

## System Security Plan Assessment Matrix

<b>APPLICATION/SYSTEM IDENTIFICATION</b>	<b>Yes / No</b>
<b>Application/System Category</b>	
Is application/system identified as a Major Application (MA) or a General Support System (GSS)?	
<b>Application/System Name/Title</b>	
Does application/system have a unique identifier & name given to the application/system?	
<b>Responsible Organization</b>	
Is the responsible organization for the application/system identified?	
<b>Information Contact(s)</b>	
Is the owner(s) of the application/system and at least one other manager identified by: Name, Title, Address, Phone Number, Fax Number, E-mail Address?	
<b>Assignment of Security Responsibility</b>	
Is the person(s) responsible for security of the application/system and an alternate emergency contact identified by: Name, Title, Address, Phone Number, Fax Number, E-mail Address?	
Are the roles and responsibilities of all users having access to the application/system described? Include approximate number of authorized users and their physical location.	
<b>Application/System Operational Status</b>	
Is the current operational status identified. If more than one status is appropriate, list which part(s) of the application/system are covered under each status. The operational status options are: Operational, Under Development, Undergoing a Major Modification?	
<b>General Description/Purpose</b>	
Is the function or purpose of the application/system described?	
Is the information process identified and described?	
Is the processing flow of the application/system from input to output described? This description should address both the processes executed by the system and a logical model of the system.	
Is there a list user organizations (internal & external) and the type of data and processing provided?	

<b>Application/System Environment</b>	
Is there a general description of the technical application/system? Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.). Include a diagram of architecture here or in an appendix, if applicable.	
Is there a description of the primary computing platform(s) used and a description of the principal application/system components, including hardware, software, and communications resources?	
Has all security software protecting the application/system and information been identified?	
Are all the physical location(s) of the application/system identified?	
<b>Application/System Interconnection/Information Sharing</b>	
Are all interconnected applications/systems and application/system identifiers (if appropriate) listed?	
If connected to an external application/system not covered by a security plan, is there a discussion of any security concerns that need to be considered for protection?	
Are the rules for interconnecting applications/systems and for protecting shared data included with this security plan. These guidelines are required, see section regarding Rules of Behavior for further detail?	
Are interconnections with other systems/applications codified via MOUs or MOAs? NIST highly recommends the use of MOUs or MOAs for this purpose.	
<b>Applicable Laws or Regulations Affecting the Application/System</b>	
Is there a list identifying any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the application/system?	
<b>Information Sensitivity and Criticality Assessment</b>	
Is there a description, in general terms, of the information handled by the application/system and the need for protective measures?	
Is there a list of the types of sensitive information the application/system accesses? Examples may include: administrative, financial, grant/contract, patient, proprietary, research, Privacy Act.	
Is there a description relating the information processed to each of the three basic protection requirements: Confidentiality, Integrity, Availability? This description often takes the form of a matrix listing Confidentiality, Integrity, Availability and describing them in terms of High, Medium, or Low sensitivity. This matrix should also include a statement of the estimated risk and magnitude of harm resulting from	

the loss, misuse, or unauthorized access to or modification of information in the application/system?	
---	--

<b>MANAGEMENT CONTROLS</b>	<b>Yes / No</b>
<b>Risk Assessment and Management</b>	
Is the risk assessment methodology used to identify the threats and vulnerabilities of the application/system described?	
Has the group that conducted the assessment and the date(s) the review was conducted been identified?	
If there is no application/system risk assessment, is a milestone date (month and year) for completion of the assessment identified?	
<b>Review of Security Controls</b>	
Are all independent security reviews conducted on the application/system in the last three years documented? Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.	
<b>Rules of Behavior</b>	
Has a set of rules of behavior, in writing, been established for the application/system? The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the application/system. They should state the consequences of inconsistent behavior or non-compliance. They should also include appropriate limits on interconnections to other application/systems.	
Are the rules of behavior made available to every user prior to the user receiving access to the application/system, with a signature page to acknowledge receipt?	
<b>Planning for Security in the Life Cycle</b>	
Is there a description of which phase(s) of the life cycle the application/system, or parts of the application/system, are in? The phases are: Initiation, Development/Acquisition, Implementation, Operation/Maintenance and Disposal.	
Has a plan been developed to identify how security has been / will be handled during each of the listed applicable life cycle phases?	

<b>OPERATIONAL CONTROLS</b>	<b>Yes / No</b>
<b>Personnel Security</b>	
Are all positions reviewed for sensitivity level?	
Have all individuals received background screenings appropriate for the position to which they are assigned?	
Is user access restricted to the minimum necessary to perform the job?	
Is there a process for requesting, establishing, issuing, and closing user accounts?	
Are critical functions divided among different individuals (separation of duties)?	
Are mechanisms in place for holding users responsible for their actions?	
Are the friendly and unfriendly termination procedures established?	
<b>Physical and Environmental Protection</b>	
Are physical locations where application/system processing takes place identified and security requirements documented?	
Are physical protections for each location identified (e.g., locks on terminals, physical barriers around the building and processing area, etc.)?	
<b>Production, Input/Output Controls</b>	
Are the controls used for marking, processing, storage, and disposal of input and output information and media as well as the labeling and distribution procedures for information and media documented?	
Are the controls used to monitor the installation of application/system software updates documented?	
Are there procedures in place documenting how to recognize, handle, report, and track security incidents and/or problems?	
Do the incident procedures outline how to categorize and prioritize incidents?	
Are there procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?	
Are there procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media?	
Are there audit trails for receipt of sensitive inputs/outputs?	
Are there procedures for restricting access to output products?	
Is there internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary, etc)?	
Is there external labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)?	
Are there audit trails for inventory management?	

Is there a media storage vault or library containing physical, environmental protection controls/procedures?	
Are there procedures for sanitizing electronic media for reuse?	
Are there procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse?	
Are there procedures for shredding or other destructive measures for hardcopy media when no longer required?	
<b>Contingency Planning</b>	
Does a formal contingency plan exist. If so, reference the plan?	
Are there formal agreements for backup processing?	
Are application and data backup procedures, including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup), documented?	
Are the location of stored backups and generations of backups identified?	
Are test results from contingency/disaster recovery plan exercises documented?	
Is the periodicity of contingency/disaster recovery plan exercises documented?	
Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?	
<b>Application/System Hardware and Software Maintenance Controls</b>	
Are there restrictions/controls on those who perform hardware and software maintenance and repair activities?	
Are there special procedures for performance of emergency repair and maintenance?	
Are there procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?	
Are there procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements?	
Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?	
Does the government own the software?	
Is the application/system software a copyrighted commercial off-the-shelf product or shareware?	
Has the software been properly licensed, and have enough copies been purchased for the application/system?	
Are there organizational policies against illegal use of copyrighted software and shareware?	
Are periodic audits conducted of users' computers to ensure that only	

legal licensed copies of software are installed?	
Are procedures established to protect against illegal use of software?	
Is there a formal change control process in place?	
Is there version control that allows association of application/system components to the appropriate application/system version?	
Are all changes to the application/system software or application/system components documented?	
Are there impact analyses to determine the effect of proposed changes on existing security controls, to include the required training for both technical and user communities associated with the change in hardware/software?	
Are there change identification, approval, and documentation procedures?	
Are there procedures for ensuring contingency plans and other associated documentation are updated to reflect application/system changes?	
Does the change control process require that all changes to the application/system software be tested and approved before being put into production?	
Are there procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production?	
Does system testing use live data?	
Do test plans trace back to the original security requirements?	
Are test results documented?	
<b>Data Integrity/Validation Controls</b>	
Is virus detection and elimination software installed?	
Are procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting documented?	
Are reconciliation routines used by the application/system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.	
Are integrity verification programs used by the application/system to look for evidence of data tampering, errors, and omissions?	
Is an intrusion detection tool installed to monitor the application/system?	
Are procedures in place to handle and close out security incidents?	
Are other network security software packages used?	
Is application/system performance monitoring used to analyze performance logs in real time to look for availability problems, including active attacks, and application/system and network slowdowns and crashes?	
Is penetration testing performed on the application/system? If so, are procedures are in place to ensure that tests are conducted appropriately?	

Is message authentication used in the application/system to ensure that the sender of a message is known and that the message has not been altered during transmission?	
<b>Documentation</b>	
Identify the documentation maintained for the application/system. Typical items include:	
security plan?	
vendor documentation of hardware/software?	
functional requirements?	
design specifications?	
source code documents?	
testing procedures and results?	
records of verification reviews/site inspections?	
standard operating procedures?	
user rules/manuals?	
emergency procedures?	
contingency plans?	
risk assessments?	
Are the procedures used to update documentation identified?	
Is the physical location of documentation identified?	
<b>Security Awareness and Training</b>	
Does an application/system specific security training curriculum exist?	
Is the application/system specific security training curriculum role based?	
Do all system users attend a security awareness program for the application/system annually (this includes employees, contractor personnel, and external system users) ?	
Is the attendance of awareness training documented?	
<b>Incident Response Capability</b>	
Are there procedures for reporting incidents either by application/system personnel or externally?	
Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?	
Are personnel identified to receive and respond to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?	
Are preventative measures in place to identify or capture incident events, i.e., intrusion detection tools, automated audit logs, penetration testing?	

<b>TECHNICAL CONTROLS</b>	<b>Yes / No</b>
<b>Identification and Authentication</b>	
Is there a description of the application/systems user authentication control mechanisms (password, token, and biometrics) ?	
Are password control procedures documented? Indicate the frequency of password changes, describe how changes are enforced, and identify who changes the passwords (the user, the system administrator, or the application/system).	
The following items should be documented:	
password length (minimum, maximum) ?	
allowable character set?	
password aging time frames and enforcement approach?	
number of generations of expired passwords disallowed for use?	
procedures for password changes (after expiration and forgotten/lost) ?	
procedures for handling password compromise?	
procedures for training users and the materials covered?	
the level of enforcement of the access control mechanism (network, operating system, and application/system) ?	
how the access control mechanism supports individual accountability and audit trails (e.g., passwords associated with a user ID that is assigned to a single person) ?	
the self-protection techniques for the user authentication mechanism (e.g., passwords encrypted while in transmission, automatically generated, or checked against a dictionary of disallowed passwords) ?	
the number of invalid access attempts that may occur for a given user ID or access location (terminal or port) and describe the actions taken when that limit is exceeded?	
the procedures for verifying that all administrative default passwords have been changed?	
the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch application/systems) ?	
the policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host	

identifiers, and group user identifiers) and any compensating controls?	
any use of digital or electronic signatures, the standards used and the management procedures for key generation, distribution, storage, and disposal?	
<b>Logical Access Controls</b>	
Are the controls used to authorize or restrict the activities of users and personnel within the application/system documented?	
Is a description provided of the hardware or software features that are designed to permit only authorized access to or within the application/system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists [ACLs]) ?	
Are privileges granted based on job function?	
Is there a description of the application/system's capability to establish an ACL or register?	
Is there a description of how users are restricted from accessing the operating system or other application/system resources not required in the performance of their duties?	
Are controls established to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the application/system outside of normal work hours or on weekends?	
Does user inactivity on the application/system automatically blank associated display screens and/or disconnects inactive users?	
Is the user required to enter a unique password before reconnecting after a period of user inactivity?	
Is encryption is used to prevent access to sensitive files as part of the application/system access control procedures?	
Are warning banners used, and an example provided if banners are used?	
<b>Public Access Controls</b>	
Does the public access the application/system. If yes, a description of the additional security controls used to protect the application/system's integrity, additional controls used to protect the confidence of the public in the application/system, and the segregating of information made directly accessible to the public from official agency record is required?	
Is there a requirement for some form of identification and authentication from public users?	
Are there access controls to limit what the public users can read, write, modify, or delete?	
Does the application/system accept digital signatures from public users?	

Are copies of information for public access available on a separate application/system?	
Are there controls to prohibit the public from accessing live databases?	
Does the application/system verify that programs and information distributed to the public are virus-free?	
Does the application/system use audit trails and protect user confidentiality?	
Are system availability requirements identified?	
<b>Audit Trails</b>	
Does the audit trail support accountability by providing a trace of user actions?	
Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection and remediation?	
Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them (e.g., type of event, when the event occurred, user ID associated with the event, program or command used to initiate the event) ?	
Is access to online audit logs strictly enforced?	
Is the confidentiality of audit trail information protected if it records personal user information?	
Do guidelines exist to describe how frequently audit trails are reviewed?	
Does the appropriate application/system level administrator review audit trails following a known application/system software problem, an unexplained application/system or user problem, or a known violation of existing requirements by a user?	