SMALL BUSINESS ADMINISTRATION
STANDARD OPERATING PROCEDURE

AUTOMATED INFORMATION SYSTEMS SECURITY PROGRAM 90 47 2

INTRODUCTION

1. Purpose. To establish guidelines and procedures for SBA's Automated Information Systems Security.

2. Personnel Concerned. All SBA employees, contractors, and other users who use automated information systems.

3. Directive Cancelled. SOP 90.47.1

4. Originator. Office of the Chief Information Officer (OCIO)

5. Distribution. Standard

Effective Date: 7/20/2005

Table of Contents

CHAPTER 1

INTRODUCTION

1. What Is the Purpose of the Small Business Administration's Automated Information Systems Security Program?

The purpose of the Small Business Administration's (SBA) Automated Information Systems (AIS) Security Program is to ensure adequate protection of SBA's AIS. AIS is an automated, discrete set of information resources (which includes both Government information and information technology) organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures. This document supercedes 90.47.1, "Automated Information Systems Security Program," dated July 17, 2000.

2. What Rules Govern the AIS Security Program?

The AIS Security Program is mandated by the following two authorities:

a. The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems." OMB Circular A-130 implements a number of Federal laws relating to information resources management (for example, the Paperwork Reduction Act, the Clinger-Cohen Act; and the Government Performance and Results Act).

b. The Federal Information Security Management Act of 2002 (FISMA).

3. What Are the General Requirements of SBA's AIS Security Program?

SBA must maintain an AIS Security Program to ensure that computerized data and other valuable Agency resources controlled by computers are safeguarded from inadvertent or deliberate access, disclosure, modification, destruction, or misuse. A full-time Director, Information Security reporting to the Chief Information Officer or the Deputy Chief Information Officer, will manage the AIS Security Program.

In accordance with OMB Circular A-130, Appendix III, the SBA AIS Security Program must include:

a. A personnel security program for all personnel, including both Federal and contractor, who are involved with the operation or maintenance of AIS. This program must be in accordance with guidance from the Office of Personnel Management.

b. A security awareness and training program to ensure that all individuals involved with the operation or maintenance of AIS are aware of AIS security policies and procedures.

c. Sensitivity determinations for all data contained in AIS installations or automated applications within SBA.

d. A risk assessment program to evaluate vulnerabilities existing in AIS. Appropriate cost-effective controls are identified and implemented during the annual internal control process carried out by the program office responsible for each AIS, in accordance with the Agency internal control requirements of OMB Circular A-123, "Management Accountability and Control."

e. A management control process to ensure that appropriate administrative, physical, personnel, and technical AIS security requirements are specified in bid offerings, proposals, and contracts for AIS equipment and services.

f. An Agency continuity of operations program to ensure that critical Agency AIS are available and operable in the event computer processing is not available due to incapacitation of SBA's AIS.

g. Defined security responsibilities assigned in writing to specific individuals.

h. Security plan prepared and tested for each AIS (a System Security Plan Template is available from OCIO to be used for this purpose). The plan must include system configuration, links to other AIS, an overview of the security requirements of the AIS, controls in place or planned to be implemented in order to meet security requirements and delineation of responsibilities and expected conduct of users who access the AIS. The security plan must be dated for ease of tracking modifications and approvals.

i. System usage and final risk determinations authorized in writing and reviewed and reauthorized at least every 3 years or when major changes are made.

j. Specialized system and security training for all users, annually refreshed, before the users are allowed access to an AIS.

k. Identification of material weaknesses and deficiencies in systems in the annual Federal Managers' Financial Integrity Act (FMFIA) report.

l. A summary of systems security plans and major applications plans in the Strategic Information Resources Plan required by the Paperwork Reduction Act of 1995, 44 U.S.C. Section 3506 (b) (2).

m. User access to SBA computer systems based on a need-to-know, need-to-use basis. User access to SBA major applications are also based on a least privilege basis; that is, users will be granted the least amount of privilege needed to perform their duties. User privileges will be reevaluated quarterly to ensure that the least amount of access privilege is continually in-force for access to SBA major applications.

4. To Whom Does this SOP Apply?

This SOP applies primarily to SBA employees, and the term “you” means an SBA employee. Portions of this SOP, where indicated, also apply to SBA’s contractors and employees of such contractors, where those contractors or employees have access to and are authorized to use SBA’s AIS. To the extent that this SOP applies to outside contractors and their employees, SBA’s contracts with those contractors will incorporate such SOP provisions by reference or restate such provisions within the contracts themselves in order to make them binding on such contractors.

This page is left blank intentionally.

CHAPTER 2

RESPONSIBILITIES

1. What Are the Responsibilities of the SBA Administrator?

In accordance with FISMA, the SBA Administrator is responsible for:

a. Providing information security protections commensurate with risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information within SBA's information systems;

b. Complying with all applicable laws and regulations concerning information security;

c. Ensuring that information security management is integrated with Agency strategic and operational planning; and

d. Ensuring that senior Agency officials provide information security for the information and information systems that support the operations and assets under their control.

2. What Are the Responsibilities of the CIO?

The CIO has been delegated the overall responsibility for the development and implementation of the Agency AIS security program. The CIO is responsible for:

a. Designating a management official, the Director, Information Security who will have overall responsibility for the development and implementation of the Agency AIS security program.

b. Establishing policies, standards, and procedures to ensure that specific administrative, physical, and technical security controls are in place for SBA's AIS.

c. Maintaining an accurate list of all networking devices.

d. Applying security patches and updates to SBA's AIS devices in a timely fashion.

e. Ensuring that only certified and accredited systems are moved into production.

3. What Are the Responsibilities of the Director, Information Security?

The responsibilities of the Director, Information Security are to:

a. Develop and maintain an Agency AIS Security program consistent with Government-wide policies, procedures, and standards concerning the security of applications, personnel, and computer installations.

b. Develop and disseminate information security policy and standards for the SBA AIS Security program, including SOPs and other AIS Security program directives.

c. Ensure that an appropriate level of security is maintained in all SBA AIS, which level will depend on risk and magnitude of potential harm.

d. Establish a program of periodic testing and evaluation of each general support system (GSS) and major application (MA) as (defined in OMB Circular A-130, Appendix III, paragraphs A.2.c and A.2.d). Within this SOP, each SBA GSS and MA will be referred to as a system. The testing and evaluation will focus on the effectiveness of information security policies, procedures, and practices and will include testing of management, operational, and technical controls of each AIS.

e. Create and maintain a comprehensive continuity of operations (COOP) and a Business Resumption Plan (BRP) for each AIS.

f. Establish a security awareness training program to inform Agency and contractor personnel of their security responsibilities and how to fulfill them.

g. Establish procedures for responding to and reporting on security incidents.

h. Establish a process to ensure that implementation of OMB Circulars A-130 and A-123 is coordinated to maximize the effectiveness of computer security and internal control procedures employed.

i. Conduct vulnerability assessments on Agency automated data processing (ADP) resources and assist SBA management and system owners in determining the level of threat to ADP resources.

j. Refer all suspected criminal violations, including theft of computer hardware and software, to the Office of the Inspector General (OIG), Investigations Division.

k. Coordinate with the OIG, Investigations Division, in the investigation of AIS security breaches and recommend emergency procedures if necessary.

l. Work with the designated Agency official responsible for meeting the requirements of the Privacy Act of 1974 (5 U.S.C. 552a).

4. What Are the Responsibilities of the Computer Emergency Response Team?

The Computer Emergency Response Team (CERT) was established to investigate computer security related incidents under the supervision of the Director, Information Security. The CERT has review and disposition authority for incidents assigned to it. The CERT includes personnel from the OCIO, Headquarters program personnel, and district information resource managers (IRMs); SBA Service Center security officers will be included on an ad hoc basis, when appropriate. The CERT will report its findings to the CIO for transmittal to the affected organization and the Administrator. Security incidents should be reported to the Director, Information Security in the OCIO. More detailed information can be found in the SBA CERT Guide. The SBA CERT Guide can be found at: http://yes.sba.gov/offices/ociosec/ on the SBA Intranet.

5. What Are the Responsibilities of the System Owner?

Under OMB Circular A-130, Appendix III, paragraph A.3, functional program managers are responsible for ensuring the security and integrity of each MA AIS containing information for which that program manager is responsible. These program managers are called the "system owner" for that MA, and the system owner must be a Management Board member. The OCIO will coordinate with the system owner of each MA the required security reviews to ensure that adequate procedures and controls are in place to ensure the security and integrity of each MA. The OCIO is responsible for the security of all GSS. See Appendix 3 for a list of all MA and GSS systems within SBA and the corresponding system owner.

The responsibilities of the MA system owner are to:

a. Assign or ensure the assignment of an appropriate information sensitivity level to the information processed, stored, or transmitted by the AIS, based on categories provided by OCIO, for example, Sensitive but Unclassified (SBU), Privacy Act, Procurement Sensitive, For Official Use Only (FOUO), etc.

b. Appoint in writing a system owner's point of contact, and forward a copy of the appointment memorandum to the Director, Information Security.

c. Ensure that any investment or budget request includes resources and funds necessary to adequately secure the AIS.

d. Establish timeframes to correct system weaknesses identified in risk assessments, internal control reviews, or audits.

e. Report as required on the progress in correcting system weaknesses for the SBA Plan of Action and Milestones (POA&M).

f. Validate that weaknesses have been corrected and maintain an audit trail of the modifications or corrections as back-up for a third-party review.

g. Work with the OCIO – Office of Information Security, and particularly with the Compliance Division within that office, to develop and test semi-annually a COOP and a BRP.

6. What Are the Responsibilities of the System Owner's Point of Contact?

The responsibilities of the system owner's point of contact (POC) are to:

a. Prepare or oversee the preparation of AIS security plans, risk assessments, disaster recovery/contingency plans, and system interconnection agreements, and maintain other system-related documentation for each AIS for which he or she is appointed.

b. Grant access to MA systems based upon need-to-know, need-to-use basis. Also, grant system access based upon the least privilege necessary to perform assigned duties.

c. Review system access user privilege listings on a quarterly basis to ensure that access privileges are necessary to perform their assigned duties.

d. Promptly notify System or Database Administration personnel when system access requirements change or are terminated.

e. Conduct, oversee, or facilitate the annual computer security "self-assessment."

f. Coordinate with the Director, Information Security any actions necessary to correct any weaknesses identified in the AIS he or she manages.

g. Perform and document a computer security risk assessment in the design phase, and write a system security plan during the development/acquisition phase, of the system development life cycle (SDLC) for both new and modified systems.

h. Coordinate with the Agency's Privacy Act responsible official and the Director, Information Security to conduct a system test and evaluation during the implementation/test phase of the SDLC for both new and modified systems.

i. Coordinate with the SBA Office of Administration to publish a "System of Records" in the *Federal Register* for any system that contains information protected by the Privacy Act.

j. Ensure that any new systems or modifications of existing systems conform to the SBA System Development Methodology (SDM).

k. Ensure that data is retained and archived in compliance with Federal records retention requirements.

l. Develop and document system interconnection/information sharing agreements. Obtain approval from the OCIO and Office of General Counsel of the interconnection/information sharing agreement with outside agencies before the connections are made. The OCIO requires that an interconnection/information sharing agreement be developed and documented for connections between a non–OCIO managed system and an OCIO managed system. The Office of General Counsel does not need to approve internal connections.

m. Complete the Computer Security Awareness Tool (CSAT) for Functional Program Managers annually.

7. What Are the Responsibilities of the Regional Administrators, District Directors, Branch Office Managers, and Disaster Area Office Directors?

Regional Administrators, District Directors, Branch Office Managers, and Disaster Area Office Directors are responsible for:

a. Implementing procedures to ensure that administrative, physical, and technical security controls are in place for AIS activities within their offices.

b. Maintaining appropriate security controls in sensitive AIS maintained within their offices.

c. Developing and testing semi-annually a COOP and a BRP.

8. What Are the Responsibilities of the District AIS Security Officers?

District AIS Security Officers (DSO) are responsible for:

a. Using the special password-generating transaction to generate passwords for users of the mainframe data communications network who must have access to sensitive/critical transactions.

b. Implementing procedures to ensure that administrative, physical, and technical security controls are in place for AIS within their offices.

c. Maintaining appropriate security controls in sensitive AIS within their offices.

d. Implementing an AIS contingency plan that addresses the timely recovery of ADP operations at the district office.

e. Supporting all IT Security initiatives initiated by the OCIO or the Director, Information Security which are essential for the Agency to comply with federal regulations and mandates (such as FISMA and OMB Circular A-130, Appendix III).

9. What Are the Responsibilities of an Outside Contractor Which Performs AIS Security Functions?

The Director, Information Security, may contract with outside contractors for computer facilities to process SBA information. The terms of such contracts must require the outside contractor to:

a. Designate a point of contact (for example, a project manager) that will be responsible for ensuring that the outside contractor complies with the remainder of the requirements listed in this paragraph.

b. Ensure that an appropriate level of security is maintained to protect the outside contractor's computer(s) and facility that process SBA information.

c. Assist the Director, Information Security in the investigation of AIS security breaches that affect processing at the outside contractor's facility.

d. Implement, at the direction of the Director, Information Security, SBA AIS policies, procedures, and standards that affect computer systems that process SBA information at the outside contractor's facility.

e. Represent the outside contractor as the focal point for periodic information security audits and internal control reviews.

f. Recommend security enhancements and improvements where appropriate.

g. Ensure the timely correction or remediation of discrepancies found during the periodic information security audits and internal control reviews.

h. Ensure that an accurate list of all networking devices is maintained.

i. Ensure that security patches and updates are applied to SBA-owned computing devices in a timely fashion.

j. Forward a list of computer security incidents detected during each month to the Director, Information Security by the fifth working day of the following month. Examples of the types of incidents to report are: successful/unsuccessful network penetrations; root or user account compromises; denial of service attacks; website defacing attacks; malicious code and viruses; probes; and scans.

k. Complete the CSAT for contractors annually.

10. What Are My Responsibilities If I Am a System Administrator or Database Administrator?

A System Administrator is an individual responsible for maintaining a multi-user computer system, including a local-area network (LAN), wide-area network (WAN), telephone system, or voice-mail system. The System Administrator also can be called the Sysadmin or SA. A Local Area Network (LAN) Administrator is a System Administrator assigned responsibility only for one LAN.

Database Administrators work with database management systems software and determines ways to organize and store the data. They determine requirements, set up computer databases, and test and coordinate changes. The Database Administrator ensures the database's performance, understands the platform the database runs on, and adds new users. The Database Administrator also plans and coordinates security measures.

The responsibilities of the System Administrator or Database Administrator are:

a. Ensuring that security patches and updates are applied in a timely fashion after testing, and maintaining a log of what patches were applied to each AIS; when the patch was applied; and if a patch was not applied, why not.

b. Ensuring that anti-virus software is installed, updated signature files are applied in a timely fashion, all files are scanned for viruses when accessed (if the anti-virus software is capable of performing this function), all files are scanned weekly, and the automatic virus-reporting tool is enabled at all times.

c. Reviewing audit logs/trails for anomalies at least weekly and reporting any anomalies detected to his or her supervisor or the Director, Information Security.

d. Ensuring that servers are assigned OCIO-provided static IP addresses and are properly registered in the Domain Name Service (DNS).

e. Ensuring the timely correction or remediation of discrepancies found during the periodic information security audits and internal control reviews.

f. Ensuring that AIS are set up using OCIO-developed and Director, Information Security-approved standard configuration guides.

g. Maintaining an administrator guide or continuity folder/book in the format prescribed by OCIO – Office of Communications and Technology Services (OCTS). A copy must be maintained on site as well as in the designated backup facility.

h. Assisting the Director, Information Security and CERT team in investigating a security incident and assisting in correcting any weakness that was exploited and that resulted in a security incident.

i. Ensuring that audit logs/trails provide the capability to support after-the-fact investigations of how, when, and why normal operations ceased, and the capability to trace user actions, both successful and unsuccessful.

j. Ensuring that audit logs are maintained for the time prescribed by the SBA records management program.

k. Ensuring that an Office of General Counsel–approved warning banner/notice is displayed whenever someone attempts to log on to the system.

l. Upon receipt of notification from a user's supervisor (for an SBA employee) or from a COTR (for a contractor's employee), performing all necessary actions for suspending or deleting old user accounts and reassigning or deleting the data sets associated with those old accounts.

m. Performing regular back-ups of the SBA AIS for which the administrator is responsible, as often as appropriate for the particular AIS and preparing documentation associated with such back-ups.

n. Completing the CSAT for System Administrators annually.

11. What Are My Responsibilities If I Am a District Information Resources Manager (IRM)?

You are responsible for:

a. Scanning all software received, regardless of source, prior to releasing or loading it.

b. After receiving software from vendors, Headquarters, or district personnel, contacting the OCIO – Network Integration Branch for clearance prior to releasing or loading it.

c. Testing and validating that SBA-required security requirements are in place for the non-SBA IT mobile equipment to be used by District office personnel.

d. Participating on the Computer Emergency Response Team (CERT).

e. Completing the CSAT for DSOs/IRMs annually.

12. What Are My Responsibilities If I Am an AIS User?

As an AIS user, you are accountable for all actions associated with your AIS user identification (ID). You may be held liable for actions which you perform within your official duties, but which constitute improper access or modification to a system; unauthorized distribution of system information to third parties; or improper modification of information within a system. For purposes of this paragraph, "you" also refers to outside contractors and their employees who have access to SBA's AIS.

You are responsible for:

a. Actions taken while you use an SBA AIS, or actions taken with your User ID and password. The Director, Information Security, may examine any actions attributed to your User ID and password combination to identify whether you are the actual originator of any improper abusive actions occurring within the AIS or whether someone else has misappropriated your User ID and password.

b. Being familiar with and complying with all Agency standards, policies, and procedures established pursuant to the AIS security program, both as identified in this SOP and pursuant to instructions issued by the Director, Information Security.

c. Changing your LAN/WAN password(s) every 90 days, and ensuring that all passwords you select comply with policies and guidelines issued by the Director, Information Security (See Appendix II). A password must not be easily guessed but should be easily remembered. It must be a minimum of 8 characters and contain at least three of the following: upper case letters, lower case letters, numerals, and special characters. Users must not divulge their passwords to others.

d. Invoking the password-protected screen saver before leaving your assigned workstation while your computer is accessing AIS. Also, you must protect your workstation by using a password-protected screen saver that will secure the workstation after 5 minutes of inactivity.

e. Reporting security incidents to your supervisor or Director, Information Security.

f. Reporting to your supervisor when you receive a computer-generated message, or otherwise have reason to believe, that Agency-approved virus protection software is not installed or functioning properly on the SBA-provided personal computer (PC) assigned to your use. At the time you start up your PC, observe the log-on script to see whether the installed virus protection software is running, and report any PC viruses that you observe or detect to your supervisor immediately.

g. For SBA employees and contractors: Completing the Computer Security Awareness Tool (CSAT) for end-user on-line training within 45 days of entry on duty and annually thereafter. New employees will be instructed by their immediate supervisor to take the CSAT online for end users within their first 45 days of employment. The OCIO will issue an annual Information Notice to remind all employees to complete the CSAT annually.

h. Reading and signing the "Information Technology – Computer Security Rules of Behavior" form. You must give the signed form to your supervisor (for SBA employees) or COTR (for outside contractor employees) prior to signing-on to the SBA LAN for the first time.

i. Storing information on a file server, not on the hard drive of the user's assigned PC. Users storing SBA information on a PC hard drive must back-up that information at least monthly. Users also must not file non-shared information on a common or shared directory on a LAN.

This page is left blank intentionally.

CHAPTER 3

AIS SECURITY POLICIES

1. What Security Controls Are Required for SBA Computer Facilities and Computer Facilities Contracted by the Agency?

The following minimum controls must be in effect for SBA automated data processing (ADP) facilities and server rooms housing any SBA AIS. Any SBA official contracting with a facility outside SBA to house any SBA AIS, including networking equipment, must include as a contract term, the provisions stated in this paragraph. OCIO and system owners may implement additional security controls when supported by risk assessment.

a. Responsibility for day-to-day security management of SBA ADP facilities must be assigned to a specific individual knowledgeable in ADP technology and computer security methodology.

b. Automated physical security controls must be in place to limit physical access to only authorized personnel. A list of authorized personnel must be maintained and access revalidated at least quarterly.

c. Physical and technical controls must be implemented to safeguard computer media.

d. Operating system software must contain adequate security controls to minimize the likelihood of unauthorized access to or use of AIS resources.

e. There must be a statement that declares to the user at logon that the system is protected against inappropriate use and violators will be prosecuted to the fullest extent of the law. The Office of General Counsel must approve the statement or warning banner.

f. Password change screens must revalidate the old password and new password. The new password must be typed in a secure field to prevent compromise.

g. User access control procedures must include the following:

   1) Passwords must be used to authenticate the account user. User accounts and passwords may not be shared between individuals.

   2) The password must be changed immediately if there is a reason to suspect that the password has been compromised. When necessary, administrators must be able to assign new passwords after confirming the user's identity.

3) Passwords must be protected by administrative, physical, and technical security controls from unauthorized disclosure or misuse. Password files must be encrypted.

4) Passwords must be a minimum of eight characters and contain at least three of the following: upper case letters, lower case letters, numerals, and special characters. Automated password complexity checking should be enabled if available for the operating system or database management system. Note: The Director, Information Security has granted an exception for the QTERM application. This exception allows user passwords of six characters in length. QTERM users will be revalidated once each calendar year.

5) Users must be able to change their own passwords, and passwords must be set to automatically expire every 90 days.

6) The initial password or a reissued password must be forced to change with the first use. A forgotten password will be replaced, not reissued.

7) Accounts will be removed as quickly as possible but no more than three working days from the time the user is no longer authorized access to the computer system or computer application. Inactive accounts must be suspended after 120 days of inactivity. Supervisors of departing employees and COTRs for contractor employees must immediately notify system administrators and the Director, Information Security, when such users no longer need access to SBA AIS.

8) Expiration dates must be assigned to temporary accounts.

9) A history of at least eight passwords must be maintained before a password can be reused.

h. System software and data must be backed up on a regular basis. Full system backups must be performed at least once weekly. Incremental data backups (backups of data that has changed since the last full backup) must be performed nightly. The backup procedure must include the production of a second set of full backup media, which is stored off-site in an approved data repository. Additional backups may be taken as necessary. See Appendix V for more information.

i. Audit logs and audit trails are required on all SBA AIS, to maintain user accountability. Audit logs and trails must work in concert with logical access controls, to identify and provide information about users' activities, including improper modification of data (e.g., introducing errors into a database). The audit log or trail must record "before" and "after" versions of records. The System or Database Administrator must review security log files or audit logs/trails at least weekly to detect unauthorized access to sensitive data, misuse of the computer system, or other unauthorized activity.

j. The computer facility must be equipped with auxiliary power-generating equipment that will provide sufficient power to allow graceful system shutdown in the event of a power failure.

k. Remote access security controls must include:

1) The use of communications servers to permit remote dial-in access to SBA's wide area network (WAN).

2) The use of secure servers for Internet access to SBA's private network. The connection should be protected by a National Institute of Standards and Technology (NIST)–approved encryption method.

l. The following personnel security controls must be in place for SBA AIS:

1) Sensitive ADP positions must be identified and forwarded to the Office of Human Capital Management in accordance with instructions furnished by that office.

2) Contractors filling sensitive ADP positions are required to meet the same personnel security requirements as their Federal employee counterparts.

m. Magnetic media must be sanitized (i.e., information on such media must be removed) prior to disposal by one of the following three approved methods, and a log of who completed the sanitization action must be maintained.

1) Overwriting – the use of a software program to write meaningless information over the existing information on the media. Common practice is to overwrite the media three times. Overwriting is not the same as merely deleting a pointer to a file (which is what typically happens when a delete command is used). SBA has a license for a program called "Kill Disk" (available through OCIO and IRMs) that will overwrite diskettes and hard drives.

2) Degaussing – a method by which data is magnetically erased from a media. Two types of degaussing exist: strong permanent magnets, and electric degaussing.

3) Destruction – destruction of the media by shredding, burning, or crushing. The preferred method of destruction for back-up magnetic tapes is to cut the tape into pieces.

n. More than one individual must perform different portions of system support functions to ensure that one individual does not control all stages of a process. If one individual controls all stages of system support functions the potential exists for malicious acts to go unnoticed. Specifically:

1) There must be a separation of duties between the security personnel who administer the access control functions and those who administer the audit trail.

2) Documented job descriptions should accurately reflect assigned duties and segregation of functions.

3) Where resource limitations make segregation of duties impossible to implement, senior management must ensure that appropriate supervisory review measures are in place to compensate for the lack of separation of duties.

2. What Are the Minimum Security Controls for Mainframe Computers?

a. Responsibility for day-to-day security management of the ADP facility must be assigned to a specific individual knowledgeable in ADP technology and computer security methodology.

b. Using Team Quest Site Management Complex (SIMAN), the Director, Information Security or designated District AIS Security Officer will establish the initial user account and password or reissue a user's password after proper use verification.

c. User validation must occur at logon or the initial connection to the computer environment.

d. Users will be granted full access (read/write authority) to their personal data areas and the common shared area. Access to application areas will be restricted to "read only." Access to system areas will be restricted to the System Administrator.

e. Accounts must be suspended immediately when a user leaves SBA employment. Accounts must be monitored periodically to remove inactive accounts. Inactive accounts must be suspended after 120 days of inactivity.

f. Accounts must be locked after three invalid access attempts. Where possible, the station also should be locked to prevent the user from repeating the attempts.

g. Workstations must be logged out, or locked, with re-access only with entry of a password after 15 minutes of inactivity.

h. The OCIO must approve connections to the private network from any source outside the network before connection attempts are made.

3. What Are the Minimum Security Controls, Software Distribution Procedures, and Copyright Policies for Personal Computers?

a. The following minimum security controls apply to usage at SBA

1) The manager with operational responsibility for an office or organizational unit is responsible for the protection of the PC hardware, system software, and sensitive data, within that office or organizational unit.

2) PCs must be securely maintained. Laptop computer equipment located in open areas should be secured to the desk when possible.

3) PCs should be protected using a password-protected screensaver that secures the workstation after 5 minutes of inactivity. Prior to leaving the work space for a short period of time, the user should manually activate the password-protected screensaver by pressing the Ctrl, Alt, and Delete keys simultaneously; the password-protected screen saver will then be invoked. Users should power off their PC when the user leaves the workstation for the day.

4) SBA information should be stored on a file server and not in the hard drive of individual PCs. If SBA information is stored on a PC, it is the user's responsibility to back up the data at least monthly.

5) Agency standard computer virus detection and eradication software must be installed on all Agency computers. The software must be installed in such a manner as to be loaded each time the system is turned on or reset (rebooted via ctrl-alt-del). Virus detection software updates must be applied as soon as available to maintain the maximum level of protection against viruses. The anti-virus software must be configured to automatically scan all files when they are accessed.

6) Files and diskettes received from any source must be scanned for viruses before being used on Agency AIS.

7) Sensitive data files on laptop computers must be, at a minimum, password protected.

8) Additional controls may be instituted where warranted.

b. The following guidelines must be followed when distributing or receiving software for SBA PCs:

1) OCIO – OCTS, Network Integration Branch (NIB) must coordinate and control the distribution of computer software to regional and district offices. Software intended for regional or district office use must be sent directly to the NIB for security analysis and distribution.

2) (2) District IRMs must scan all software received, regardless of source, prior to releasing or loading it.

3) Regional and district program personnel receiving software from vendors or Headquarters must submit the software to NIB or District IRM for analysis before

loading it. District IRMs receiving software from vendors, Headquarters, or district personnel must contact NIB for clearance prior to releasing or loading it.

4) At Headquarters, the OCIO will be the review point for software developed or provided for general distribution. All such software must be submitted to the OCIO for security analysis prior to being released or loaded and tested for compatibility.

5) Headquarters program offices must submit all commercial software to NIB for compatibility testing and security scanning prior to loading it for internal use.

6) The preferred method of software distribution is a software push conducted by NIB.

c. The following is SBA's PC software copyright policy:

1) An employee of the SBA must not copy, except as provided below, any software that is protected by a copyright unless authorized by the software license agreement that accompanies such software.

2) In order to protect the Agency's investment in software and to ensure the operational continuity of Agency programs, it is permissible to make a backup copy of copyrighted software.

3) The removal of Agency-purchased computer software from any Government-owned computer, office, or building for purposes other than official business is prohibited. Installation of software obtained in violation of copyright restrictions on Agency computers is also strictly prohibited.

4) This policy applies equally to employees of the Agency, contractors or other users doing business with or acting for the Agency, and any others who may have access to or be required to use commercial software in the performance of their assignments.

5) Employees violating this policy will be subject to appropriate disciplinary action.

6) Should the owners, vendors, or authorized custodians of copyrighted software choose to sue the individuals concerned, and if the Agency determines that such copying was illegal and unauthorized by SBA, the Agency may choose not to provide such employee any support, legal or otherwise, in defense of such action.

7) Program managers must provide lists of purchased software to the OCIO – Office of Productivity Enhancement Staff (PES) which will maintain a master list of authorized software licenses.

8) NIB will conduct software inventory scans of all SBA-owned PCs at least quarterly to ensure an accurate listing of installed software. Results of the software inventory

scans will be compared to approved software lists and number of license information. Any discrepancies will be reported to the Director, Information Security.

4. What Are the Minimum Security Controls for UNIX, Linux, or AIX-Based Computers?

Computers running UNIX, Linux, or AIX operating systems require special security precautions. Improper setup or misuse of UNIX-based computers can jeopardize the security of the SBA network. Therefore, any individual wishing to acquire UNIX, Linux, or AIX-based computers must first receive authorization from the CIO. The OCIO will coordinate the installation and configuration of the system to ensure that it poses no security risk. Configuration must include the installation of OCIO user accounts on the system to aid in problem analysis and in security evaluations.

Because UNIX and Linux operating systems can be installed on any type of computer, laptop to mainframe, the following guidelines apply to all systems running a UNIX operating system:

a. The SUPERUSER account (ROOT) must be protected with a password of at least eight characters, two of which must be special characters (!,$,%,*). ROOT passwords must be changed at least once every 2 months. Passwords should be changed more frequently as conditions warrant.

b. All user accounts must be protected by passwords of at least 8 characters and contain at least three of the following: upper case letters, lower case letters, numerals, and special characters. At a minimum, user passwords must be set to expire every 90 days. If the operating system comes with password complexity checking software, it must be enabled.

c. Users must not create files that are “world writeable” (meaning writeable by anyone). User IDs not listed in /etc/ftpusers must not transfer files using FTP. This will ensure that files are not deleted, altered, moved, or mismanaged by anyone other than the owner or group associated with the file. Files, at a minimum, should have the write bit for “other” removed from the file permissions.

d. UNIX, Linux, or AIX-based computers requiring remote user logon access must have authentication software installed that can generate one-time passwords.

e. UNIX-based computers that do not require remote access must have all remote services/utilities disabled. When possible, users should be isolated from the operating system through the use of user interfaces or menus.

f. Modems must not be connected to UNIX, Linux, or AIX-based systems. Access to external information sources (e.g., Internet) must be made through the WAN. Direct connections are prohibited.

g. System software and data must be backed up on a regular basis. Full system backups must be performed at least once weekly. Incremental data backups (data that has changed since the last full backup) must be performed nightly. The backup procedure must include the production of a second set of full backup media, which is stored off-site in an approved data repository. Additional backups may be taken and stored as necessary.

h. A programmable uninterruptible power supply (UPS) capable of supplying power for at least 15 minutes must be installed on each machine. The UPS must be programmed to gracefully shut down the computer when five minutes of UPS power remains.

i. Types of UNIX, Linux, and AIX servers include:

1) Client Servers - In addition to the foregoing, the following guidelines apply to client servers:

a. Users must access client servers through approved client front-end software provided by the OCIO. Other access methods are prohibited.

b. The Director, Information Security will establish client server accounts upon presentation of a request signed by the appropriate program manager. Client server accounts must not be shared. Users must not divulge their passwords to others.

c. The “/etc/ftpusers” file must be maintained to limit users’ access to FTP. User IDs not listed in /etc/ftpusers must not transfer files using FTP. At a minimum, this file should contain the ROOT user ID and other accounts generated by the UNIX, Linux, or AIX operating system.

d. The ROOT crontab should be monitored for chronological entries that execute scripts that don’t exist. In cases like this, any user can simply create the script specified, and thus have “root” execute any command the user desires.

e. All systems must be closed systems, not allowing access via another host’s security. Systems must be monitored for the presence of “.rhost” files and “/etc/hosts.equiv” files. Entries in these files give outside users access to the current system using remote shell commands.

f. User IDs that are deleted from the system must have their files either removed from the system or have their ownership given to another user ID on the system.

g. Users that successfully use the switch user command “su” will be logged and monitored. The “su” log will report use of the “ROOT” privileged activities.

h. Only the OCIO or the Office of Disaster Assistance may operate and maintain client server systems.

i. If the vendor supplies or supports a "lockdown tool" like Solaris Jumpstart Architecture and Security Scripts (JASS) toolkit, it should be used.

2) World Wide Web Servers - In addition to the general guidelines for client servers above, the following guidelines apply to Agency web servers:

a. UNIX-level user accounts are not permitted on web servers.

b. Users must access web servers through standard web browsers.

c. Web servers are for the dissemination of publicly available Agency information. Sensitive information relating to businesses or individuals doing business with SBA must not be placed on web servers. Information intended for dissemination via web servers must be reviewed by the OCIO, Office of General Counsel, Office of the Inspector General (OIG), and/or the Freedom of Information Act (FOIA) office to determine appropriateness for disclosure before being placed on Agency web servers. These offices also must review and clear in advance the disclosure of any material related to their operations.

d. Only OCIO may operate and maintain web servers.

e. OCIO must coordinate and approve all Web-based application development before any development is initiated. Offices wishing to have a web-based application developed must contact the OCIO's web development group for the appropriate procedures.

f. System Administrators must review for anomalies daily.

g. System Administrators may, if necessary, use Secure Shell (SSH) to remotely connect to web servers from inside the SBA private network.

h. A Privacy Act notice approved by the Office of General Counsel and responsible Privacy Act official must be displayed on any web page that requests data protected by the Privacy Act.

3) Communications Servers - Communications servers provide dial-in users access to the WAN. In addition to the general guidelines for client servers above, the following apply to communications servers:

a. OCIO will establish user accounts for employees upon presentation of an approved request signed by the appropriate program official. The employee will be given access to his/her LAN server and its associated privileges. No additional privileges will be granted.

b. User accounts must not be shared. Users must not divulge their passwords to others.

c. UNIX-level user accounts are not permitted on communication servers.

d. Only OCIO or an approved vendor under contract to the SBA may operate and maintain communications servers.

4) Internet Secure Servers - Internet secure servers are established to permit secure communications between SBA, customers, and business partners via the Internet. In addition to the general guidelines for client servers above, the following apply to Internet secure servers:

a. UNIX-level user accounts are not permitted on secure servers. The security agent of the server must generate logon IDs. The Director, Information Security will review and approve applications for user IDs upon presentation of a request approved by the appropriate program office.

b. Only OCIO may operate and maintain secure servers. OCIO will approve, coordinate, supervise and accomplish program office requests for access to, or use of, secure servers, including necessary program development/modification. Independent third-party development of secure server applications is not permitted.

5. What Are the Minimum Security Controls for the SBA Wide Area Network (WAN)?

The SBA WAN is the interconnection of SBA’s local area networks (LANs), web and secure servers, and Internet connection. The WAN is divided into private and public networks. The private or “corporate” network contains the LANs, client servers, communication servers, and the mainframe system. The public network contains the Internet connection, web servers, secure servers, and bulletin board. The public network is separated from the private network by a firewall.

The following guidelines apply to the WAN:

a. Government or sensitive data must not be placed on public systems. Government or sensitive data transmitted to official destinations via the Internet or other public or semi-public networks must be encrypted either by point-to-point session encryption or virtual private network (VPN) encryption. Acceptable encryption mechanisms include secure browsers (Microsoft Explorer 6.0 or above that support 128-bit encryption) to secure servers, secure telnet or secure ftp (source and destination), or other encryption methods that can guarantee session decryption only by the intended recipient.

b. Public-side access to Government data must be accomplished only via SBA's secure servers. No other access method is permitted.

c. Dial-in access to the private network must be accomplished via communications servers, unless OCIO has granted an exception.

d. OCIO and Office of General Counsel must approve connections to the private network from any source outside the network. Documenting the connection with an Interconnection Security Agreement is the responsibility of the program manager requesting the connection; however, the OCIO will assist with the technical details. Once approved, all such connections must be secured with a filtering router and a stateful packet inspection (SPI) firewall system. The standard Agency firewall system is Checkpoint Technology's Next Generation (NG) Firewall.

6. What Are the Minimum Security Controls for Local Area Networks (LAN)?

The following guidelines must be implemented and followed on all SBA LANs (servers and LANs):

a. LAN Administrators must perform a daily full-system backup on each server if not supported by the Live Vault system. Backups must be cycled through a minimum of 10 tapes (2-week cycle). One of the daily full backups must be maintained off site until replaced the following week.

b. Accounts granted administrative privileges must be limited to the minimum privileges required for administration of the LAN. Administrative passwords must be changed every 30 days rather than every 90 days as required for non-administrative users. Administrative accounts must be reviewed monthly to determine continuing need.

c. With the exception of the System Administrator and alternate, no employee will be granted permissions at the Root directory level (global permissions). Employees will be granted minimum access (normally "read only" or "read/execute") to needed directories. The general philosophy is that users have no permissions unless specifically granted (as opposed to granting global permissions and then removing unneeded authority).

d. Users will be granted full access ("read/write" authority) to their personal data areas and the common shared area. Access to application areas must be restricted to "read only." Access to system areas must be restricted to the LAN Administrator.

e. With the exception of the LAN Administrator, no accounts are created for specific application/function. Permissions must be granted only for that application or function and station restricted.

f. All LAN users must be assigned unique accounts.

g. All accounts must be password protected. Passwords must be a minimum of eight characters. Automatic password complexity checking software must be enabled to ensure that passwords are unique and hard to guess. Passwords must automatically expire every 90 days. "Grace" log-ins, (i.e., the log-ins allowed immediately after password expiration) must be limited to three and then lock the user out until a LAN Administrator unlocks the account.

h. "Guest" accounts are not permitted. Personnel requiring temporary access to a LAN must be issued a temporary user ID with an expiration date commensurate with need.

i. Accounts must be suspended immediately when an employee leaves SBA employment. LAN accounts must be monitored monthly for excess accounts. Accounts that have been inactive for more than 120 days must be locked.

j. Users must not store non-shared data in the common shared area. Common areas are reserved for temporary storage of working group files (files that need to be accessed by other employees). Non-shared data must be stored in the user's home directory on the LAN.

k. All system and application files, where possible, must be flagged as "read only."

l. The OCIO and the Office of General Counsel must approve connections to the private network from any source outside of SBA before connection attempts are made. Documenting an Interconnection Security Agreement is the responsibility of the program manager requesting the connection; however, the OCIO will assist with the technical details.

m. All servers connected to the LAN must use a static IP address assigned by the OCIO and be registered in the DNS.

n. All Windows servers connected to the LAN must have the SBA Domain Administrators Group added to the Local Administrators Group.

o. The appropriate anti-virus software must be installed and set to scan all files for viruses when accessed. At least once each week the anti-virus software must scan all files on the server for computer viruses. Anti-virus signature files must be updated whenever a new signature file is released by the anti-virus software vendor.

7. What Are the Minimum Security Controls for IT Mobil-Devices?

a. Before purchasing any IT mobile-devices such as laptop computers, personal digital assistants (PDA), smart phones, and other handheld computing devices you must obtain OCIO approval. OCIO must approve for connection to the SBA network all IT mobile-devices prior to connection. IT mobile-devices not owned and managed by SBA must have a waiver on file in the OCIO approved by the Director, OCTS, and the Director, Information Security, prior to connecting to the SBA network. Waiver approval procedures can be found in Appendix IV.

b. In the past IT mobile-devices have not generally been viewed as posing security threats. However, their increased computing power and ease of accessing networks and exchanging data with other such devices introduces new security risks into SBA's computing environment. As these devices begin supporting more networking capabilities, system administrators must carefully assess the potential risk they introduce into the current computing environment. To control and reduce the potential security risks, system administrators and system owners need to:

- conduct risk assessments,
- implement management controls,
- implement operational countermeasures, and
- implement technical countermeasures to safeguard the IT mobile-devices and SBA's networks.

c. System administrators can also implement the security standards recommended in the NIST (Draft) Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Device.* NIST Special Publication 800-48 provides practical guidelines and recommendations for mitigating the risks associated with these technologies. NIST Special Publication 800-48 is available at (http://csrc.nist.gov/publications/drafts.html).

8. What Are the Security Control Requirements for Development of Sensitive AIS?

The Director, Information Security in conjunction with the responsible program office must define the security requirements and specifications for sensitive AIS.

9. What Is the Disaster Recovery Plan (DRP)?

a. The DRP ensures continued operations in the event of a disaster or extended loss of computer processing power.

b. An AIS DRP must be in force to facilitate the timely recovery of ADP operations in the event of a disaster or extended loss of computer processing power. The AIS DRP is part of the Continuity of Operations Plan (COOP) developed by SBA.

c. The creation and implementation of appropriate disaster recovery plans is the responsibility of the system owner, regional administrator, district directors, branch office managers, and Disaster Area Office directors. The Director, Information Security and the OCIO Disaster Recovery Manager will provide guidance, coordination, and assistance.

d. A DRPmust be prepared and tested semi-annually for each MA system, each regional and district AIS, the Office of Financial Operations, and SBA's mainframe computer center. Each disaster recovery plan must address three areas:

1) Emergency procedures.

2) Backup operations.

3) Recovery procedures.

e. The disaster recovery planning process will consider:

1) Extent of emergencies.

2) Essential applications.

3) Backup alternatives.

4) Backup resources.

5) Contingency plan tests.

6) Contingency plan maintenance.

f. Tests of the DRP must be documented and retained for 1 year. Test documentation should include but is not limited to:

1) Personnel participating in the disaster recovery test.

2) The application(s) tested.

3) Initial planning meeting minutes.

4) High-level test criteria.

5) Test results, including obstacles, action items, exception conditions, and resolution.

10. What Are the Policies for Personnel Security?

a. ADP positions within SBA that involve programming, operation, design, or use of AIS or data must be evaluated as “critical sensitive,” “non-critical,” or “non-sensitive” using guidelines established by OPM (5 CFR Parts 731 and 732), OIG (SOP 90 21), and the Office of Human Capital Management (SOP to be issued at a later date).

b. SBA personnel must not allow contractor personnel occupying ADP positions designated as critical-sensitive to have access to SBA sensitive data until an appropriate clearance has been granted.

c. The Director, Information Security, must complete a Position Sensitivity Level Determination Form for each contractor position on SBA contracts for ADP services. The Director, Information Security, must forward a copy of the form to the OIG.

d. All SBA and contractor employees who have access to sensitive data must be made fully aware of their responsibilities for protecting sensitive data and for detecting and preventing misuse of AIS resources. They must also read and sign the SBA confidentiality agreement.

e. It is strongly recommended that managers introduce a policy in their offices that mandates shift rotation for individuals that are accessing high-risk, sensitive AISon a day-to day basis.

11. What Are the Security Policies for SBA ADP Contracts?

SBA ADP contracts that require contractors to access the SBA LAN or process SBA data at the contractor’s facility must include the requirements below:

a. General: The contractor must establish administrative, technical, and physical security measures at its computer facility to protect sensitive SBA information from unauthorized disclosure or misuse and to prevent unauthorized access to the contractor’s computer system. The contractor must describe in the proposal the specific measures that will be taken to meet this requirement. SBA reserves the right to inspect the contractor’s security measures, data handling procedures, and other security safeguards to determine the security posture of the contractor facility.

b. Protection of Sensitive SBA Data: Physical access to the contractor’s office areas that contain sensitive SBA data must be controlled to prevent unauthorized personnel from acquiring access to this data. Contractors who are authorized to access the SBA Network Security System must ensure that telephone numbers of the SBA AIS, logon passwords, identifiers, and access procedures are safeguarded from unauthorized use and disclosure. Contractor personnel must comply as follows:

   1) The Computer Access/Clearance Form must be read and signed.

   2) Passwords must be changed every 90 days.

3) The Contracting Officer's Technical Representative (COTR) must be promptly notified when a contractor is no longer authorized access to the SBA computer system.

4) The contractor must not release SBA data outside of its facility, either orally or in written form, without the express written consent of SBA. The contractor must refer to SBA for action, all requests it receives for SBA data.

5) When the contract specifies the handling of sensitive data, the contractor must agree to permit an inspection by authorized SBA personnel during the performance of the contract to ensure the continued effectiveness and efficiency of safeguards and the discovery and countering of new threats and hazards. Authorized SBA personnel include the Director, Information Security, the COTR, the OIG, and other personnel designated by the CIO.

6) Weaknesses in physical, personnel, or computer security noted by SBA during routine inspections must be corrected as quickly as possible. Quarterly updates of the status of the corrective actions must be in writing and forwarded through the COTR to the appropriate SBA official.

c. Contractor Background Investigations. The following guidelines apply to contractor background investigations:

1) OMB Circular A-130 requires that as a condition for access to Government AIS (including data); SBA must screen contractor personnel commensurate with the level of risk presented by their access to sensitive SBA AIS. All SBA AIS and data are considered sensitive. SBA policy is to perform background investigations on all such personnel.

2) An SBA official or designated representative will perform background investigations.

3) The Director, Information Security will assign each contract labor category a security sensitivity rating which will determine the type of background investigation performed for the labor category position(s).

4) The OIG and the Director, Information Security, will review investigation results. The COTR will notify the contractor of the results of the investigation.

5) The COTR must immediately notify the OIG, or the Director, Information Security, when contract personnel are hired, identifying the contractor's name, labor category, and date of entry on duty. The OIG or the Director, Information Security will provide appropriate forms and instructions to the COTR for transmission to the contractor personnel. Completed forms must be returned directly to the issuing official within two weeks from date of issuance.

12. What is a System Interconnection, System Interconnection Agreement (SIA) and Memorandum of Understanding (MOU) for System Interconnection; and Who is Responsible for Developing the SIA and MOU?

a. A system interconnection is defined as the direct connection of two or more AIS for the purpose of sharing data and other information resources. Significant benefits that can be realized through a system interconnection include: reduced operating costs, greater functionality, improved efficiency, and centralized access to data. OMB Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their AIS to other systems, based on acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection and such rules of behavior and controls should be included in the organization's system security plan.

b. The SIA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. It also supports the MOU between the organizations. Specifically, the SIA documents the requirements for connecting the AIS, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line.

c. The MOU documents the terms and conditions for sharing data and information resources in a secure manner. Specifically, the MOU defines the purpose of the interconnection; defines relevant authorities; specifies the responsibilities of both organizations; and defines the terms of agreement, including apportionment of costs and timeline for terminating or reauthorizing the interconnection. The MOU should not include technical details on how the interconnection is established or maintained; that is the function of the SIA.

d. All system owners are responsible for developing the MOU and SIA. NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, contains instructions for developing the MOU and SIA.

e. The OCIO, Director of Information Security and the Office of General Counsel must approve all interconnection agreements before connections are made with other entities. Interconnection agreements are required, and OCIO must approve such agreements, for any interconnections between an internal SBA AIS that OCIO does not manage and one that OCIO does manage. The system owner must maintain the official Agency copy of all interconnection agreements for its own AIS, once such agreements are approved and signed.

APPENDIX I – Abbreviations

ADP	Automated Data Processing
AIS	Automated Information System
BRP	Business Resumption Plan
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
COTR	Contracting Officer's Technical Representative
CSAT	Computer Security Awareness Training
CTS	Communications and Technology Services
DIRM	District Information Resources Manager
DNS	Domain Name Service
DSO	District Security Officer
ESC	Eagan Service Center
FMFIA	Federal Managers Financial Integrity Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GAO	Government Accountability Office
GSS	General Support System
HQ	Headquarters
IP	Internet Protocol
IRM	Information Resources Manager
IT	Information Technology
JASS	Jump Start Architecture and Security Scripts
LAN	Local Area Network
MA	Major Application
NG	Next Generation
NIB	Network Integration Branch
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PA	Privacy Act
PC	Personal Computer
PES	Productivity Enhancement Staff
SBA	Small Business Administration
SBU	Sensitive But Unclassified
SDLC	System Development Life Cycle
SDM	System Development Methodology
SIA	System Interconnection Agreement
SIMAN	Site Management Complex
SPI	Stateful Packet Inspection
SSH	Secure Shell
UPS	Uninterruptible Power Source

VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX II – Password Management Guidance

The following instructions are provided to clarify password compliance requirements so that your access rights are not interrupted:

1. These password management standards are *mandatory* and apply to all individuals, organizations, and entities that process, store, or transmit any SBA information.
2. Password management standards apply to all users of SBA's LAN/WAN, laptop, desktop personal computers, and stand-alone workstations (i.e., those SBA systems that are not connected to SBA's Network).
3. All user passwords *must be complex and in compliance with SBA's password policy.* A complex password must be a minimum of 8 characters long and contain at least three of the following four properties:

    - Upper Case Letters A, B, C, … Z
    - Lower Case Letters a, b, c, ... z
    - Numerals 0, 1, 2, … 9
    - Special Characters { } [ ] < >;: ' " ? / | \ ` ~ ! @ # $ % ^ & * [ ] _ - + =.

4. One possible method of creating a good password is to create a *passphrase* that is made up of parts of multiple words that one can easily remember but would be hard for someone else to guess. (For example, the phrase "four score and seven years" could be transformed into the password "4s&7ye@rs"-- a password that would be acceptable in our current network environment.)
5. The security software has a lockout feature that SBA has set to 3 unsuccessful attempts for online and for standalone systems. An authorized administrator must remove the lockout condition from the person's account and provide the user a new unique password.
6. Local system administrators/security administrators that have direct contact with system users. Must create and distribute initial passwords.
7. SBA Network users who have reason to believe that their password has been compromised should immediately contact SBA's Help Desk and the Agency Computer Security Program Manager.
8. System Administrators should avoid using easy-to-guess sequential patterns of characters when more than one system is involved. (For example, administrators should *never* use such predictable passwords as ORACLE1, ORACLE2, ORACLE3, etc. for different servers.)
9. Passwords for networks, systems, or application accounts must be set to expire in 90 days.
10. Users must not share their passwords with anyone and should beware of illicit methods to obtain password information. For example, social engineering is a common means of illicitly obtaining a password via the manipulation of people. In the most common form of social engineering attack, the attacker telephones a help desk, pretends to be an authorized system user, and requests a new password.

11. Passwords must not be written down or left adjacent to the computer and on computer printout.
12. Password life should *never* exceed ninety (90) days, and should be far less for Administrator accounts.

Please contact SBA's Help Desk at (202) 205-6400 for assistance on changing your password.

APPENDIX III – List of Major Applications and General Support Systems

General Support Systems	Program Office
Eagan Mainframe	OCIO
Internet Connectivity Infrastructure	OCIO
National Finance Center (NFC)	OCFO
SBA Local Area Network & Wide Area Network (LAN/WAN)	OCIO
Sysbase Database Servers	OCIO

Major Applications	
7(a) and 503/504 Loan Program Service Agent (Colson)	OFA
Asset Sales Tracking System	CA, OCFO
Automated Loan Control System	ODA
Cash Reconciliation system	OCFO
Credit Bureau Reporting	OFA
Delinquent Loan Collection System	OFA
Electronic Loan Origination System	OFA
Field Cashiering System	OCFO
Financial Reporting Information System	OCFO
Financial Institution Record System	OCFO
Fresno Action Track	OFA
General Ledger Only	OCFO
Guaranty Loan Reporting	OCFO
Hazard Low Doc Credit Desk	OFA
HUBZone Application System	OED
IRS 1099C Reporting	OFA
Joint Accounting & Administration Mgt System	OCFO
Litigation & Liquidation Tracking System	OFA
Loan Accounting Daily Update Cycle	OCFO
Microloan Data Entry System	OFA
OFS Disbursement	OCFO
OFS Infrastructure	OCFO
OFA LA Accounting	OCFO
OFS Print 1201	OCFO
Partner Identification Management System	OFA
PMT-Treasury Offset	OCFO
Pre-Authorized Debit System	OCFO
Preferred Lender Program	OFA
Procurement Marketing & Access Network	OGC/BD
Sacramento Low Doc	OSG
Surety Bond / Preferred Surety Bond Guarantee	OGC/BD
Technical Resource Network	OBI

APPENDIX IV – Waiver Procedures for IT Mobile Devices

The Office of the Chief Information Officer has developed a temporary waiver form to be used to obtain a waiver of the provision outlined in Procedural Notice 9000-1382, Information Technology (IT) Mobile Devices.

1. If your IT Mobile Device (i.e., Laptop Computer, Personal Digital Assistant (PDA), Smart Phone, or other handheld computing device) **is owned by SBA you do not need to submit a waiver request.** If your IT Mobile Device **is not owned by SBA** you must submit the temporary waiver request and abide by the following guidelines;

    a. Your Office IRM Official must test and validate that the security requirements stated below are in place for the non-SBA equipment to be approved by IT Security.

    b. The employee must then submit the request to their management asking for approval to use non-agency issued equipment.

    c. The requestor's manager must:

        1) Review and approved by signing the waiver request to use non-SBA equipment

        2) Send the assigned request to IT Security for coordination and mutual approval with the office of Telecommunication Technology Services

    d. Security requirements:

        1) Devices must be password protected

        2) Wireless modems or LAN cards are not permitted

        3) Storage of SBA data is not permitted

        4) Personal firewalls are not permitted

        5) SSBA LAN/WAN or desktop computer connections are not permitted

Submit your request to the IT Security e-mail box.

APPENDIX V – Guidance on Back-up and Recovery of SBA AIS

1. To prevent loss of data from catastrophic events such as sustained power loss, fires or floods, it is vital that AIS and data be backed on a routine basis. Issues that must be addressed in order to sustain a successful data and system backup and recovery program at the Agency include:

a. **Backups** – Frequency of backups will depend upon how often data changes and how important those changes are. Critical data must be backed up daily. Offices need to document and enforce procedures on backing up and protecting IT resources.

b. **Labels** – Backup and recovery media should be labeled for a variety of purposes, including controlling access, specifying protective measures, or indicating additional handling instructions. Labeling backup media also helps to prevent them from being accidentally overwritten.

c. **Storage** - Backups should be stored securely. While stored on site, the media must be stored in fire-resistant containers. Backed up data should be moved to an off-site location at least weekly.

d. **Annual Testing** - Backup copies should be tested to ensure they are usable. A test plan should be developed and executed at least annually to ensure that recovery is achievable. Based on the test results, the plan should be modified accordingly.

e. **System Configuration** - System recovery is faster if hardware, software, and peripherals are standardized throughout an office. Although this may not always be achievable, compatibility contributes to ease of recovery.

f. **Interoperability** - To facilitate recovery, backup devices must be compatible with operating systems and applications used in backup and recovery operations.

g. **Selection of Backup Media** - Common media that can be used for backups include diskettes, tape cartridges, removable media (zip drives), compact disks, network storage devices such as networked disks, or server backups. Confidentiality procedures must be addressed prior to invoking any of these methods. In addition, it is important to ensure that the necessary hardware remains available to read backups or convert them to newer media if necessary.

2. There are a number of different types of system backups that can be employed:

a. **Full Backup** - Stores all files selected for backup.

b. **Incremental Backup** - Captures only files created or modified since the last backup.

c. **Differential Backup** - Stores files that were created or modified since the last full backup.

d. **Disk Replication Backup** - With disk replication, data is written to two different disks (a protected server and a replicating server) so that two valid copies of the data are always available.

3. To reduce the probability of a single catastrophic event such as fire or flood destroying both the operational data files and their backup, it is vital that backups be maintained at an off-site location. Selection of an off-site location should be based on completion of a formal risk assessment.

4. A number of off-site alternatives may be considered for backup and recovery capability, including: a dedicated site owned and operated by the Agency; a reciprocal site with an internal or external entity where a formal agreement has been negotiated; or a commercially leased facility. Iron Mountain, as an example, is the SBA's current off-site storage solution.

5. Regardless of which type of off-site alternate site is used, there are six possible scenarios that apply for backup and recovery capability:

a. **Cold Site** - The facility has the necessary space and infrastructure support (electric power, telecommunications support, and environmental controls), but does not contain IT equipment.

b. **Warm Site** -The facility is partially equipped with some of the necessary IT equipment. It is maintained in an operational status ready to receive the relocated system.

c. **Hot Site** - The facility is equipped with all the necessary infrastructure and IT equipment to be immediately and fully functional. A hot site is typically staffed 24 hours a day, 7 days a week.

d. **Mobile Site** - A self-contained transportable unit that is custom-fitted with specific telecommunications and IT equipment necessary to meet defined requirements.

e. **Mirrored Site** - A fully redundant facility that has real-time information mirroring and is identical in all technical aspects to the primary site.

f. **Iron Mountain Data Services** - SBA has a contract with Iron Mountain Data Services to provide real-time online backup and recovery services for LAN/WAN, using Live Vault. Live Vault is an online backup and recovery service that is operational and monitored 24 hours a day to ensure that the data is available when needed. In the event of a catastrophic error, Live Vault provides recovery services via online tape and snap server.

Regular backups by System Administrators, associated backup documentation, and the process for securing administrative passwords should be established to provide a basic level of recovery capability in addition to incorporating any of the additional techniques emphasized above.