



Department of Education 2002 GISRA Reporting Requirements Survey

Please Complete all information on Tabs 2 & 3

General Information				Point(s) of Contact:				
System #	Date	Principal Office	Automated Information Resource Name/ System Name	Computer Security Officer	Automated Information Resource Owner(s) Name	Phone #:	Automated Information Resource Manager(s): Name	Phone#:
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

**AFTER COMPLETING THE INFORMATION ABOVE PROCEED TO
TAB 2 >>**



Department of Education GISRA Reporting Requirements Survey Questions

Please provide the appropriate response and detail for all questions.

Ques #	CATEGORY & QUESTION	YEAR		REFERENCE	COMMENTS
		2002	2001		
SYSTEM PATCH PROCESS					
					<u>Note: Text will wrap</u>
1	Are you notified of necessary hardware and software patches?			Yes/No/Don't Know	
1a	If yes, how are you notified of necessary hardware and software patches?		N/A	Text	
2	Do you have a process for applying hardware and software patches?			Yes/No/Don't Know	
2a	If yes, describe your process for applying hardware and software patches.		N/A	Text	
3	Do you document software and hardware patch installations?			Yes/No/Don't Know	
3a	If no, please describe any tracking method used for patch installations			Text	
4	Do you know the average length of time from patch release to installation?			Yes/No/Don't Know	
4a	If yes, what is the average length of time from patch release to installation?			Numeric	
5	Do you know what percentage of patches are tested before installation?			Yes/No/Don't Know	
5a	If yes, what percentage of patches are tested before installation?			Numeric	
6	Do you have a process to ensure patches are installed in a timely manner?			Yes/No/Don't Know	
6a	If yes, describe the process used to determine patches are installed in a timely manner			Text	
INCIDENT RESPONSE					
7	Do you have a method of receiving information about potential incidents on your system?			Yes/No/Don't Know	
7a	If yes, how do you become aware of potential incidents?			Text	
8	Is there a method for responding and correcting incidents?			Yes/No/Don't Know	
8a	If yes, describe your incident response and correction process			Text	
9	Do you know the total number of system incidents (any adverse event affecting a Department IT system) that have occurred?			Yes/No/Don't Know	
9a	If yes, what are the total number of incidents?			Numeric	
9b	Number of successful network penetrations			Numeric	
9c	Number of unsuccessful network penetrations			Numeric	
9d	Number of root or user account compromises			Numeric	
9e	Number of denial of service attacks			Numeric	
9f	Number of website defacing attacks			Numeric	
9g	Number of malicious code and virus attacks			Numeric	
9h	Number of probes and scans			Numeric	
9i	Number of password access incidents			Numeric	
9j	Number of incidents reported to CIO			Numeric	
9k	Number of incidents reported to FedCIRC or another authority			Numeric	
9l	What is the average time to report an incident to the OCIO?			Numeric	
9m	What is the average time to report an incident to the FedCIRC?			Numeric	
10	Do you know the number of incidents resolved for your system?			Yes/No/Don't Know	
10a	If yes, what were the number of incidents resolved?			Numeric	
TRAINING					
11	Do you know the clearances held by personnel accessing the system?			Yes/No/Don't Know	
11a	If yes, Number of personnel with significant security responsibilities (hold a 6C clearance) accessing the system			Numeric	
12	Number of personnel with significant security responsibilities (hold a 6C clearance) accessing the system that have had specialized security training?			Numeric	
13	List all sources that personnel have used to receive specialized security training			Text	
LOCATIONS AND REVIEW STATUS					
14	Does your system lie outside the EDNet boundary?			Yes/No	
15	Does the system have virus protection?			Yes/No	
16	Are virus updates loaded automatically?			Yes/No	
17	Is the system housed at a contractor site?			Yes/No	
18	If yes, was an independent review performed of the contractor site in the last 12 months to ensure adequate security controls are in place?			Yes/No/Don't know	
19	Number of contractor personnel with access to the system			Numeric	

**AFTER COMPLETING THE INFORMATION
ABOVE PROCEED TO TAB 3 >>**



Department of Education

NIST SELF-ASSESSMENT SUBMISSION FORM

PLEASE NOTE: Use one template per system or resource. Answers for each question are only required in columns F through M. Enter a 'Y' in columns F through K for all that apply, comments can entered in column L for each question, and initials in column M. All questions are grouped by category and in some cases further grouped by subcategory1 & subcategory2. Click the plus signs in the far left column to expand the categories. When a minus sign is displayed, there are no further subcategories beneath.

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.					NOTE: Text will wrap within field		
MGT CONTROLS										
Risk Mgt										
1	Yes	Is risk periodically assessed?	Y	Y						
2		1.1.1 Is the current system configuration documented, including links to other systems? NIST SP 800-18	Y	Y					FSA Policy Sect 2.3	
3		1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? FISCAM SP-1	Y	Y					FSA Policy Sect 2.1	
4		1.1.3 Has data sensitivity and integrity of the data been considered? FISCAM SP-1	Y	Y					FSA Policy Sect 2.1	
5		1.1.4 Have threat sources, both natural and manmade, been identified? FISCAM SP-1	Y	Y					FSA Policy Sect 2.1	
6		1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? NIST SP 800-30[1]	Y	Y					FSA Policy Sect 2.1	
7		1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities?	Y	Y					FSA Policy Sect 2.1	
8	Yes	Do program officials understand the risk to systems under their control and determine the acceptable level of risk?	Y	Y						
9		1.2.1 Are final risk determinations and related management approvals documented and maintained on file? FISCAM SP-1	Y	Y					FSA Policy Sect 2.1	
10		1.2.2 Has a mission/business impact analysis been conducted? NIST SP 800-30	Y						FSA Policy Sect 2.1	
11		1.2.3 Have additional controls been identified to sufficiently mitigate identified risks? NIST SP 800-30	Y	Y					FSA Policy Sect 2.1	
Security Control Review										
12	Yes	Have the security controls of the system and interconnected systems been reviewed?	Y	Y						
13		2.1.1 Has the system and all network boundaries been subjected to periodic reviews? FISCAM SP-5.1	Y						FSA Policy Sect 2.2	
14		2.1.2 Has an independent review been performed when a significant change occurred? OMB Circular A-130, III FISCAM SP-5.1, NIST SP 800-18	Y	Y					FSA Policy Sect 2.2	
15		2.1.3 Are routine self-assessments conducted ? NIST SP 800-18	Y	Y					FSA Policy Sect 2.2	
16		2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? OMB Circular A-130, 8B3, NIST SP 800-18	Y	Y					FSA Policy Sect 2.2	
17		2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? FISCAM SP 3-4, NIST SP 800-18	Y	Y					FSA Policy Sect 3.8	
18	Yes	Does management ensure that corrective actions are effectively implemented?	Y	Y						

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.					NOTE: Text will wrap within field		
19		2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action? FISCAM SP 5-1 and 5.2, NIST SP 800-18	Y	Y					FSA Policy Sect 2.2	
Life Cycle										
Initiation										
20	Yes	Has a system development life cycle methodology been developed?								
21		3.1.1 Is the sensitivity of the system determined? OMB Circular A-130, III, FISCAM AC-1.1 & 1.2, NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
22		3.1.2 Does the business case document the resources required for adequately securing the system? Clinger-Cohen	Y	Y					FSA Policy Sect 2.5, SLC	
23		3.1.3 Does the Investment Review Board ensure any investment request includes the security resources needed? Clinger-Cohen	Y	Y					FSA Policy Sect 2.5, SLC	
24		3.1.4 Are authorizations for software modifications documented and maintained? FISCAM CC -1.2								
25		3.1.5 Does the budget request include the security resources required for the system? GISRA	Y	Y					FSA Policy Sect 2.5, SLC	
Development										
26		3.1.6 During the system design, are security requirements identified? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
27		3.1.7 Was an initial risk assessment performed to determine security requirements? NIST SP 800-30	Y	Y					FSA Policy Sect 2.5, SLC	
28		3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
29		3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency? OMB Circular A-130, 8B3								
30		3.1.10 Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
31		3.1.11 Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
32		3.1.12 Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
Implementation										
33	Yes	Are changes controlled as programs progress through testing to final approval?	Y							
34		3.2.1 Are design reviews and system tests run prior to placing the system in production? FISCAM CC-2.1, NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
35		3.2.2 Are the test results documented? FISCAM CC-2.1, NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
36		3.2.3 Is certification testing of security controls conducted and documented? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
37		3.2.4 If security controls were added since development, has the system documentation been modified to include them? NIST SP 800-18	Y						FSA Policy Sect 3.7.1.1	
38		3.2.5 If security controls were added since development, have the security controls been tested and the system recertified? FISCAM CC-2.1, NIST SP 800-18	Y						FSA Policy Sect 2.5, SLC	
39		3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
40		3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
Operation										
41		3.2.8 Has a system security plan been developed and approved? OMB Circular A-130, III, FISCAM SP 2-1, NIST SP 800-18	Y	Y					FSA Policy Sect 2.3	
42		3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? NIST SP 800-18	Y	Y					FSA Policy Sect 2.8	
43		3.2.10 Is the system security plan kept current? OMB Circular A-130, III, FISCAM SP 2-1, NIST SP 800-18	Y	Y					FSA Policy Sect 2.3	
Disposal										

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.						NOTE: Text will wrap within field	
44		3.2.11 Are official electronic records properly disposed/archived? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
45		3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? FISCAM AC-3.4, NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
46		3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized? NIST SP 800-18	Y	Y					FSA Policy Sect 2.5, SLC	
Authorize Processing										
47	Yes	Has the system been certified/recertified and authorized to process (accredited)?	Y	Y					FSA Policy Sect 2.6	
48		4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred? NIST SP 800-18		Y						
49		4.1.2 Has a risk assessment been conducted when a significant change occurred? NIST SP 800-18	Y	Y					FSA Policy Sect 2.1	
50		4.1.3 Have Rules of Behavior been established and signed by users? NIST SP 800-18	Y	Y					FSA Policy Sect 2.4	
51		4.1.4 Has a contingency plan been developed and tested? NIST SP 800-18	Y	Y					FSA Policy Sect 3.4	
52		4.1.5 Has a system security plan been developed, updated, and reviewed? NIST SP 800-18	Y	Y					FSA Policy Sect 2.3	
53		4.1.6 Are in-place controls operating as intended? NIST SP 800-18		Y						
54		4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity? NIST SP 800-18		Y						
55		4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? NIST SP 800-18	Y	Y					FSA Policy Sect 2.8	
56	Yes	Is the system operating on an interim authority to process in accordance with specified agency procedures?	Y	Y						
57		4.2.1 Has management initiated prompt action to correct deficiencies? NIST SP 800-18	Y	Y					FSA Policy Sect 2.6	
System Security Plan										
58	Yes	Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?	Y	Y						
59		5.1.1 Is the system security plan approved by key affected parties and management? FISCAM SP-2.1, NIST SP 800-18	Y	Y					FSA Policy Sect 2.3	
60		5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? NIST SP 800-18	Y	Y					FSA Policy Sect 2.3	
61		5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? OMB Circular A-130, III, NIST SP 800-18	Y						FSA Policy Sect 2.3	
62	Yes	Is the plan kept current?	Y	Y						
63		5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks? NIST SP 800-18, FISCAM SP-2.1	Y	Y					FSA Policy Sect 2.3	
OPERATIONAL CONTROLS										
Personnel Security										
64	Yes	Are duties separated to ensure least privilege and individual accountability?	Y	Y						
65		6.1.1 Are all positions reviewed for sensitivity level? FISCAM SD-1.2, NIST SP 800-18	Y						FSA Policy Sect 3.1.3	
66		6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? FISCAM SD-1.2	Y						FSA Policy Sect 3.1.2	
67		6.1.3 Are sensitive functions divided among different individuals? OMB Circular A-130, III, FISCAM SD-1, NIST SP 800-18	Y						FSA Policy Sect 3.1.7	
68		6.1.4 Are distinct systems support functions performed by different individuals? V	Y						FSA Policy Sect 3.1.7	
69		6.1.5 Are mechanisms in place for holding users responsible for their actions? OMB Circular A-130, III, FISCAM SD-2 & 3.2	Y						FSA Policy Sect 2.4	
70		6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required? FISCAM SD-1.1, FISCAM SP-4.1	Y						FSA Policy Sect 3.1.7	
71		6.1.7 Are hiring, transfer, and termination procedures established? FISCAM SP-4.1, NIST SP 800-18	Y						FSA Policy Sect 3.1.1	

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.						NOTE: Text will wrap within field	
72		6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? FISCAM SP-4.1, NIST 800-18	Y						FSA Policy Sect 3.1.1	
73	Yes	Is appropriate background screening for assigned positions completed prior to granting access?	Y							
74		6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? OMB Circular A-130, III, FISCAM SP-4.1	Y						FSA Policy Sect 3.1.4	
75		6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? FISCAM SP-4.1	Y						FSA Policy Sect 3.1.6	
76		6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? OMB Circular A-130, III	Y						FSA Policy Sect 3.1.4	
77		6.2.4 Are there conditions for allowing system access prior to completion of screening? FISCAM AC-2.2, NIST SP 800-18	Y						FSA Policy Sect 3.1.4	
Physical Environment Protection										
Physical Access										
78	Yes	Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?	Y							
79		7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics? FISCAM AC-3, NIST SP 800-18	Y	Y					FSA Policy Sect 3.2.1	
80		7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities? FISCAM AC-3.1	Y						FSA Policy Sect 3.2.1	
81		7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? FISCAM AC-3.1	Y						FSA Policy Sect 3.3	
82		7.1.4 Are keys or other access devices needed to enter the computer room and tape/media library? FISCAM AC-3.1	Y						FSA Policy Sect 3.2.1	
83		7.1.5 Are unused keys or other entry devices secured? FISCAM AC-3.1	Y						FSA Policy Sect 3.2.1	
84		7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc? FISCAM AC-3.1	Y						FSA Policy Sect 3.2.1	
85		7.1.7 Are visitors to sensitive areas signed in and escorted? FISCAM AC-3.1	Y						FSA Policy Sect 3.2.1	
86		7.1.8 Are entry codes changed periodically? FISCAM AC-3.1	Y						FSA Policy Sect 3.2.1	
87		7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? FISCAM AC-4	Y						FSA Policy Sect 3.2.1	
88		7.1.10 Is suspicious access activity investigated and appropriate action taken? FISCAM AC-4.3	Y						FSA Policy Sect 3.2.1	
89		7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? FISCAM AC-3.1	Y						FSA Policy Sect 3.2.1	
Fire Safety										
90		7.1.12 Are appropriate fire suppression and prevention devices installed and working? FISCAM SC-2.2, NIST SP 800-18	Y						FSA Policy Sect 3.2.2	
91		7.1.13 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically? NIST SP 800-18	Y						FSA Policy Sect 3.2.2	
Supporting Utilities										
92		7.1.14 Are heating and air-conditioning systems regularly maintained? NIST SP 800-18	Y						FSA Policy Sect 3.2.2	
93		7.1.15 Is there a redundant air-cooling system? FISCAM SC-2.2	Y						FSA Policy Sect 3.2.2	
94		7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? FISCAM SC-2.2, NIST SP 800-18	Y						FSA Policy Sect 3.2.2	
95		7.1.17 Are building plumbing lines known and do not endanger system? FISCAM SC-2.2, NIST SP 800-18	Y						FSA Policy Sect 3.2.2	
96		7.1.18 Has an uninterruptible power supply or backup generator been provided? FISCAM SC-2.2	Y						FSA Policy Sect 3.2.2	
97		7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.? FISCAM SC-2.2	Y	Y					FSA Policy Sect 3.2.2	
Data Interception										

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.					NOTE: Text will wrap within field		
98	Yes	Is data protected from interception?	Y							
99		7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? NIST SP 800-18	Y						FSA Policy Sect 3.2.1	
100		7.2.2 Is physical access to data transmission lines controlled? NIST SP 800-18	Y						FSA Policy Sect 3.2.1	
Mobile Portable Systems										
101	Yes	Are mobile and portable systems protected?	Y	Y						
102		7.3.1 Are sensitive data files encrypted on all portable systems? NIST SP 800-14	Y						FSA Policy Sect 3.2.1	
103		7.3.2 Are portable systems stored securely? NIST SP 800-14	Y	Y					FSA Policy Sect 3.1.5	
Production Input/Output Controls										
104	Yes	Is there user support?	Y							
105		8.1.1 Is there a help desk or group that offers advice? NIST SP 800-18	Y						FSA Policy Sect 3.3	
106	Yes	Are there media controls?	Y							
107		8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? NIST SP 800-18	Y						FSA Policy Sect 3.3	
108		8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media? NIST SP 800-18	Y						FSA Policy Sect 3.3	
109		8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? NIST SP 800-18	Y						FSA Policy Sect 3.3	
110		8.2.4 Are controls in place for transporting or mailing media or printed output? NIST SP 800-18	Y						FSA Policy Sect 3.3	
111		8.2.5 Is there internal/external labeling for sensitivity? NIST SP 800-18	Y						FSA Policy Sect 3.3	
112		8.2.6 Is there external labeling with special handling instructions? NIST SP 800-18	Y						FSA Policy Sect 3.3	
113		8.2.7 Are audit trails kept for inventory management? NIST SP 800-18	Y						FSA Policy Sect 3.3	
114		8.2.8 Is media sanitized for reuse? FISCAM AC-3.4, NIST SP 800-18	Y	Y					FSA Policy Sect 3.3	
115		8.2.9 Is damaged media stored and/or destroyed? NIST SP 800-18	Y						FSA Policy Sect 3.3	
116		8.2.10 Is hardcopy media shredded or destroyed when no longer needed? NIST SP 800-18	Y	Y					FSA Policy Sect 3.3	
Contingency Planning										
117	Yes	Have the most critical and sensitive operations and their supporting computer resources been identified?	Y							
118		9.1.1 Are critical data files and operations identified and the frequency of file backup documented? FISCAM SC- SC-1.1 & 3.1, NIST SP 800-18	Y						FSA Policy Sect 3.4, 3.4.3	
119		9.1.2 Are resources supporting critical operations identified? FISCAM SC-1.2	Y						FSA Policy Sect 3.4	
120		9.1.3 Have processing priorities been established and approved by management? FISCAM SC-3.1	Y						FSA Policy Sect 3.4	
121	Yes	Has a comprehensive contingency plan been developed and documented?	Y							
122		9.2.1 Is the plan approved by key affected parties? FISCAM SC-3.1	Y						FSA Policy Sect 3.4, 3.4.1	
123		9.2.2 Are responsibilities for recovery assigned? FISCAM SC-3.1	Y						FSA Policy Sect 3.4	
124		9.2.3 Are there detailed instructions for restoring operations? FISCAM SC-3.1	Y						FSA Policy Sect 3.4	
125		9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place? FISCAM SC-3.1, NIST SP 800-18	Y						FSA Policy Sect 3.4.2	
126		9.2.5 Is the location of stored backups identified? NIST SP 800-18	Y						FSA Policy Sect 3.4.3	
127		9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? FISCAM SC-2.1	Y						FSA Policy Sect 3.4.3	
128		9.2.7 Is system and application documentation maintained at the off-site location? FISCAM SC-2.1	Y						FSA Policy Sect 3.4.1	
129		9.2.8 Are all system defaults reset after being restored from a backup? FISCAM SC-3.1	Y						FSA Policy Sect 3.4	
130		9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? FISCAM SC-2.1	Y						FSA Policy Sect 3.4.3	
131		9.2.10 Has the contingency plan been distributed to all appropriate personnel? FISCAM SC-3.1	Y						FSA Policy Sect 3.4.	
132	Yes	Are tested contingency/disaster recovery plans in place?	Y							

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.					NOTE: Text will wrap within field		
133		9.3.1 Is an up-to-date copy of the plan stored securely off-site? FISCAM SC-3.1	Y						FSA Policy Sect 3.4.1	
134		9.3.2 Are employees trained in their roles and responsibilities? FISCAM SC-2.3, NIST SP 800-18	Y						FSA Policy Sect 3.4	
135		9.3.3 Is the plan periodically tested and readjusted as appropriate? FISCAM SC-3.1, NIST SP 800-18	Y						FSA Policy Sect 3.4.1	
Hardware & Software Maintenance										
136	Yes	Is access limited to system software and hardware?								
137		10.1.1 Are restrictions in place on who performs maintenance and repair activities? OMB Circular A-130, III, FISCAM SS-3.1, NIST SP 800-18	Y						FSA Policy Sect 3.7.2	
138		10.1.2 Is access to all program libraries restricted and controlled? FISCAM CC-3.2 & 3.3	Y						FSA Policy Sect 4.2	
139		10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)? NIST SP 800-18	Y						FSA Policy Sect 3.7.2	
140		10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls? FISCAM SS-1.2	Y						FSA Policy Sect 4.2	
141		10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities? FISCAM SS-2.1								
142	Yes	Are all new and revised hardware and software authorized, tested and approved before implementation?	Y							
143		10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control? NIST SP 800-18	Y						FSA Policy Sect 3.7.1.1	
144		10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production? FISCAM SS-3.1, 3.2, & CC-2.1, NIST SP 800-18	Y						FSA Policy Sect 3.7.1.1	
145		10.2.3 Are software change request forms used to document requests and related approvals? FISCAM CC-1.2, NIST SP 800-18	Y						FSA Policy Sect 3.7.1	
146		10.2.4 Are there detailed system specifications prepared and reviewed by management? FISCAM CC-2.1	Y						FSA Policy Sect 3.7.1.1	
147		10.2.5 Is the type of test data to be used specified, i.e., live or made up? NIST SP 800-18	Y						FSA Policy Sect 3.7.1.1	
148		10.2.6 Are default settings of security features set to the most restrictive mode? PSN Security Assessment Guidelines	Y						FSA Policy Sect 3.7.2.1	
149		10.2.7 Are there software distribution implementation orders including effective date provided to all locations? FISCAM CC-2.3	Y						FSA Policy Sect 3.7.1.1	
150		10.2.8 Is there version control? NIST SP 800-18	Y						FSA Policy Sect 3.7.1	
151		10.2.9 Are programs labeled and inventoried? FISCAM CC-3.1	Y						FSA Policy Sect 3.3	
152		10.2.10 Are the distribution and implementation of new or revised software documented and reviewed? FISCAM SS-3.2	Y						FSA Policy Sect 3.7.1.1	
153		10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact? FISCAM CC-2.2	Y						FSA Policy Sect 3.7.1.1	
154		10.2.12 Are contingency plans and other associated documentation updated to reflect system changes? FISCAM SC-2.1, NIST SP 800-18	Y						FSA Policy Sect 3.7.1.1	
155		10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented? NIST SP 800-18	Y						FSA Policy Sect 3.7.2.2	
156	Yes	10.3. Are systems managed to reduce vulnerabilities?	Y	Y						
157		10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)? NIST SP 800-18	Y						FSA Policy Sect 3.7.2.1	
158		10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed? NIST SP 800-18	Y	Y					FSA Policy Sect 3.7.2.1	
Data Integrity										
159	Yes	Is virus detection and elimination software installed and activated?	Y							
160		11.1.1 Are virus signature files routinely updated? NIST SP 800-18	Y						FSA Policy Sect 3.5.1	
161		11.1.2 Are virus scans automatic? NIST SP 800-18	Y						FSA Policy Sect 3.5.1	
162	Yes	Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?	Y							

QUESTION	CRITICAL ELEMENT	POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
		Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.					NOTE: Text will wrap within field		
163		11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? NIST SP 800-18	Y					FSA Policy Sect 3.5.3	
164		11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken? FISCAM SS-2.2	Y	Y				FSA Policy Sect 3.8.2	
165		11.2.3 Are procedures in place to determine compliance with password policies? NIST SP 800-18	Y					FSA Policy Sect 4.1.2	
166		11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? NIST SP 800-18	Y					FSA Policy Sect 3.5.2	
167		11.2.5 Are intrusion detection tools installed on the system? NIST SP 800-18	Y					FSA Policy Sect 3.5.6	
168		11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? NIST SP 800-18	Y					FSA Policy Sect 3.5.6	
169		11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks? NIST SP 800-18	Y					FSA Policy Sect 3.5.5	
170		11.2.8 Is penetration testing performed on the system? NIST SP 800-18	Y					FSA Policy Sect 3.5.7	
171		11.2.9 Is message authentication used? NIST SP 800-18	Y					FSA Policy Sect 3.5.4	
Documentation									
172	Yes	Is there sufficient documentation that explains how software/hardware is to be used?	Y						
173		12.1.1 Is there vendor-supplied documentation of purchased software? NIST SP 800-18	Y					FSA Policy Sect 3.6	
174		12.1.2 Is there vendor-supplied documentation of purchased hardware? NIST SP 800-18	Y					FSA Policy Sect 3.6	
175		12.1.3 Is there application documentation for in-house applications? NIST SP 800-18	Y					FSA Policy Sect 3.6	
176		12.1.4 Are there network diagrams and documentation on setups of routers and switches? NIST SP 800-18	Y					FSA Policy Sect 3.6	
177		12.1.5 Are there software and hardware testing procedures and results? NIST SP 800-18	Y					FSA Policy Sect 3.6	
178		12.1.6 Are there standard operating procedures for all the topic areas covered in this document? NIST SP 800-18	Y					FSA Policy Sect 3.6	
179		12.1.7 Are there user manuals? NIST SP 800-18	Y					FSA Policy Sect 3.6	
180		12.1.8 Are there emergency procedures? NIST SP 800-18	Y					FSA Policy Sect 3.7.1.1	
181		12.1.9 Are there backup procedures? NIST SP 800-18	Y					FSA Policy Sect 3.4.3	
182	Yes	Are there formal security and operational procedures documented?	Y						
183		12.2.1 Is there a system security plan? OMB Circular A-130, III, FISCAM SP-2.1, NIST SP 800-18	Y	Y				FSA Policy Sect 3.6	
184		12.2.2 Is there a contingency plan? NIST SP 800-18	Y	Y				FSA Policy Sect 3.4	
185		12.2.3 Are there written agreements regarding how data is shared between interconnected systems? OMB A-130, III, NIST SP 800-18	Y					FSA Policy Sect 2.8	
186		12.2.4 Are there risk assessment reports? NIST SP 800-18	Y	Y				FSA Policy Sect 2.1	
187		12.2.5 Are there certification and accreditation documents and a statement authorizing the system to process? NIST SP 800-18	Y	Y				FSA Policy Sect 3.6	
Security Awareness Training & Education									
188	Yes	Have employees received adequate training to fulfill their security responsibilities?	Y	Y					
189		13.1.1 Have employees received a copy of the Rules of Behavior? NIST SP 800-18	Y					FSA Policy Sect 2.4	
190		13.1.2 Are employee training and professional development documented and monitored? FISCAM SP-4.2	Y					FSA Policy Sect 2.7	
191		13.1.3 Is there mandatory annual refresher training? OMB Circular A-130, III	Y					FSA Policy Sect 2.7	
192		13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets? NIST SP 800-18	Y					FSA Policy Sect 1.9	
193		13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? NIST SP 800-18	Y					FSA Policy Sect 1.1	
Incident Response									
194	Yes	Is there a capability to provide help to users when a security incident occurs in the system?	Y	Y					
195		14.1.1 Is a formal incident response capability available? FISCAM SP-3.4, NIST SP 800-18	Y					FSA Policy Sect 3.8	

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.					NOTE: Text will wrap within field		
196		14.1.2 Is there a process for reporting incidents? FISCAM SP-3.4, NIST SP 800-18	Y	Y					FSA Policy Sect 3.8	
197		14.1.3 Are incidents monitored and tracked until resolved? NIST SP 800-18	Y						FSA Policy Sect 3.8	
198		14.1.4 Are personnel trained to recognize and handle incidents? FISCAM SP 3.4, NIST SP 800-18	Y						FSA Policy Sect 3.8.2	
199		14.1.5 Are alerts/advisories received and responded to? NIST SP 800-18	Y						FSA Policy Sect 3.8.1	
200		14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs? NIST SP 800-18	Y						FSA Policy Sect 3.8.3	
201	Yes	Is incident related information shared with appropriate organizations?	Y							
202		14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems? OMB A-130, III, NIST SP 800-18	Y						FSA Policy Sect 3.8.1	
203		14.2.2 Is incident information shared with FedCIRC[1] concerning incidents and common vulnerabilities and threats? GISRA, OMB A-130,III	Y						FSA Policy Sect 3.8.2	
204		14.2.3 Is incident information reported to FedCIRC, NIPC[2], and local law enforcement when necessary? GISRA, OMB A-130,III	Y						FSA Policy Sect 3.8.2	
TECHNICAL CONTROLS										
Identification & Authentication										
205	Yes	Are users individually authenticated via passwords, tokens, or other devices?	Y							
206		15.1.1 Is a current list maintained and approved of authorized users and their access? FISCAM AC-2, NIST SP 800-18	Y						FSA Policy Sect 4.2.1	
207		15.1.2 Are digital signatures used and conform to FIPS 186-2? NIST SP 800-18	Y						FSA Policy Sect 4.1.3	
208		15.1.3 Are access scripts with embedded passwords prohibited? NIST SP 800-18	Y						FSA Policy Sect 4.1.2	
209		15.1.4 Is emergency and temporary access authorized? FISCAM AC-2.2	Y						FSA Policy Sect 4.1.2	
210		15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? FISCAM AC-3.2	Y						FSA Policy Sect 4.2.1	
211		15.1.6 Are passwords changed at least every ninety days or earlier if needed? NIST SP 800-18, FISCAM AC-3.2	Y						FSA Policy Sect 4.1.2	
212		15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? NIST SP 800-18, FISCAM AC-3.2	Y						FSA Policy Sect 4.1.2	
213		15.1.8 Are inactive user identifications disabled after a specified period of time? NIST SP 800-18, FISCAM AC-3.2	Y						FSA Policy Sect 4.2	
214		15.1.9 Are passwords not displayed when entered? NIST SP 800-18, FISCAM AC-3.2	Y						FSA Policy Sect 4.1.1	
215		15.1.10 Are there procedures in place for handling lost and compromised passwords? NIST SP 800-18, FISCAM AC-3.2	Y						FSA Policy Sect 4.1.2	
216		15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? NIST SP 800-18	Y						FSA Policy Sect 4.1.2	
217		15.1.12 Are passwords transmitted and stored using secure protocols/algorithms? FISCAM AC-3.2, NIST SP 800-18	Y						FSA Policy Sect 4.1.2	
218		15.1.13 Are vendor-supplied passwords replaced immediately? FISCAM AC-3.2, NIST SP 800-18	Y						FSA Policy Sect 4.1.2	
219		15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user? FISCAM AC-3.2, NIST SP 800-18	Y						FSA Policy Sect 4.2, 4.1	
220	Yes	Are access controls enforcing segregation of duties?	Y							
221		15.2.1 Does the system correlate actions to users? OMB A-130, III, FISCAM SD-2.1	Y						FSA Policy Sect 4.1	
222		15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate? FISCAM AC-2.1	Y						FSA Policy Sect 4.2.1	
Logical Access										
223	Yes	Do the logical access controls restrict users to authorized transactions and functions?	Y							
224		16.1.1 Can the security controls detect unauthorized access attempts? FISCAM AC-3.2, NIST SP 800-18	Y						FSA Policy Sect 4.2	

QUESTION	CRITICAL ELEMENT	POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
		Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.						NOTE: Text will wrap within field	
225		16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion? FISCAM AC-3.2, NIST SP 800-18	Y					FSA Policy Sect 4.2	
226		16.1.3 Is access to security software restricted to security administrators? FISCAM AC-3.2	Y					FSA Policy Sect 4.2	
227		16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity? FISCAM AC-3.2, NIST SP 800-18	N/A					EDnet	
228		16.1.5 Are inactive users' accounts monitored and removed when not needed? FISCAM AC-3.2, NIST SP 800-18	Y					FSA Policy Sect 4.2.1	
229		16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files? FISCAM AC-3.2 NIST SP 800-18	Y					FSA Policy Sect 4.2	
230		16.1.7 If encryption is used, does it meet federal standards? NIST SP 800-18	Y					FSA Policy Sect 4.1.3	
231		16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? NIST SP 800-18	Y					FSA Policy Sect 4.1.3	
232		16.1.9 Is access restricted to files at the logical view or field? FISCAM AC-3.2	Y					FSA Policy Sect 4.2	
233		16.1.10 Is access monitored to identify apparent security violations and are such events investigated? FISCAM AC-4	Y					FSA Policy Sect 4.2, 3.8	
234	Yes	Are there logical controls over network access?	Y						
235		16.2.1 Has communication software been implemented to restrict access through specific terminals? FISCAM AC-3.2	N/A					EDnet	
236		16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled? PSN Security Assessment Guidelines	Y					FSA Policy Sect 4.2	
237		16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings? PSN Security Assessment Guidelines	Y					FSA Policy Sect 4.2	
238		16.2.4 Are there controls that restrict remote access to the system? NIST SP 800-18	Y					FSA Policy Sect 4.2.3	
239		16.2.5 Are network activity logs maintained and reviewed? FISCAM AC-3.2	Y					FSA Policy Sect 4.3	
240		16.2.6 Does the network connection automatically disconnect at the end of a session? FISCAM AC-3.2	Y					FSA Policy Sect 4.2	
241		16.2.7 Are trust relationships among hosts and external entities appropriately restricted? PSN Security Assessment Guidelines	Y					FSA Policy Sect 1.3	
242		16.2.8 Is dial-in access monitored? FISCAM AC-3.2	Y					FSA Policy Sect 4.2.3	
243		16.2.9 Is access to telecommunications hardware or facilities restricted and monitored? FISCAM AC-3.2	Y					FSA Policy Sect 3.2.1	
244		16.2.10 Are firewalls or secure gateways installed? NIST SP 800-18	Y					FSA Policy Sect 4.2	
245		16.2.11 If firewalls are installed do they comply with firewall policy and rules? FISCAM AC-3.2	Y					FSA Policy Sect 4.2	
246		16.2.12 Are guest and anonymous accounts authorized and monitored? PSN Security Assessment Guidelines	N/A						
247		16.2.13 Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished? FISCAM AC-3.2, NIST SP 800-18	Y					FSA Policy Sect 4.1.1	
248		16.2.14 Are sensitive data transmissions encrypted? FISCAM AC-3.2	Y					FSA Policy Sect 4.2	
249		16.2.15 Is access to tables defining network options, resources, and operator profiles restricted? FISCAM AC-3.2	Y					FSA Policy Sect 4.2.1	
250	Yes	If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?	Y					FSA Policy Sect 4.2.2	
251		16.3.1 Is a privacy policy posted on the web site? OMB-99-18	Y					FSA Policy Sect 4.2.2	
Audit Trails									
252	Yes	Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?	Y						
253		17.1.1 Does the audit trail provide a trace of user actions? NIST SP 800-18	Y					FSA Policy Sect 4.3	
254		17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? NIST SP 800-18	Y					FSA Policy Sect 4.3	
255		17.1.3 Is access to online audit logs strictly controlled? NIST SP 800-18	Y					FSA Policy Sect 4.3	

QUESTION	CRITICAL ELEMENT		POLICY	PROCEDURE	IMPLEMENTED	TESTED	INTEGRATED	RISK DECISION	COMMENTS	INITIALS
			Check 'Y' for Yes where controls are in place. If not applicable, place an "N/A" in the field. Leave blank if control is not in place.					NOTE: Text will wrap within field		
256		17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? NIST SP 800-18	Y						FSA Policy Sect 4.3	
257		17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? NIST SP 800-18	Y						FSA Policy Sect 4.3	
258		17.1.6 Are audit trails reviewed frequently? NIST SP 800-18	Y						FSA Policy Sect 4.3	
259		17.1.7 Are automated tools used to review audit records in real time or near real time? NIST SP 800-18	Y						FSA Policy Sect 4.3	
260		17.1.8 Is suspicious activity investigated and appropriate action taken? FISCAM AC-4.3	Y						FSA Policy Sect 4.3	
261		17.1.9 Is keystroke monitoring used? If so, are users notified? NIST SP 800-18	Y						FSA Policy Sect 4.3	

**YOUR SURVEY IS NOW COMPLETE.
 THANK YOU FOR YOUR ASSISTANCE!**