

FSA BASELINE SECURITY REQUIREMENTS

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
MANAGEMENT CONTROLS					
Administration and Management Security					
Assignment of Responsibilities					
1.	Assign responsibility for security in writing to an individual trained in the technology used in the system and in providing security for such technology (OMB Circular A-130, Appendix III, Section B-a.1, b.1)	X			Robert Ingwalson is the Chief Information Security Officer for FSA.
2.	Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology (OMB Circular A-130, Appendix III, Section A-3, a.1)	X			Denise Leifeste, CDDTS manager, is responsible for overall CDDTS security. David Yang is System Security officer. The ACS contractor responsible for security of CDDTS is Raj Raghu.
3.	Clear lines of authority and responsibility will be established within the Department for the allocation of resources in securing critical infrastructure assets. (<i>Presidential Decision Directive-PDD 63</i>)	X			FSA has defined lines of security responsibility defined in the FSA Information Technology Security and Privacy Policy.
System/Application Security Plan					
4.	Require and develop system security plan for all Federal computer systems that contain sensitive information; update and review the System Security Plan every three years (OMB Circular A-130 Appendix III, Section A-3, a.2, b.2, Section B-a.2, b.2; Computer Security Act of 1987, Section 6.b)	X			
5.	The security plan is implemented and adequately secures the system or application (OMB Circular A-130 Appendix III, Section A-3, a.2, b.2; A-130, 8a.2.c. (iv))			X	All major elements of the controls defined in the CDDTS System Security Plan have been implemented. However, the plan does not include a copy of the Rules of Behavior for CDDTS, or the Memorandum of Understanding. Also, some findings noted in the attached assessment indicate additional security controls that should be considered to secure the system.

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
Rules of Behavior					
6.	Establish rules of behavior for system and application use. The rules should clearly delineate responsibilities of and expectations for all individuals with access to the system (OMB Circular A-130 Appendix III, Section A-3, a.2.a, b.2.a, Section B-a.2.a, b.2.a)			X	Users sign this agreement, but it should also appear as part of the system security plan.
Training					
7.	Provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency (OMB Circular A-130 Appendix III, Section A-3, a.2.b, b.2.b, Section B-a.2.b, b.2.b; Computer Security Act of 1987, Section 5.a)			X	A security training and awareness program was being developed at the time this assessment was conducted. The program is planned for deployment in the near future.
8.	OPM regulation requires training for new employees within 60 days of hire. (<i>Practices for Securing Critical Information Assets</i> , p.6)			X	CDDTS security policy and procedures are addressed briefly during ACS new employee orientation. The security topics that are addressed should be documented to help demonstrate that security issues relevant for new users are covered adequately.
9.	Provide specialized training for all individuals given access to the system/application (OMB Circular A-130 Appendix III, Section A-3, b.2.b, Section B, b.2.b)		X		No formal security training specific to CDDTS security issues is provided for new CDDTS users.
10.	The Office of the CIO and CIAO shall develop and promulgate training standards to ensure that personnel staffed in key positions within the Department's critical infrastructure are proficient in their jobs. (<i>Presidential Decision Directive-PDD 63</i>)	X			
11.	Computer security training should be implemented into existing training programs such as orientation programs for new employees, and training courses involved with information technology systems equipment and software packages (FIPS PUB 191, Appendix A GP9)			X	See #8.

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
12.	Training shall be provided to all users on the security features of the office automation software resident on their respective systems. They also need to understand the security features of the local area network (LAN) to which they are connected, as well as security issues related to the Internet, intranet, and/or extranet. (<i>Practices for Securing Critical Information Assets</i> , p.6)			X	Not assessed directly; see #8.
13.	OPM regulation requires training when an employee enters a new position that deals with sensitive information. (<i>Practices for Securing Critical Information Assets</i> , p.6)			X	See #8.
14.	OPM regulation requires refresher courses based on the sensitivity of the information the employee handles. (<i>Practices for Securing Critical Information Assets</i> , p.6)			X	See #7.
Personnel Security					
15.	Controls include individual accountability, least privilege, and separation of duties enforced by access controls (OMB Circular A-130 Appendix III, Section A-3, a.2.c, b.2.c, Section B-a.2.c, b.2.c)	X			
16.	Segregation of duties within the IT function should include the following: separation between operations and programming, an independent control group, implementation of a librarian function, rotation of operators, closed-shop operations, and required vacations for all employees (OMB Circular A-130, <i>Practices for Securing Critical Information Assets</i> , p.18).	X			
17.	Require personnel controls to screen individuals prior to being authorized for system access and periodic screening thereafter (OMB Circular A-130 Appendix III, Section A-3, a.2.c, b.2.c)	X			CDDTS users must have a 5c clearance. CDDTS managers must have a 6c clearance.
Incident Response Capability					
18.	Establish an incident response capability to provide help to users when a security incident occurs (OMB Circular A-130 Appendix III, Section A-3, a.2.d Section B-a.2.d, <i>Practices for Securing Critical Information Assets</i> , p.47, <i>Presidential Decision Directive-PDD 63</i>)	X			Provided now by the ACS Security Organization. A question to be addressed is who will provide these services if the ACS Security Organization is included in the part of ACS acquired by a third-party (as recently announced).

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
Continuity of Support					
19.	Establish continuity of support to periodically test the capability to provide continual service to users within a system (OMB Circular A-130 Appendix III, Section A-3, a.2.e, Section B-a.2.e)			X	Business continuity plans are in place but have not yet been tested. Testing is scheduled for mid-September.
20.	Areas of control will include continuity of service operations. (<i>Practices for Securing Critical Information Assets</i> , p.18)			X	See #19.
21.	Establish contingency planning to periodically test the capability of the major application to perform and function in event of failure of its automated support (OMB Circular A-130 Appendix III, Section A-3, b.2.d)			X	See #19.
Information Sharing					
22.	Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exist (OMB Circular A-130 A130-8.a.9. (c))	X			
23.	Assure that information which is shared with Federal organizations, state and local governments, and the private sector is appropriately protected comparable to the protection provided when the information is within the application (OMB Circular A-130 Appendix III, Section A-3, b.2.f, Section B-b.2.f)	X			
Public Access Control					
24.	Implement appropriate public access control where application promotes or permits public access. Additional security controls shall be added to protect the integrity of application and the confidence the public has in the application (OMB Circular A-130 Appendix III, Section A-3, b.2.g, Section B-b.2.g)			X	Not applicable; no public access is allowed.
Review of Security Controls					
25.	Perform an independent review or audit of the security controls in each system or application at least every three years (OMB Circular A-130 Appendix III, Section A-3, b.3, Section B-b.3)			X	This review is the first security audit or assessment that has been performed on CDDTS.

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
Risk Assessment					
26.	A risk analysis shall be performed whenever there is a significant change to the installation. A significant modification made to an SBU AIS or network shall require a review to determine the impact on the security of the processed SBU information. (OMB A-130, III-4, 3.c.2.b)		X		There is a detailed configuration management process defined for CDDTS, which includes an Impact Analysis. However, a security risk analysis is not an explicit part of the impact review. (No major changes or upgrades have been made to CDDTS since October 2002, with the Phase III release.)
27.	Vulnerabilities assessments (reviews to identify existing weaknesses but not to determine if all requirements are met) of all assessable units (i.e., computer system or application) shall be performed, at a minimum, every three years. (OMB A-123, 6, 8c)	X			Provided now by the ACS Defense Division. A question to be addressed is who will provide these services if the ACS Defense Division is acquired by a third-party (as recently announced).
28.	A vulnerability audit will be performed to find and document the vulnerabilities in critical information assets. (<i>Practices for Securing Critical Information Assets</i> , p.17)	X			See #27.
29.	Perform risk assessment to include a consideration of major factors in risk management to determine adequate security for the AIS (OMB Circular A-130 Appendix III Section B)	X			See #27.
Authorize Processing					
30.	The system/application must be authorized prior to operation and re-authorized at least every 3 years thereafter (OMB Circular A-130 Appendix III, Section A-3, a.4, b.4, Section B-a.4)	X			CDDTS has been operational for less than three years.
Security Management					
31.	Standards should include minimum expected control guidance including: computer facilities controls; computer operations controls; input/output handling controls; network management controls, and technical support and user liaison policy (NIST: Executive Guide to the Protection of Information Resources)	X			
32.	Based on the results of the vulnerability assessments, remedial action plans will be developed to mitigate the impact of the threats identified. (<i>Presidential Decision Directive-PDD 63</i>)	X			Procedures for upgrades and patches are defined by the Configuration Management procedures.

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
33.	Implement and maintain IT programs to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal AIS (OMB Circular A-130 Appendix III, Section A-3)			X	Other than the issues noted in this assessment, security controls are in place to address security issues defined in the FSA Baseline Security Requirements.
34.	Establish a level of security for all agency information systems that is commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system (OMB Circular A-130, 8.1.g)	X			
Data and File Protection					
35.	Establish procedures to ensure the proper disposal of printed output based on the sensitivity of the data. (GBP)	X			
36.	Establish procedures to ensure compliance with The Privacy Act (OMB Circular A-130, 7.g)	X			
37.	Prohibit smoking and eating in magnetic computer tape storage libraries that contain permanent or unscheduled records (GBP)	X			
38.	The classification of sensitive data that requires protection shall be determined. Appropriate action will be taken to ensure that proper labeling banners are attached on the document (GBP)	X			
Anti-Virus Protection					
39.	LAN servers should be scanned by the area responsible for LAN management to assure no virus becomes resident on the LAN server (FIPS PUB 191, Appendix A, 4.LA4)		X		Anti-virus tools are run on the administrator and developer workstations used for CDDTS, but not the CDDTS server.
Backup of Software and Data					
40.	Backup procedures shall be properly documented; understood by IT personnel; and be integrated/coordinated with the organization's disaster recovery plan (GBP)	X			
41.	Backup procedures shall provide for off-site secured storage (GBP)	X			
42.	Off-site facilities should be sufficiently distant from the operating facility to provide adequate protection against major natural disasters (e.g. earthquakes and hurricanes) (GBP)		X		Offsite storage is in the local area (<300 miles) so major disasters (e.g., hurricanes, terrorist attacks) could affect both the data center and the backup site.
43.	Weekly, monthly and yearly backup of magnetic media is rotated and transported to an off-site storage facility (GBP)	X			

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
44.	External labels for diskettes or removable disks used when processing or temporarily storing permanent or unscheduled records shall include the following information: name of the organizational unit responsible for the records, descriptive title of the contents, dates of creation, data sensitivity, if applicable, and identification of the software and hardware used (<i>GBP</i>)	X			
Configuration Management					
45.	Systems should be thoroughly tested according to accepted standards and moved into a secure production environment through a controlled process (NIST: Executive Guide to the Protection of Information Resources)			X	Functional testing of security features is part of testing procedures. Vulnerability testing, penetration testing, system scanning, and network scanning is not a defined element of the configuration management plan.
46.	Adequate documentation should be considered an integral part of the information system and be completed before the system can be considered ready for use (NIST: Executive Guide to the Protection of Information Resources)	X			
47.	All program changes should be approved before implementation to determine whether they have been authorized, tested, and documented (<i>GBP</i>)	X			
48.	Ensure that there is adequate and effective deployment of hardware or software/firmware changes across multiple sites, (<i>GBP</i>)	X			
49.	Updates and changes in LAN communication hardware and software should be tested thoroughly to prevent unintentional access exposures (<i>GBP</i>)	X			
50.	Data standards are established and promulgated to ensure that consistent data definitions, coding schemes, naming conventions and formats are employed (<i>GBP</i>)	X			
51.	All operating systems and applications are patched with the latest vendor security patches, as applicable. (<i>GBP</i>)	X			
52.	A configuration management process is in place to test and install vendor security patches. (<i>GBP</i>)	X			

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
53.	All applications are tested for input boundary conditions to prevent buffer overflows and other privileged access. (GBP)			X	Details of application security testing were not directly evaluated, but test plans covered functional testing and did not specify security code reviews and testing for issues such as buffer overflows.
54.	Passwords shall be encrypted (GBP)		X		User passwords are stored in an Oracle table in plain text. The Oracle database administrator password is encrypted and stored in an external file.
TECHNICAL CONTROLS					
Communications Security					
Remote Access/ Dial-Up Access					
55.	Appropriate access controls should be in place to support dial-up access to the organization's computer resources. Remote interfaces to the network should provide the same security available when connecting to the network locally (GBP)	X			
56.	Controls should be established to ensure that remote users are positively identified and authenticated before connection to the network is authorized (GBP)	X			
57.	Dial-up authority should only be granted to the organization's personnel having a "need-to-access" the network. (GBP)	X			
58.	Request for dial-up access must be approved by the requester's LAN administrator (GBP)	X			
59.	Procedure should be developed to facilitate the removal of dial-up capabilities when the organization's personnel are no longer authorized to dial-in (GBP)	X			
60.	Dial-up ports should be protected from unauthorized access (GBP)	X			
61.	Do not leave personal computers containing sensitive data which are connected to answering modems unattended (GBP)			X	Scanning for unauthorized modems was not included in this assessment and should be part of periodic vulnerability analyses.
62.	If the auto-answer mode for a system is only used during normal working hours, disable that mode after hours (GBP)	X			
63.	Dial-up to the organization's computer resources must only occur through approved entry points (centrally managed) to ensure integrity of network security (GBP)	X			

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
Firewalls					
64.	Firewalls will be installed to control access to the internal network. (<i>Practices for Securing Critical Information Assets</i> , p.33)	X			Access to Department of Education networks are controlled in the ACS Data Center by firewall and access control lists that allow connections to servers only from authorized IP addresses. This is a recommendation recently implemented after an OIG audit of the DLSS network.
65.	Firewalls will be used for blocking unauthorized incoming traffic (<i>Practices for Securing Critical Information Assets</i> p.34)	X			
66.	Intrusion detection systems (IDS) will be used to: Monitor and analyze user and system activity Assess the integrity of critical system and data files Recognize activity patterns involved in known attacks Perform statistical analyses to spot abnormal activity patterns that may indicate an attack Manage the operating system audit trail and alert system managers to user behavior (<i>Practices for Securing Critical Information Assets</i> , p.36)			X	Intrusion detection system (IDS) sensors are in the process of being deployed but are not yet fully operational. IDS monitoring is provided by the ACS Defense Division. A question to be addressed is who will provide these services if the ACS Defense Division is acquired by a third-party (as recently announced).
67.	Vulnerability scanners will be used to identify weaknesses which could lead to security violations and uncover possible breaches. (<i>Practices for Securing Critical Information Assets</i> , p.33)	X			Provided by the ACS Defense Division. A question to be addressed is who will provide these services if the ACS Defense Division is acquired by a third-party (as recently announced).
Encryption					
68.	Sensitive data files should be protected during transmission from one location to another (<i>GBP</i>)			X	File transfers are via direct connection to DLSS or FTP. FTP controls should be defined to protect transmitted data, or a secure form of file transfer (e.g., a secure FTP product, or encryption of files before transmission) should be used if files are transmitted over public networks.
69.	Encryption should be available for sensitive information transmissions, whenever needed (<i>GBP</i>)	X			External connections to CDDTS are via VPN (encrypted) channels.

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
Interconnection					
70.	Require system interconnection to obtain written management authorization, prior to connecting with other systems (OMB Circular A-130 Appendix III, Section A-3, a.2.g, Section B-a.2.g)	X			
71.	The area responsible for LAN management should secure the LAN environment within the site and interfaces to outside networks (FIPS PUB 191, Appendix A, 3. NM3)	X			
Router					
72.	Screening routers shall have the capability to filter based on TCP and UDP ports as well as IP addresses and incoming network interfaces (<i>GBP</i>)	X			
73.	A screening router shall not be used as the sole segment of a firewall system, rather it should form a portion of the security bastion (<i>GBP</i>)	X			
74.	Inbound filtering will be performed to exclude or reject all data packets that have an internal host address (<i>GBP</i>)			X	Firewall filtering rules and policies were not assessed during this review.
Inventory of Network Hardware and Software					
75.	Accurate records of hardware/software inventory, configurations, and locations should be maintained (NIST: Executive Guide to the Protection of Information Resources)	X			
76.	Develop and maintain a comprehensive inventory of IT equipment, hardware and software configurations, and major information systems/applications, identifying those systems/applications which process sensitive information (<i>GBP</i>)			X	Not included in documentation provided.
77.	An asset inventory shall be conducted to determine what systems, data, and associated assets- facilities, equipment, personnel- constitute the critical information infrastructure. (<i>Practices for Securing Critical Information Assets</i> , p. 10)			X	Not included in documentation provided.

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
Computer Security					
78.	Interrelate technical, operational, and management controls to assure adequate security for all information processed, transmitted, or stored in Federal AIS; (e.g., password protection will only be effective if both a strong technology is employed, and it is managed to assure that it is used correctly) (OMB Circular A-130 Appendix III, Section B)	X			
79.	Establish technical controls to ensure appropriate security controls are specified, designed into, tested and accepted in the application in accordance with NIST guidance (OMB Circular A-130 Appendix III, Section A-3, b.2.e)			X	Penetration testing and application vulnerability scanning are not included in the test plan defined by the Configuration Management procedures. (Also, see #45.)
80.	The area responsible for LAN management (or designated personnel) should rigorously apply available security mechanisms to enforce local security policies (FIPS PUB 191, Appendix A, 3.NM1)	X			
Identification and Authentication					
81.	If automatic-login scripts for LAN or server access are utilized, the script cannot contain the password (<i>GBP</i>)	X			
82.	Users should be able to initiate a change of their password independently (<i>GBP</i>)	X			
83.	The system shall support a lock-out threshold if excessive invalid access attempts are input (<i>GBP</i>)		X		This security function is not described in the system security plan.
84.	User IDs must be revoked if a password attempt threshold of three failed login attempts is exceeded (<i>GBP</i>)		X		This security function is not described in the system security plan.
85.	All passwords that are included in a new system when it is delivered transferred or installed shall be immediately changed (FIPS 112, 3.4.2)	X			
86.	Passwords must be stored with one-way encryption (<i>GBP</i>)		X		User passwords are stored in an Oracle table in plain text. (Also, see #54.)
87.	No one but the user ID owner can have the ability to know or view passwords (<i>GBP</i>)		X		User passwords are stored in an Oracle table in plain text, so they are available for viewing by database administrators. This situation affects accountability for system users.
88.	Users must be authenticated to the LAN before accessing LAN resources (FIPS PUB 191, Appendix A, GP6)	X			

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
89.	LAN user IDs should not be permitted to initiate multiple concurrent logins to the LAN network (<i>GBP</i>)	X			
90.	Terminals, workstations, and networked personal computers should never be left unattended when user ID and password have been logged in (<i>GBP</i>)			X	If not already included, this policy should be communicated during security awareness training and during new employee and new user orientation.
Access Control					
91.	Access control software and/or network operating system security should be kept current and controls limiting user access to sensitive data, applications, and programs should be in place (<i>GBP</i>)	X			
92.	Access controls should encompass systems and programs that edit, update, and store information. Controls should permit access only when specific authorization has been granted (<i>GBP</i>)	X			
93.	Users must be restricted to only those resources required for the efficient completion of their job responsibilities (<i>GBP</i>)	X			
94.	Where appropriate, terminals/ workstations should automatically log out if inactive for a specified period of time (<i>GBP</i>)		X		This function is not defined in the system security plan.
System Audit					
95.	The system shall be able to create, maintain, and protect from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects (<i>GBP</i>)		X		User activity is not logged, although logs are maintained for IDS data and operating system-level security events.
96.	For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and the success or failure of the event (<i>GBP</i>)		X		See #95.
97.	The area responsible for LAN management should conduct timely audits of LAN server logs (FIPS PUB 191, Appendix A, 3. NM6)		X		Routine periodic reviews of event and security logs are not performed. Logs are reviewed when security incidents or other operational issues need to be investigated.
98.	Unauthorized attempts to change, circumvent, or otherwise violate security features shall be detectable and reported within a known time by the system (<i>GBP</i>)	X			Audit logs are not archived off the server, and they are protected by the operating system security controls for log files.
99.	The security administrator will review reports to determine if there have been repeated unsuccessful attempts to login to the network (<i>GBP</i>)		X		This logging capability is not defined in the System Security Plan. (Also see #83 and #84.)

No.	Security Requirement	Compliance			Comments
		Yes	No	Other or N/A	
Object Reuse					
100.	When a storage object (e.g., core area, disk file, etc.) is initially assigned, allocated, or reallocated to a system user, the system shall assure that it has been cleared (GBP)	X			
OPERATIONAL CONTROLS					
Physical Security					
101.	Employee access to the data site shall be controlled by an electronic access system (GBP)	X			
102.	Logs shall be required for recording all physical access to the facility by unauthorized individuals (GBP)	X			
103.	Escorts shall be provided for unauthorized individuals at all times. Escorts will have authorization for access to all areas of the facility (GBP)	X			
104.	The distribution of keys should be strictly limited and an effective control system established (GBP)	X			
105.	Tapes, disks, and other storage media shall be kept in a secure access controlled environment when not being utilized by computer operations (GBP)	X			
106.	Secure methods are employed to safeguard PCs and related hardware that contain information during relocation (GBP)	X			
107.	File servers shall be located in areas where access is restricted (GBP)	X			
108.	The list of persons with authorized access <i>should be reviewed and recertified annually</i> (GBP)		X		This procedure is not defined in the System Security Plan.
Environmental Security					
109.	The primary and backup processing sites as well as the tape storage areas shall be equipped with fire detection and suppression systems that detect and suppress fire in the incipient stage (GBP)	X			