TSA Registered Traveler

Appendix E:
Sample System Security Plan Template

Version 3.1, January 2008

Transportation
Security
Administration

RT
Registered Traveler™

Appendix E: Sample System Security Plan Template

The following sample has been provided ONLY as one example based on NIST SP 800-18 Revision 1 – Guide for Developing Security Plans for Federal Systems. Service Providers (SPs) may be using other formats and choose to update those to reflect any existing omissions based on this guidance. This is not a mandatory format; it is recognized that SPs may have developed and implemented various approaches for information system security plan development and presentation to suit their own needs for flexibility. SPs may use the Program-level System Security Plan to outline the overall makeup of their operational systems and the Site-specific System Security Plan to outline details and controls specific to Sponsoring Entity (SE) locations.

Program-level System Security Plan

1. Information System Name/Title:

[Unique identifier and name given to the system.]

2. Information System Categorization:

[Identify the FIPS 199 categorization.]

3. Information System Owner:

[Name, title, department, address, email address, and phone number of person who owns the system.]

4. Authorizing Sr. Management:

[Name, title, department, address, email address, and phone number of the senior management official designated as the authorizing official.]

5. Other Designated Contacts:

[List other key personnel, if applicable; include their title, addresses, email addresses, and phone numbers.]

6. Assignment of Security Responsibility:

[Name, title, address, e-mail address, and phone number of person responsible for the security of the system.]

7. Information System Operational Status:

[Indicate the operational status of the system. If more than one status is indicated, list which part of the system is covered under each status.]

8. Information System Type:

[Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 9, "General System Description/Purpose."]

9. General System Description/Purpose

[Describe the function or purpose of the system and the information processes.]

10. System Environment

[Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.]

11. System Interconnections/Information Sharing

[List interconnected systems and system identifiers (if appropriate); provide the system, name, organization, and system type (major application or general support system); and indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, and the name of the authorizing official.]

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	Auth. Official

12. Related Laws/Regulations/Policies

[List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.]

13. Minimum Security Controls

[Provide a description of how the TSA-recommended security controls are being implemented or are planned to be implemented. The description shall contain: (1) the security control title; (2) how the security control is being implemented or is planned to be implemented; (3) any scoping guidance that has been applied and the type of consideration; and (4) indicate if the security control is a common control and who is responsible for its implementation.]

14. Information System Security Plan Completion Date: ______________________________

15. Information System Security Plan Approval Date: ______________________________

National Institute of Standards and Technology. (2006). *Special Publication* 800-53: *Recommended Security Controls for Federal Information Systems*. Gaithersburg, MD: A. Johnson, S. Katze, A. Lee, G. Rogers, R. Ross, M. Swanson, G. Stoneburner.

Site-Specific System Security Plan

Information System Security Plan

1. Information System Name/Title:

[Unique identifier and name given to the system.]

2. Information System Owner:

[Name, title, department, address, e-mail address, and phone number of person who owns the system.]

3. Authorizing Senior Management:

[Name, title, department, address, e-mail address, and phone number of the SP senior management official designated as the authorizing official.]

[Name, title, department, address, e-mail address, and phone number of the SE senior management official designated as the authorizing official.]

4. Other Designated Contacts:

[List other key personnel, if applicable; include their titles, addresses, e-mail addresses, and phone numbers.]

5. Assignment of Security Responsibility:

[Name, title, address, e-mail address, and phone number of person responsible for the security of the system.]

6. Information System Operational Status:

[Indicate the operational status of the system. If more than one status is indicated, list which part of the system is covered under each status.]

7. General System Description/Purpose

[Describe the function or purpose of the system and the information processes.]

8. System Environment

[Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.]

9. System Interconnections/Information Sharing

[List interconnected systems and system identifiers (if appropriate); provide the system, name, organization, and system type (major application or general support system); and indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, and the name of the authorizing official.]

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	Auth. Official

10. Related Laws/Regulations/Policies

[List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.]

11. Minimum Security Controls

[Provide a description of how the TSA-recommended security controls are being implemented or are planned to be implemented. The description shall contain: (1) the security control title; (2) how the security control is being implemented or is planned to be implemented; (3) any scoping guidance that has been applied and what type of consideration (unclear); and (4) indicate if the security control is a common control and who is responsible for its implementation.]

[The site-specific minimum security controls defined in the following section must be documented in the SSP.]

Site-Specific Minimum Security Controls

Note: Refer to Appendix C for Control Descriptions

Control Number	Control
ACCESS CONTROL	
AC-1	ACCESS CONTROL POLICY AND PROCEDURES
AC-2	ACCOUNT MANAGEMENT
AC-3	ACCESS ENFORCEMENT
AC-4	INFORMATION FLOW ENFORCEMENT
AC-5	SEPARATION OF DUTIES
AC-13	SUPERVISION AND REVIEW ACCESS CONTROL
AC-17	REMOTE ACCESS
AC-18	WIRELESS ACCESS RESTRICTIONS

Control Number	Control
AWARENESS AND TRAINING	
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
AT-2	SECURITY AWARENESS
AT-3	SECURITY TRAINING
AT-4	SECURITY TRAINING RECORDS
AUDIT AND ACCOUNTABILITY	
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
AU-2	AUDITABLE EVENTS
AU-6	AUDIT MONITORING, ANALYSIS, AND REPORTING
CONTINGENCY PLANNING	
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES
CP-2	CONTINGENCY PLAN
CP-3	CONTINGENCY TRAINING
CP-4	CONTINGENCY PLAN TESTING
CP-5	CONTINGENCY PLAN UPDATE
CP-6	ALTERNATE STORAGE SITES
CP-8	TELECOMMUNICATIONS SERVICES
CP-9	INFORMATION SYSTEM BACKUP
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
INCIDENT RESPONSE	
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES

Control Number	Control
IR-2	INCIDENT RESPONSE TRAINING
IR-3	INCIDENT RESPONSE TESTING
IR-4	INCIDENT HANDLING
IR-5	INCIDENT MONITORING
IR-6	INCIDENT REPORTING
IR-7	INCIDENT RESPONSE ASSISTANCE
MAINTENANCE	
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES
MA-2	PERIODIC MAINTENANCE
MA-3	MAINTENANCE TOOLS
MA-4	REMOTE MAINTENANCE
MA-5	MAINTENANCE PERSONNEL
MEDIA PROTECTION	
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES
MP-2	MEDIA ACCESS
MP-3	MEDIA LABELING
MP-4	MEDIA STORAGE
MP-6	MEDIA SANITIZATION AND DISPOSAL
PHYSICAL AND ENVIRONMENTAL PROTECTION	
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
PE-2	PHYSICAL ACCESS AUTHORIZATIONS

Control Number	Control
PE-3	PHYSICAL ACCESS CONTROL
PE-5	ACCESS CONTROL FOR DISPLAY MEDIUM
PE-6	MONITORING PHYSICAL ACCESS
PE-11	EMERGENCY POWER
PE-12	EMERGENCY LIGHTING
PE-13	FIRE PROTECTION
PE-14	TEMPERATURE AND HUMIDITY CONTROLS
PE-15	WATER DAMAGE PROTECTION
PE-16	DELIVERY AND REMOVAL
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS
SECURITY PLANNING	
PL-1	SECURITY PLANNING POLICY AND PROCEDURES
PL-2	SYSTEM SECURITY PLAN
PL-3	SYSTEM SECURITY PLAN UPDATE
PL-4	RULES OF BEHAVIOR
PL-5	PRIVACY IMPACT ASSESSMENT
PL-6	SECURITY-RELATED ACTIVITY PLANNING
RISK ASSESSMENT	
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES
RA-3	RISK ASSESSMENT
RA-4	RISK ASSESSMENT UPDATE

Control Number	Control
RA-5	VULNERABILITY SCANNING
SYSTEM AND COMMUNICATIONS PROTECTION	
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
SC-7	BOUNDARY PROTECTION
SC-8	TRANSMISSION INTEGRITY
SC-9	TRANSMISSION CONFIDENTIALITY
SC-10	NETWORK DISCONNECT
SC-11	TRUSTED PATH
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
SC-13	USE OF VALIDATED CRYPTOGRAPHY
SC-14	PUBLIC ACCESS PROTECTIONS
SYSTEM AND INFORMATION INTEGRITY	
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
SI-4	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES
ENROLLMENT PROCESS	
EP-1	BIOGRAPHIC INFORMATION COLLECTION
EP-6	EXCESS DATA
EP-7	INFORMATION PROVIDED TO AND RECEIVED FROM APPLICANT
VERIFICATION PROCESS	
VP-1	CHECKPOINT VERIFICATION

Control Number	Control
PRIVACY	
PR-1	OPENNESS
PR-2	COLLECTION LIMITATION
PR-3	PURPOSE SPECIFICATION
PR-4	USE LIMITATION
PR-5	DATA QUALITY
PR-6	INDIVIDUAL PARTICIPATION
PR-7	SECURITY SAFEGUARDS
PR-8	ACCOUNTABILITY
REGISTERED TRAVELER	
RT-1	EQUAL ACCESS
RT-6	APPROVAL TO OPERATE
RT-7	OVERSIGHT

12. Information System Security Plan Completion Date: ______________________________

13. Information System Security Plan Approval Date: ______________________________