

ID	WBS	Task Name	% Complete				
				M	T	W	T
1	1	Vision	0%				
2	1.1	Security Funding and Business Case	0%				
3	1.1.1	Deliverable: Business Case	0%				
4	1.1.1.1	Include necessary resources for adequately securing the system	0%				
5	1.2	Security Requirements	0%				
6	1.2.1	Deliverable: RFP Security Requirements	0%				
7	1.2.1.1	Include security requirements and evaluation/test procedures in RFP	0%				
8	1.2.1.2	Include language in RFP to permit updating security controls as new threats/vulnerabilities are identified and as new te	0%				
9	1.2.2	Deliverable: Task Order Security Components	0%				
10	1.2.2.1	Security Plan	0%				
11	1.2.2.2	Risk Assessment	0%				
12	1.2.2.3	Disaster Recovery Plan	0%				
13	1.2.2.4	Federal Policy and Regulations	0%				
14	1.2.2.5	Departmental Policy and Regulations	0%				
15	1.2.2.6	Controls for Personnel Security	0%				
16	1.2.2.7	Configuration Management	0%				
17	1.3	MOU/SLA	0%				
18	1.3.1	Deliverable: List of Potential Business Partners	0%				
19	1.3.1.1	Document list of potential business partners	0%				
20	1.3.1.2	Initiate MOU/SLA dialogue with applicable partners	0%				
21	1.4	Roles and Responsibilities	0%				
22	1.4.1	Deliverable: Assignment Letters	0%				
23	1.4.1.1	Letter from Functional Manager (FM) assigning System Manager (SM)	0%				
24	1.4.1.2	Letter from System Manager assigning SSO	0%				
25	1.5	System Security Documentation	0%				
26	1.5.1	Deliverable: Security artifact file system	0%				
27	1.5.1.1	Create file system to maintain security artifacts	0%				
28	1.5.2	Deliverable: Electronic Security artifact file structure	0%				
29	1.5.2.1	Create electronic file structure to maintain security artifacts	0%				
30	1.6	Deliverable: Signed and Dated Vision Checklist	0%				
31							
32	2	Definition	0%				
33	2.1	Roles and Responsibilities	0%				
34	2.1.1	Deliverable: System Roles and Responsibilities	0%				
35	2.1.1.1	Identify User and Developer Roles (including SFA employees)	0%				

ID	WBS	Task Name	% Complete	M	T	W	T
36	2.2	Security Requirements	0%				
37	2.2.1	Deliverable:GSS/MA Inventory Form	0%				
38	2.2.1.1	Define System as General Support System, Major Application, or Application	0%				
39	2.2.1.2	Define system as new system or major modification	0%				
40	2.2.1.3	Classify system sensitivity	0%				
41	2.2.1.3.1	Use Confidentiality, Integrity, and Availability to determine sensitivity	0%				
42	2.2.1.4	Define system criticality	0%				
43	2.3	System Security Documentation	0%				
44	2.3.1	Deliverable: Interconnected system'(s) security documentation	0%				
45	2.3.1.1	Obtain all relevant security documentation from connected systems	0%				
46	2.4	MOU/SLA	0%				
47	2.4.1	Deliverable: MOU/SLA Drafts	0%				
48	2.4.1.1	Draft all appropriate MOU/SLA agreements with business partners and/or system owners	0%				
49	2.4.1.1.1	Adequately address security controls in MOU/SLA's	0%				
50	2.4.1.2	Submit security control input for MOU/SLA to business partners and/or system owners	0%				
51	2.5	Training	0%				
52	2.5.1	Deliverable: SSO Training certification(s)	0%				
53	2.5.1.1	Attend appropriate SSO training curriculum	0%				
54	2.6	Certification and Accreditation	0%				
55	2.6.1	Deliverable: C&A Project Plan	0%				
56	2.6.1.1	Identify responsible organizations/individuals	0%				
57	2.6.1.2	Identify resources and funding	0%				
58	2.6.1.3	Define system boundaries	0%				
59	2.6.1.4	Create C&A schedule	0%				
60	2.6.1.5	Register C&A with Agency Security Office	0%				
61	2.7	Personnel Security	0%				
62	2.7.1	Deliverable: System Rules of Behavior	0%				
63	2.7.1.1	Review 800-18 Appendix B for applicable guidance	0%				
64	2.7.1.2	Develop System Rules of Behavior	0%				
65	2.7.1.3	Ensure Privacy Act considerations are included	0%				
66	2.7.2	Deliverable: Constructed clearance requirement matrix	0%				
67	2.7.2.1	Determine user clearance requirements (including SFA employees)	0%				
68	2.7.2.2	Determine contractor clearance requirements	0%				
69	2.7.3	Deliverable: Completed contractor background investigation clearance forms	0%				
70	2.7.3.1	Issue request(s) for contractor background investigations per requirements	0%				

ID	WBS	Task Name	% Complete				
				M	T	W	T
71	2.7.3.2	Collect completed contractor background investigations	0%				
72	2.7.4	Deliverable: Approved contractor access request forms	0%				
73	2.7.4.1	Distribute access request forms to contractors	0%				
74	2.7.4.2	Provide contractors System Rules of Behavior (users sign privacy statement)	0%				
75	2.7.4.3	Collect contractor access request forms	0%				
76	2.8	Deliverable: Signed and Dated Definition Phase Checklist	0%				
77							
78	3	Construction	0%				
79	3.1	System Security Documentation	0%				
80	3.1.1	Deliverable: Draft System Security Plan	0%				
81	3.1.1.1	Organize security documentation to write security plan	0%				
82	3.1.1.1.1	Architecture Diagram and/or design diagram	0%				
83	3.1.1.1.2	Security Requirements	0%				
84	3.1.1.1.3	Interfaces and connectivity	0%				
85	3.1.1.1.4	Operating environment	0%				
86	3.1.1.1.5	User role descriptions	0%				
87	3.1.1.1.6	Description of data	0%				
88	3.1.1.1.7	Process map	0%				
89	3.1.1.2	Draft system security plan using NIST 800-18 as guidance	0%				
90	3.1.2	Deliverable: Draft COOP	0%				
91	3.1.3	Deliverable: Draft DRP	0%				
92	3.2	Certification and Accreditation	0%				
93	3.2.1	Deliverable: Draft System Security Authorization Agreement (SSAA)	0%				
94	3.2.1.1	Gather necessary information from System Security Plan, COOP, DRP, etc.	0%				
95	3.3	Risk Assessment	0%				
96	3.3.1	Deliverable: Risk Assessment Report	0%				
97	3.3.1.1	Vulnerability and Threat Assessment	0%				
98	3.3.1.1.1	Vulnerability Analysis	0%				
99	3.3.1.1.1.1	Perform Vulnerability, Penetration, etc Testing	0%				
100	3.3.1.1.1.2	Review system controls for A-130 compliance	0%				
101	3.3.1.1.1.3	Review system controls for GISRA compliance (NIST Self-Assessment)	0%				
102	3.3.1.1.1.4	Review system controls for ED policy compliance	0%				
103	3.3.1.1.1.5	Review system controls for SFA policy compliance	0%				
104	3.3.1.1.2	Threat Source Association	0%				
105	3.3.1.2	Level of Risk Determination	0%				

ID	WBS	Task Name	% Complete				
				M	T	W	T
106	3.3.1.2.1	Impact Assessment	0%				
107	3.3.1.2.2	Likelihood Determination	0%				
108	3.3.1.2.3	Compare Impact to Likelihood to determine overall risk rating for vulnerability/threat pair	0%				
109	3.3.2	Deliverable: Corrective Action Plan	0%				
110	3.3.2.1	Develop CAP from risk assessment findings	0%				
111	3.3.3	Deliverable: Cost/Benefit Analysis	0%				
112	3.3.3.1	Determine which security controls should be corrected according to a costs vs. benefit determination	0%				
113	3.4	MOU/SLA	0%				
114	3.4.1	Deliverable: Final MOU/SLA	0%				
115	3.4.1.1	Obtain MOU/SLA and review for inclusion of appropriate security controls	0%				
116	3.4.1.2	If necessary, make and submit additional security control inputs to business partners and/or system owners	0%				
117	3.5	Personnel Security	0%				
118	3.5.1	Deliverable: Completed user background investigation clearance forms	0%				
119	3.5.1.1	Issue request(s) for user background investigations per requirements	0%				
120	3.5.1.2	Collect completed contractor background investigations	0%				
121	3.5.2	Deliverable: Approved user access request forms	0%				
122	3.5.2.1	Distribute access request forms to users	0%				
123	3.5.2.2	Provide users System Rules of Behavior (users sign privacy statement)	0%				
124	3.5.2.3	Collect user access request forms	0%				
125	3.5.3	Deliverable: System access letters to contractor employees	0%				
126	3.5.3.1	Grant system access to contractor employees (user ID and passwords)	0%				
127	3.6	Deliverable: Signed and Dated Construction Phase Checklist	0%				
128							
129	4	Deployment	0%				
130	4.1	Risk Mitigation	0%				
131	4.1.1	Deliverable: Documented completion of CAP from Construction Phase	0%				
132	4.1.1.1	Implement recommended corrective actions from CAP	0%				
133	4.1.1.2	Submit implemented CAP	0%				
134	4.1.2	Deliverable: Security Test Plan	0%				
135	4.1.2.1	Draft the Security Test Plan	0%				
136	4.1.2.1.1	Security Test and Evaluation	0%				
137	4.1.2.1.2	Penetration Testing	0%				
138	4.1.2.1.3	System Management Infrastructure Analysis	0%				
139	4.1.2.1.4	Site Evaluation	0%				
140	4.1.2.1.5	Contingency Plan Evaluation	0%				

ID	WBS	Task Name	% Complete				
				M	T	W	T
141	4.1.3	Deliverable: Test results	0%				
142	4.1.3.1	Test newly implemented security controls	0%				
143	4.1.3.2	Document system tests	0%				
144	4.2	Certification and Accreditation	0%				
145	4.2.1	Deliverable: System Security Authorization Agreement (SSAA)	0%				
146	4.2.1.1	Provide SSAA to System Manager (SM) for review	0%				
147	4.2.2	Deliverable: Certification letter from System Manager (SM) to Designated Approving Authority (DAA)	0%				
148	4.2.2.1	Recommend full accreditation, IATO, or not to turn on	0%				
149	4.2.2.2	Provide SSAA to DAA for review and discuss executive level SSAA findings	0%				
150	4.2.3	Deliverable: Signed Accreditation letter	0%				
151	4.2.3.1	Attend PRR as security representative	0%				
152	4.2.3.2	Obtain copy of signed accreditation letter	0%				
153	4.3	Security Documentation	0%				
154	4.3.1	Deliverable: Final System Security Plan	0%				
155	4.3.1.1	Submit System Security Plan to SFA/OCIO Security Office for compliance review	0%				
156	4.3.2	Deliverable: Final Continuity of Operation Plan	0%				
157	4.3.2.1	Test COOP	0%				
158	4.3.3	Deliverable: Final Disaster Recovery Plan	0%				
159	4.3.3.1	Test DRP	0%				
160	4.4	Training	0%				
161	4.4.1	Deliverable: User Training schedule	0%				
162	4.4.1.1	Identify opportunities for training	0%				
163	4.4.1.2	Schedule SSO Training	0%				
164	4.5	Personnel Security	0%				
165	4.5.1	Deliverable: Approved user access request forms	0%				
166	4.5.1.1	Distribute access request forms to users	0%				
167	4.5.1.2	Collect user access request forms	0%				
168	4.6	Deliverable: Signed and Dated Deployment Phase Checklist	0%				
169							
170	5	Support	0%				
171	5.1	Security Documentation	0%				
172	5.1.1	Follow System Security Plan SFA/Dept/Fed guidance and implement changes as required	0%				
173	5.1.2	Review security control areas every three years or upon major system change as mandated in OMB A-130 Appendix III	0%				
174	5.1.3	Complete Annual Program Review IAW GISRA	0%				
175	5.2	Certification and Accreditation	0%				

ID	WBS	Task Name	% Complete				
				M	T	W	T
176	5.2.1	Deliverable: Re-certified and accredited SSAA	0%				
177	5.2.1.1	Re-certify and accredit system as necessary (every three years or upon major change)	0%				
178	5.3	Personnel Security	0%				
179	5.3.1	Continuous personnel security maintenance	0%				
180	5.3.1.1	Review and Authorize System Access	0%				
181	5.3.1.1.1	Identify new users	0%				
182	5.3.1.1.2	Remove access no longer needed	0%				
183	5.3.1.1.3	Ensure access forms completed by requestors	0%				
184	5.3.1.2	Initiate and complete clearance process for new users	0%				
185	5.3.1.2.1	Identify new users	0%				
186	5.3.1.2.2	Ensure clearance forms completed by new users	0%				
187	5.3.1.2.3	Track	0%				
188	5.3.1.2.4	Notify users of completed clearance status	0%				
189	5.3.1.3	Retain copy of authorized access requests	0%				
190	5.4	Training	0%				
191	5.4.1	Provide new users Rules of Behavior	0%				
192	5.4.2	Ensure users complete annual security awareness training/ new users take awareness training	0%				
193	5.5	Risk Management	0%				
194	5.5.1	Deliverable: Documented completion of test results	0%				
195	5.5.1.1	Implement test results from Deployment Phase	0%				
196	5.5.2	Deliverable: Updated Operational Procedures (see System Configuration Management Procedures)	0%				
197	5.5.2.1	Update security controls based on new threats discovered from system monitoring (audit logs, security alerts)	0%				
198	5.5.2.2	Update Operational Procedures in System Security Plan	0%				
199	5.5.3	Deliverable: Updated Testing Results	0%				
200	5.5.3.1	Test new/changed system security controls as needed	0%				
201	5.5.3.2	Test COOP annually	0%				
202	5.5.3.3	Test DRP annually	0%				
203	5.5.3.4	Incorporate test results into System Security Plan	0%				
204	5.6	Deliverable: Signed and Dated Support Phase Checklist	0%				
205							
206	6	Retirement	0%				
207	6.1	Security Documentation	0%				
208	6.1.1	Create Archive Data Retention Matrix and Destruction Plan	0%				
209	6.1.2	Archive data in a usable format if required	0%				
210	6.1.2.1	Dispose/archive electronic records properly	0%				

ID	WBS	Task Name	% Complete				
				M	T	W	T
211	6.2	Physical Destruction	0%				
212	6.2.1	Sanitize all Electronic media when no longer required	0%				
213	6.2.1.1	Purge, overwrite, degauss, or destroy information or media	0%				
214	6.2.2	Destroy all printed paper products with sensitive information	0%				
215	6.2.3	Destroy all documents when all data is destroyed	0%				
216	6.3	Deliverable: Signed and Dated Retirement Phase Checklist	0%				