[ORGANIZATION} IT SYSTEMS

SYSTEMS SECURITY PLAN (SSP)

Untitled Assessment 1

7/9/2017

Assessor:

Disclaimer

The analysis, data, and reports in CSET® are provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not

limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, tort, or otherwise, whether injury was sustained from, or arose out of the results of, or reliance upon the report.

DHS does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia, or other visual identities of DHS. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of the seal.

The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the CSET Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the CSET Program Office.

Signatures

My signature indicates that I have reviewed and approve this Site Cyber Security Plan and the corresponding appendices. To the best of my knowledge, they accurately describe the security profile of the Untitled Assessment 1 security policies and procedures, including the operational, management, and technical controls under which they will be operated.

(Example only. Copy and replace the text in this signature block for each applicable position.)

Sample Corporate Officer, CEO John Doe	***Date***

Table of Contents

Introduction

Template instructions and directives are given in italicized 10 point font and should be replaced appropriately.

This security plan template is intended to be used as a tool for the development of a security plan. This template will assist you in identifying the controls in place and those needing further implementation based upon the answers provided in the accompanying Cybersecurity Evaluation Tool (CSET) assessment. The basic process for this plan development would be to first determine risk, second select the countermeasures necessary to mitigate the risk to an acceptable level, and finally follow through to ensure that the countermeasures are implemented to the expected level.

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned, for meeting those requirements. The site cyber security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

The System Owner is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners, the System Administrator, and the System Security Manager

This template may also include:

- *Recommended templates for policies or procedures that have been identified as needed but not currently available based on the assessment answers.*
- *The basic network diagram*
- *An Inventory List of the components included in the diagram that will be associated with specific controls.*
- *The List of recommended security controls along with a status as can be determined from the assessment questions.*
- *A recommended implementation priorities list. This priority is based on incident occurrences on the Industrial Control System Cyber Emergency Response Team (ICS-CERT) watch floor and cybersecurity expert opinion. These recommendations do not take into account any cost benefit analysis with respect to implementing a control.*
- *Basic security assurance level determinations carried over from the assessment. In developing a security plan it is recommended that a deeper risk analysis is conducted to ensure that the selection of controls is not overly conservative (incurring undo costs) or optimistic (leaving excessive risk exposure).*

1. System Identification

Provide a brief (1-2 paragraphs) description of the main system assests and the necessary protection levels for confidentiality, integrity, and availability. See section 3.1 for a more detailed description of confidentiality, integrity, and availability.

1.1. System Environment

Provide a brief (1-3 paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- *The system is connected to the Internet;*
- *It is located in a harsh or overseas environment;*
- *Software is rapidly implemented;*
- *The software resides on an open network used by the general public or with overseas access;*
- *The application is processed at a facility outside of the organization's control; or*
- *The general support mainframe has dial-up lines.*

Describe the primary computing platform(s) used (e.g., mainframe, desk top, LAN or Wide Area Network (WAN). Include a general description of the principal system components, including hardware, software, and communications resources. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet). Describe controls used to protect communication lines in the appropriate sections of the security plan.

Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

2. Roles and Responsibilities

This section defines the roles and responsibilities for cybersecurity within the company. Use this section to define the roles and responsibilities with respect to this plan for your company.

2.1. Executive Management

Often this role is comprised of the Board of Directors and CEO. Executive management is ultimately responsible for the security of the organization but will most likely delegate tasks and actual implementation.

2.2. Chief Security Officer or Chief Information Security Officer (CISO)

CSO or CISO is the senior level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining processes across the organization to reduce information and information technology (IT) risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information related compliance.

Typically, the CISO's influence reaches the whole organization. Responsibilities include:

- Information security and information assurance
- Information regulatory compliance (e.g., US PCI DSS, FISMA, GLBA, HIPAA; UK Data Protection Act 1998; Canada PIPEDA)
- Information risk management
- Supply chain risk management
- Cybersecurity
- Information technology controls for financial and other systems
- Information privacy
- Computer Emergency Response Team / Computer Security Incident Response Team
- Identity and access management
- Security Architecture (e.g. Sherwood Applied Business Security Architecture)
- IT investigations, digital forensics, eDiscovery
- Disaster recovery and business continuity management
- Information Security Operations Center (ISOC)

2.3. Security Steering Committee

The security steering committee is composed of a representative of all the key stakeholders in IT security. These stake holders are often representatives of the executive council, CISO or CSO, IT management, physical security personnel, help desk, and key application and digitial asset owners. This committee meets regularly often quarterly to review policies and procedures, security controls implementation progress, and determine future direction for security within a company.

The security steering committee is responsible for making decisions on tactical and strategic security issues within the enterprise as a whole and should not be tied to one or more business units. The group should be made up of people from all over the organization so they can view risks and the effects of security decisions on individual departments and the organization as a whole. The CEO should head this committee, and the CFO, CIO, department managers, and chief internal auditor should all be on it. This committee should meet at least quarterly and have a well defined agenda. Some of the group's responsibilities are listed next:

- Define the acceptable risk level for the organization.
- Develop security objectives and strategies.
- Determine priorities of security initiatives based on business needs.
- Review risk assessment and auditing reports.
- Monitor the business impact of security risks.
- Review major security breaches and incidents.
- Approve any major change to the security policy and program.

They should also have a clearly defined vision statement in place that is set up to work with and support the organizational intent of the business. The statement shouldbe structured in a manner that provides support for the goals of confidentiality, integrity, and availability as they pertain to the business objectives of the organization. This in turn should be followed, or supported, by a mission statement that provides support and definition to the processes that will apply to the organization and allow it to reach its business goals.

2.4. System Owners

The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure the systems are properly

assessed for vulnerabilities and must report any to the incident response team and data owner.

2.5. Data Owners

The data owner (information owner) is usually a member of management who is incharge of a specific business unit, and who is ultimately responsible for the protection and use of a specific subset of information. The data owner has due care responsibilities and thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data he is responsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting. The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian.

2.6. Security Administrators

Anyone who has a root account on Unix or Linux systems or an administrator account on Windows or Macintosh systems actually has security administrator rights. (Unfortunately, too many people have these accounts in most environments.) This means they can give and take away permissions and set security configurations. However, just because a person has a root or administrator account does not mean they are fulfilling the security administrator role. A security administrator's tasks are many, and include creating new system user accounts, implementing new security software, testing security patches and components, and issuing new passwords. The security administrator should not actually approve new system user accounts. This is the responsibility of the supervisor. The security administrator must make sure access rights given to users support the policies and data owner directives.

2.7. Supervisors/Managers

The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. The supervisor responsibilities would include ensuring that employees understand their responsibilities with respect to security, distributing initial passwords, making sure the employees' account information is up-to-date, and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

2.8. Users

The user is any individual who routinely uses the data for work related tasks. The user must have the necessary level of access to the data to perform the duties within their position and is responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others.

3. Risk Analysis

A good security plan will require that a risk evaluation is performed to determine the level of necessary rigor and cost benefit analysis for the level of controls selected. It is recommended that a general risk analysis be performed. A good risk assessment should include an evaluation of the value of the protected assets and information, an examination of the consequences to the organization in the event of a successful attack, an examination of the threat if possible, and the cost of implementing mitigating controls.

threats × vulnerability × asset value = total risk

total risk – countermeasures = residual risk

Consequence

The examination of the consequences of an attack should include:

- *How many people could sustain injuries requiring a hospital stay?*
- *How many people could be killed?*
- *Estimate the potential cost of losing capital assets or the overall economic impact. (Consider the cost of site buildings, facilities, equipment, etc.)*
- *Estimate the potential cost in terms of economic impact to both the site and surrounding communities. (Consider any losses to community structures and any costs associated with displacement.)*
- *Estimate the potential cost of environmental cleanup to the site and surrounding communities. (Consider the cost for cleanup, fines, litigation, long term monitoring, etc.)*

Threat

The threat portion of the equation can be deduced from the recommended implementation priorities list. The priorities are based on incident data collected by the ICS-CERT watch floor and subject matter experts as of the time of publication of CSET. Top priorities are controls that mitigate the most actively exploited vulnerabilities with the most significant consequences.

Cost Benefit Analysis

The cost of implementing controls with respect to the additional security provided is the final step in selecting the controls to implement.

3.1. Basic Model

Traditional security models define three areas of consideration Confidentiality, Integrity, and Availability. The security plan should address each of these areas with respect to data and systems.

3.1.1. Confidentiality

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card

number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

3.1.2. Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID (Atomicity, Consistency, Isolation, Durability) model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

3.1.3. Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

3.2. Security Assurance Level (SAL)

	Confidentiality	Integrity	Availability
Overall Values	Moderate	Moderate	Moderate

Calculated General Security Assurance Levels

	Onsite	Offsite
Physical Injury	None	None
Hospital Injury	None	None
Death	None	None
Capital Assets	None	None
Economic Impact	None	None
Environmental Impact	None	None

3.3. FIPS 199 Security Assurance Level Guidance

NIST SP800-60 (FIPS 199) Based Security Assurance Levels with CNSS Special Factors

	Confidentiality	Integrity	Availability
Adjusted For System Questions	Low	Low	Low
Information Type	Low	Low	Low

Type	Special Factors
Availability	none
Confidentiality	none
Integrity	none

3.1.1-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).		

3.1.2-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Limit information system access to the types of transactions and functions that authorized users are permitted to execute.		

3.1.3-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Control the flow of CUI in accordance with approved authorizations.		

3.1.4-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Separate the duties of individuals to reduce the risk of malevolent activity without collusion.		

3.1.5-Access Control		Access Control
Low	0%	SP800-171

Requirement Answer: U
Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Use non-privileged accounts or roles when accessing nonsecurity functions.		

3.1.7-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Prevent non-privileged users from executing privileged functions and audit the execution of such functions.		

3.1.8-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Limit unsuccessful logon attempts.		

3.1.9-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Provide privacy and security notices consistent with applicable CUI rules.		

3.1.10-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.		

3.1.11-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Terminate (automatically) a user session after a defined condition.		

3.1.12-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Monitor and control remote access sessions.		

3.1.13-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.		

3.1.14-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Route remote access via managed access control points.		

3.1.15-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Authorize remote execution of privileged commands and remote access to security-relevant information.		

3.1.16-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Authorize wireless access prior to allowing such connections.		

3.1.17-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Protect wireless access using authentication and encryption.		

3.1.18-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Control connection of mobile devices.		

3.1.19-Access Control		Access Control
Low	0%	SP800-171

Requirement Answer: U
Encrypt CUI on mobile devices.

3.1.20-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Verify and control/limit connections to and use of external information systems.		

3.1.21-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Limit use of organizational portable storage devices on external information systems.		

3.1.22-Access Control		Access Control
Low	0%	SP800-171
Requirement Answer: U		
Control information posted or processed on publicly accessible information systems.		

3.2.1-Awareness and Training		Awareness and Training
Low	0%	SP800-171
Requirement Answer: U		
Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organi		

3.2.2-Awareness and Training		Awareness and Training
Low	0%	SP800-171
Requirement Answer: U		
Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.		

3.2.3-Awareness and Training		Awareness and Training
Low	0%	SP800-171
Requirement Answer: U		
Provide security awareness training on recognizing and reporting potential indicators of insider threat.		

3.3.1-Audit and Accountability		Audit and Accountability
Low	0%	SP800-171
Requirement Answer: U		
Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.		

3.3.2-Audit and Accountability		Audit and Accountability
Low	0%	SP800-171
Requirement Answer: U		
Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.		

3.3.3-Audit and Accountability	Audit and Accountability

Low	0%	SP800-171
Requirement Answer: U		
Review and update audited events.		

3.3.4-Audit and Accountability		Audit and Accountability
Low	0%	SP800-171
Requirement Answer: U		
Alert in the event of an audit process failure.		

3.3.5-Audit and Accountability		Audit and Accountability
Low	0%	SP800-171
Requirement Answer: U		
Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.		

3.3.6-Audit and Accountability		Audit and Accountability
Low	0%	SP800-171
Requirement Answer: U		
Provide audit reduction and report generation to support on-demand analysis and reporting.		

3.3.7-Audit and Accountability		Audit and Accountability
Low	0%	SP800-171
Requirement Answer: U		

Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

3.3.8-Audit and Accountability		Audit and Accountability
Low	0%	SP800-171
Requirement Answer: U		
Protect audit information and audit tools from unauthorized access, modification, and deletion.		

3.3.9-Audit and Accountability		Audit and Accountability
Low	0%	SP800-171
Requirement Answer: U		
Limit management of audit functionality to a subset of privileged users.		

3.4.1-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		
Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.		

3.4.2-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		
Establish and enforce security configuration settings for information technology products employed in organizational information systems.		

3.4.3-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		
Track, review, approve/disapprove, and audit changes to information systems.		

3.4.4-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		
Analyze the security impact of changes prior to implementation.		

3.4.5-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		
Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.		

3.4.6-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		
Employ the principle of least functionality by configuring the information system to provide only essential capabilities.		

3.4.7-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		

Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.

3.4.8-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		
Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software.		

3.4.9-Configuration Management		Configuration Management
Low	0%	SP800-171
Requirement Answer: U		
Control and monitor user-installed software.		

3.5.1-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Identify information system users, processes acting on behalf of users, or devices.		

3.5.2-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.		

3.5.3-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.		

3.5.4-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.		

3.5.5-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Prevent reuse of identifiers for a defined period.		

3.5.6-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Disable identifiers after a defined period of inactivity.		

3.5.7-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		

Enforce a minimum password complexity and change of characters when new passwords are created.

3.5.8-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Prohibit password reuse for a specified number of generations.		

3.5.9-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Allow temporary password use for system logons with an immediate change to a permanent password.		

3.5.10-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Store and transmit only encrypted representation of passwords.		

3.5.11-Identification And Authentication		Identification and Authentication
Low	0%	SP800-171
Requirement Answer: U		
Obscure feedback of authentication information.		

3.6.1-Incident Response	Incident Response

Low	0%	SP800-171
Requirement Answer: U		
Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.		

3.6.2-Incident Response		Incident Response
Low	0%	SP800-171
Requirement Answer: U		
Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.		

3.6.3-Incident Response		Incident Response
Low	0%	SP800-171
Requirement Answer: U		
Test the organizational incident response capability.		

3.7.1-Maintenance		Maintenance
Low	0%	SP800-171
Requirement Answer: U		
Perform maintenance on organizational information systems.		

3.7.2-Maintenance		Maintenance
Low	0%	SP800-171
Requirement Answer: U		

Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

3.7.3-Maintenance		Maintenance
Low	0%	SP800-171
Requirement Answer: U		
Ensure equipment removed for off-site maintenance is sanitized of any CUI.		

3.7.4-Maintenance		Maintenance
Low	0%	SP800-171
Requirement Answer: U		
Check media containing diagnostic and test programs for malicious code before the media are used in the information system.		

3.7.5-Maintenance		Maintenance
Low	0%	SP800-171
Requirement Answer: U		
Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.		

3.7.6-Maintenance		Maintenance
Low	0%	SP800-171
Requirement Answer: U		
Supervise the maintenance activities of maintenance personnel without required access authorization.		

3.8.1-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		
Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.		

3.8.2-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		
Limit access to CUI on information system media to authorized users.		

3.8.3-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		
Sanitize or destroy information system media containing CUI before disposal or release for reuse.		

3.8.4-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		
Mark media with necessary CUI markings and distribution limitations.		

3.8.5-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		

Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

3.8.6-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		
Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.		

3.8.7-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		
Control the use of removable media on information system components.		

3.8.8-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		
Prohibit the use of portable storage devices when such devices have no identifiable owner.		

3.8.9-Media Protection		Media Protection
Low	0%	SP800-171
Requirement Answer: U		
Protect the confidentiality of backup CUI at storage locations.		

3.9.1-Personnel Security	Personnel Security

Low	0%	SP800-171
Requirement Answer: U		
Screen individuals prior to authorizing access to information systems containing CUI.		

3.9.2-Personnel Security		Personnel Security
Low	0%	SP800-171
Requirement Answer: U		
Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.		

3.10.1-Physical Protection		Physical and Environmental Protection
Low	0%	SP800-171
Requirement Answer: U		
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.		

3.10.2-Physical Protection		Physical and Environmental Protection
Low	0%	SP800-171
Requirement Answer: U		
Protect and monitor the physical facility and support infrastructure for those information systems.		

3.10.3-Physical Protection		Physical and Environmental Protection
Low	0%	SP800-171
Requirement Answer: U		
Escort visitors and monitor visitor activity.		

3.10.4-Physical Protection		Physical and Environmental Protection
Low	0%	SP800-171
Requirement Answer: U		
Maintain audit logs of physical access.		

3.10.5-Physical Protection		Physical and Environmental Protection
Low	0%	SP800-171
Requirement Answer: U		
Control and manage physical access devices.		

3.10.6-Physical Protection		Physical and Environmental Protection
Low	0%	SP800-171
Requirement Answer: U		
Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).		

3.11.1-Risk Assessment		Risk Assessment
Low	0%	SP800-171
Requirement Answer: U		
Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.		

3.11.2-Risk Assessment		Risk Assessment
Low	0%	SP800-171

Requirement Answer: U
Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.

3.11.3-Risk Assessment		Risk Assessment
Low	0%	SP800-171
Requirement Answer: U		
Remediate vulnerabilities in accordance with assessments of risk.		

3.12.1-Security Assessment		Security Assessment and Authorization
Low	0%	SP800-171
Requirement Answer: U		
Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.		

3.12.2-Security Assessment		Security Assessment and Authorization
Low	0%	SP800-171
Requirement Answer: U		
Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.		

3.12.3-Security Assessment		Security Assessment and Authorization
Low	0%	SP800-171
Requirement Answer: U		
Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.		

3.13.1-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.		

3.13.2-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.		

3.13.3-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Separate user functionality from information system management functionality.		

3.13.4-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Prevent unauthorized and unintended information transfer via shared system resources.		

3.13.5-System and Communications Protection	System and Communications Protection

Low	0%	SP800-171
Requirement Answer: U		
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.		

3.13.6-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).		

3.13.7-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.		

3.13.8-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.		

3.13.9-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171

Requirement Answer: U
Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.13.10-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Establish and manage cryptographic keys for cryptography employed in the information system.		

3.13.11-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.		

3.13.12-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.		

3.13.13-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Control and monitor the use of mobile code.		

3.13.14-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.		

3.13.15-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Protect the authenticity of communications sessions.		

3.13.16-System and Communications Protection		System and Communications Protection
Low	0%	SP800-171
Requirement Answer: U		
Protect the confidentiality of CUI at rest.		

3.14.1-System And Information Integrity		System and Information Integrity
Low	0%	SP800-171
Requirement Answer: U		
Identify, report, and correct information and information system flaws in a timely manner.		

3.14.2-System And Information Integrity		System and Information Integrity
Low	0%	SP800-171
Requirement Answer: U		
Provide protection from malicious code at appropriate locations within organizational information systems.		

3.14.3-System And Information Integrity		System and Information Integrity
Low	0%	SP800-171
Requirement Answer: U		
Monitor information system security alerts and advisories and take appropriate actions in response.		

3.14.4-System And Information Integrity		System and Information Integrity
Low	0%	SP800-171
Requirement Answer: U		
Update malicious code protection mechanisms when new releases are available.		

3.14.5-System And Information Integrity		System and Information Integrity
Low	0%	SP800-171
Requirement Answer: U		
Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.		

3.14.6-System And Information Integrity		System and Information Integrity
Low	0%	SP800-171
Requirement Answer: U		
Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.		

3.14.7-System And Information Integrity		System and Information Integrity
Low	0%	SP800-171

Requirement Answer: U
Identify unauthorized use of the information system.