, developing, modifying, and implementing systems applications that enhanced financial operations.

Because of his computer expertise, Mr. Pettis is AFAA's only field auditor actively involved with the Committee on Paperless Auditing and the technical leader on the Access to Client Database subcommittee for the Federal Audit Executive Council. Also, he is the Eastern Audit Region representative for the AFAA Computer Technology Working Group. In addition, he is actively involved on two Patrick AFB quality groups—Year 2000 Working Group and Computer Infrastructure Working Group. Within the audit office, he is the Computer System Security Officer, Computer System Manager, and Local Area Network Administrator. As Computer System Security Officer, he wrote a comprehensive computer security plan used for gaining accreditation of the local area network in the Patrick AFB audit office.

Arnie graduated from Golden Gate University with a Masters in Business Administration degree, with a concentration in management. Also, he holds a Bachelor of Arts degree in Accounting from Saint Leo College and an Associate of Science degree in Resource Management Technology from the Community College of the Air Force.

James L. Rothwell

James Rothwell is a team leader in the Environmental Protection Agency's Office of Inspector General ADP Audit and Support Staff. Since 1990, he has been responsible for (1) providing information technology consulting services to EPA and OIG management and (2) planning and implementing information technology audits. He has a Masters degree in management in 1976 and has been a Certified Information Systems Auditor since 1988. During the past 30 years, he has directed numerous audits of information systems, computer operations, security programs, data management, and information technology procurement.

During his 30 year career, Mr. Rothwell has held a variety of audit positions within the Bureau of Engraving and Printing, U. S. Army Audit Agency, General Accounting Office, Department of Energy's Office of Inspector General, and Environmental Protection Agency's Office of Inspector General. He also spent 2 years on a detail from GAO with the Joint Financial Management Improvement Program working with a team that reviewed federal cash management by states. During his career, he spent about 25 years doing information systems audits.

William Coker

Mr. Coker has been an auditor for over 8 years at the Office of the Assistant Inspector General for Auditing, Department of Defense. He currently is working in the Automated Financial Systems Division for the Finance and Accounting Directorate. His audit experience has crossed a broad range of topics such as fuel usage for the military services, base realignment and closure, electronic data interchange/electronic commerce, and the Year 2000 computer problem. He began his Federal career at the Defense Logistics Agency in 1985.

Bill graduated with a Bachelor of Science from Virginia Tech in 1985 and is a Certified Information System Auditor.

LeRoy Stewart

LeRoy Stewart is a Headquarters Staff Auditor in the Air Force Audit Agency's (AFAA) Policy, Oversight, and Systems Division, Directorate of Operations, Arlington, Virginia. At the HQ AFAA, Mr. Stewart manages the Agency's computer security program and is responsible for computer security policies and procedures. He was instrumental in gaining accreditation of the headquarters Arlington-Rosslyn local area network recently. He also prepared a new agency-wide information systems security instruction used throughout the AFAA.

During his career, he has worked for the Naval Air Systems Command; OIG, DoD, Office of Personnel Management (OPM) Office of Inspector General; and the Office of Management and Budget (OMB). At Naval Air Systems Command (NAVAIR), he had responsibility for strategic information technology planning, information systems issues, and information systems life-cycle management. Mr. Stewart also managed NAVAIR's internal review program where he reviewed the command's video teleconferencing centers, local area network, and computer security program. At OPM, LeRoy completed a comprehensive audit of the Macon, Georgia mainframe computer facility and an agency-wide audit of the computer security process. The computer security audit resulted in a letter to the President and Congress that OPM had material weaknesses in computer security. During his detail with the Financial Integrity Task Force at OMB, LeRoy worked on computer security issues and assisted in revising OMB Circulars A-123, A-127, and A-130.

Mr. Stewart has a Master of Science degree in Information Systems Technology from George Washington University, Master in Business Administration degree from Shippensburg University, and Bachelor of Arts degree in Business Administration and History from the University of Northern Colorado. He also holds an Associate of Applied Sciences degree in Computer Information Systems (Magna Cum Laude) from Northern Virginia Community College. In 1997, he graduated from the 14-week Advanced Management Program for Information Systems Professionals at the National Defense University's Information Resource Management College in Washington, D. C.

LeRoy is certified in the Defense Department as an Acquisition Professional level 3 in the Communications-Computer career field. He has certificates from the General Services Administration's 1000 by the year 2000 Information Resource Management program, George Washington University's Information Resource Management program, Learning Tree International's Open Systems Professional and Local Area Network Professional programs, and National Defense University's Chief Information Officer program. During his career, LeRoy served as the Treasurer of the Washington Chapter of the EDP Auditor's Association and as a Board member of the Washington Chapter of the EDP Auditor's Association where he coordinated the Certified Information Systems Auditor Review course.

Anthony E. Broadnax

Mr. Broadnax is a native Washingtonian and has been a Department of Defense auditor since 1978. During his 21-year career, he worked 13 years with the Naval Audit Service and 8 years with the Defense Logistics Agency. While working for these two agencies, he has accumulated several awards and honors for outstanding performance. His diverse auditing experience includes reviews in the areas of project management; financial management; foreign military sales program; Year 2000 assessments; Morale, Welfare, and Recreation reviews; logistics; and other areas. He has been included on special projects such as information system security and several hotlines. He has also conducted assist work for the Department of Defense Inspector General's Office. In 1982, he received the honor of being named one of the Outstanding Young Men of America.

Tony obtained his undergraduate degree from Hampton University and a Master of Business and Public Administration degree from Southeastern University. He has taken numerous job-related courses. He is a part-time administrator with Maple Springs Baptist Bible College and Seminary.

James D. Raube

Mr. Raube is the Deputy Assistant Auditor General (Operations) for the Air Force Audit Agency. He is responsible for overseeing (1) development and dissemination of Agency policy, (2) internal reviews of Air Force Audit Agency operations, (3) development and operation of the Agency's management information system, (4) audit performance measurement, and (5) final report processing. He also serves as chair for the Federal Audit Executive Council's committee, Auditing in a Paperless Environment. In that role, he has convened periodic meetings in the National Capitol Region that address paperless auditing topics and also led subgroups dealing with such subjects as information systems security and audit access to client databases.

In his previous position, Jim managed the area audit office at Peterson Air Force Base (AFB) CO. In that position, he supervised 15 auditors who conducted audits at Air Force locations throughout Colorado and Wyoming, including Falcon AFB CO, F.E. Warren AFB WY, the Air Force Academy, and Peterson AFB CO. Prior to that assignment, Mr. Raube served as chief of the Agency's training division, which included responsibility for managing six in-house schools as well as arranging for a multitude of government and commercial training courses for Agency personnel.

During his career, Jim has held a variety of audit positions with the AFAA, Department of Energy, and U.S. General Accounting Office. His awards include the Association of Government Accountants National Education and Training Award. Mr. Raube is a CPA and has a Masters of Business Administration degree.