**System and Communications Protection (SC)**

**SC-1: System and Communications Protection Policy and Procedures**

NIST SP 800-53 Objective: The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:

1. System and communications protection policy [Assignment: organization-defined frequency]; and

2. System and communications protection procedures [Assignment: organization-defined frequency].

Control Translation: This control is to ensure that the organization has created system and communications protection policies and procedures that are organizational specific, available to all required personnel, and updated to ensure accuracy and contain specific information regarding the organization.

Notes: The organizational risk management strategy is a key factor in the development of the system and communications protection policy and procedures. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and System and Communications Protection Policy and Procedures. Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency. Ensure system and communications protection policy and procedures are in place, sent to the organization defined personnel, and are updated in accordance with the organization defined time frame.

Technology specific: General

**SC-2: Application Partitioning**

NIST SP 800-53 Objective: The information system separates user functionality (including user interface services) from information system management functionality.

Control Translation: This control is to ensure that users of the component are not able to access administrator accounts or obtain administrator permissions.

Notes: This is mostly tested at the application level. Many testing platforms only have administrators and do not have regular users. In many instances a user will use a graphical user interface (GUI) and an administrator will access components through SSL and SSH.

How to test and evaluate: Obtain a screenshot of the user logon interface and the administrator login interface. Ensure the administrator does not use the same logon interface as the user. Obtain the administrator access control lists (ACLs) and the user ACLs. Review the ACLs to ensure the user does not have administrator permissions.

Technology specific: All components

SC-3: Security Function Isolation

NIST SP 800-53 Objective: The information system isolates security functions from nonsecurity functions.

Control Translation: This control is to ensure that administrators and organizational personnel with security functions and responsibilities are the only personnel able to access the security function settings on components.

Notes: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains). Some examples of security functions are log reviews, account management actions, configuration capabilities, and root access (could be via sudo).

How to test and evaluate: Utilize the component ACL from SC-2 testing. Obtain a screenshots showing how the administrator with security functions accesses the component (usually SSH). This will show that the administrator is forced to logon to perform security functions, the isolation occurs through the ACL use by the component. (There are many ways to test this control, but this the most efficient using pre-obtained information). Use ACLs to validate that privileged functions (including security) are limited to authorized individuals. Validate that administrators are using their administrative accounts only for privileged functions and not for user functions, such as email or internet access.

Technology specific: All components

**SC-4: Information In Shared Resources**

NIST SP 800-53 Objective: The information system prevents unauthorized and unintended information transfer via shared system resources.

Control Translation: This control is to ensure that there is no data leakage when data is stored in one location utilized by multiple users or components.

Notes: This control should be tested at the database and storage are network (SAN) levels where multiple technologies store data. Operating systems that may use servers as shared computing space and the hypervisor that is used to prevent customers from accessing other customer information through the cloud.

How to test and evaluate: This control is most easily tested by performing an actual test. For the hypervisor, obtain permissions to setup two test instances form the client. Once the instances are complete, create dummy data in both instances. Log into instance A and attempt to access instance B data. Then log into instance B and attempt to access instance A data. For the database and SAN, sit with an administrator and try to access data within the database the administrator does not have access. For example, the administrator for RHEL may not have access to Windows data. For the operating systems, many servers share multiple functions and one physical server may be segregated and run multiple operating systems. See if the administrator can access data that is on a shared box that the administrator should not have access. (This will require some research on methods to preform these action. Bring the research for the test.)

Technology specific: Databases, SAN, operating systems, hypervisors

**SC-5: Denial of Service**

NIST SP 800-53 Objective: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].

Control Translation: This control is to ensure that the client has prepared for potential attempts at creating denial of service activity in the client environment.

How to test and evaluate: Examined the organizational and component level policies to determine the types of denial of service attacks the organization has prepared and the safeguards created for the attacks. The organizational firewalls, intrusion detection systems (IS), and intrusion prevention systems (IPS) will be configured to spot the attempts and to prevent them. Make sure that the firewalls, IDS, and IPS devices are configured as stated in the policy. Obtain 5 total tickets to show the actions that occurred when denial of service attempts were found.

Technology specific: Firewalls, IDS, IPS

**SC-7: Boundary Protection**

NIST SP 800-53 Objective: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Control Translation: This control is to ensure that the communication to and from the organizational network is done so in a secure manner.

How to test and evaluate: The best option is to obtain running configuration files for the selected sample of firewalls, routers, switches, and load balancers. Review the firewall configuration looking for signature updates and proper processing of packets with the signatures. Review the load balancers looking for configurations that move traffic across the environment without overwhelming the network. Review the routers and switches looking for configurations for managed access points to ensure all traffic is routed through specific routers and switches both external and internally to the network.

Technology specific: Firewalls, Routers, Switches, Load Balancers

**SC-8: Transmission Confidentiality And Integrity**

NIST SP 800-53 Objective: The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.

Control Translation: This control is to ensure that the component transmitted information is un-alterable and only able to viewed by intended parties.

How to test and evaluate: Obtain the screenshot from the selected testing sample for each unique component that shows the configuration used to encrypt the communication from the component. Most likely the component will use a hashing algorithm (i.e. SHA-1 or MD5) and an encryption mechanism (i.e. AES-256).

Technology specific: All Components

**SC-10: Network Disconnect**

NIST SP 800-53 Objective: The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

Control Translation: This control is to ensure that the network sessions are not established for an indefinite period of time. This control also ensures that unused network connections are dropped after a certain period of time.

How to test and evaluate: Examine the organizational and component level policies to determine the time frame defined for dropping a network session after inactivity. Obtain a screenshot from the component detailing the time frame for dropping the network connection after the defined period of inactivity. This may not be managed at the component level. Also test the setting, by having the administrator connect to the network and then leave the session idle. One minute after the required time frame, have the administrator attempt to perform activity utilizing the network. Capture screenshot to show the time frame associate with the start of no activity and the time frame when activity was resumed for testing.

Technology specific: All Components

**SC-12: Cryptographic Key Establishment And Management**

NIST SP 800-53 Objective: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

Control Translation: This control is to ensure that the organization has defined and utilizes a Certification Authority (CA) for creating and managing cryptographic keys within the environment.

How to test and evaluate: Examine the organizational and component level policies to determine the requirements for key generation, distribution, storage, access, and destruction. Obtain screenshots from the CA to detail how all of the requirements are being met. Tickets may also need to be used to show the required activities have occurred.

Technology specific: Technology used for managing keys

**SC-13: Cryptographic Protection**

NIST SP 800-53 Objective: The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Control Translation: This control is to ensure that each component is using the required cryptographic mechanisms to protect the confidentiality, availability, and integrity of the data and technology. Also, to ensure the mechanisms being used are of sufficient strength.

How to test and evaluate: Examine the organizational and component level policies to determine the required cryptographic mechanism to be utilized for each component. Utilize the screenshot(s) from SC-8. Obtain a screenshot to encryption or cryptography and the storage level of the component. Compare all mechanisms to the FIPS standards to ensure FIPS validation and compliance. Take screenshots from the FIPS website to prove verification. (There are many ways to test this control, but this is a quick and easy manner for testing.)

Technology specific: All components

**SC-15: Collaborative Computing Devices**

NIST SP 800-53 Objective: The information system:

a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and

b. Provides an explicit indication of use to users physically present at the devices.

Control Translation: This control is to ensure that only authorized remote access to user devices occurs. Additionally, ensure that remote activation of collaborative devices such as cameras and microphones is disabled.

Notes: This control mostly applies to workstation users that need assistance from a help desk or system administrator.

How to test and evaluate: Examine the organizational and component level policies to determine the exceptions where remote activation is allowed. Most components will be accessed non-locally via VPN, SSL, or SSH. Ensure this is stated within an organization or component level policy. If need be, obtain evidence to show that an explanation was provided to the user present at the device. The explanation should be in an email or a ticket.

Technology specific: All components

**SC-17: Public Key Infrastructure Certificates**

NIST SP 800-53 Objective: The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

Control Translation: This control is to ensure that only authorized public key (PKI) certificates used within the organization are obtained from an approved service provider.

How to test and evaluate: Examine the organizational and component level policies to determine the policy for issuing PKI certificates and the approved service provider. Utilize the screenshots from the testing of control SC-12 to show that the certificates issued are secure and from the approved CA. (This will only apply if the CA issues PKI certificates.) If the certificates are only used internally, then self signed certificates are permissible. If the CA does not issue PKI certificates, obtain screenshots from the PKI CA to show the proper issuance and securing of the PKI certificates.

Technology specific: General

**SC-18: Mobile Code**

NIST SP 800-53 Objective: The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;

b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorizes, monitors, and controls the use of mobile code within the information system.

Control Translation: This control is to ensure that only authorized mobile code technologies are using in the environment.

Notes: Mobile code is an easy way to introduce malicious content into an environment. This control is to mitigate the dangers surrounding mobile code. Java is the most widely used mobile code.

How to test and evaluate: Examine the organizational and component level policies to determine the acceptable and unacceptable mobile code technologies to be used in the environment; and the mobile code usage guidance (how is to be used). Obtain logs from each component. Obtain the review of the logs to show that unusual activity is monitored. Ensure the mobile code activity is records in the logs.

Technology specific: All components

**SC-19: Voice Over Internet Protocol (VoIP)**

NIST SP 800-53 Objective: The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Control Translation: This control is to ensure that the VoIP technology in the environment is secure and properly configured.

Notes: This control only applies to organization that utilize VoIP.

How to test and evaluate: Examine the organizational and component level policies to determine the usage restrictions and guidance for VoIP in the environment looking specifically for means to ensure the VoIP can’t be used in malicious manner. Obtain logs from the VoIP system. Obtain reviews of the VoIP logs to show that the VoIP devices are being monitored for unusual and malicious activity. Obtain the ticket or authorization document allowing for the VoIP technology to be utilized in the environment.

Technology specific: General

**SC-20: SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**

NIST SP 800-53 Objective: The information system:

a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Control Translation: This control is to ensure that the DNS servers are working properly and routing traffic as intended.

How to test and evaluate: Obtain the running configurations from the selected sample of unique boundary network devices. Review the configuration looking for the information added to the packets to determine where the packet originated and the final destination.

Technology specific: Boundary Network Devices

**SC-21: SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**

NIST SP 800-53 Objective: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Control Translation: This control is to ensure that the DNS servers are working properly and routing traffic as intended.

How to test and evaluate: Obtain the running configurations from the selected sample of unique boundary network devices. Review the configuration looking for the information added to the packets to determine where the packet originated and if that packet is from an authoritative source.

Technology specific: Boundary Network Devices

**SC-22: ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE**

NIST SP 800-53 Objective: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Control Translation: This control is to ensure that the DNS servers are working properly and routing traffic as intended.

Notes: To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network.

How to test and evaluate: Obtain the running configurations from the selected sample of unique boundary network devices. Review the ACL on the sample selected components to determine that developers do not have production level access enforcing role separation. Review the inventory and network diagrams to verify there are redundant authoritative DNS servers. Ensure that the primary DNS server has a backup to be used in the event an issue occurs on the primary server. Obtain tickets to show the use of the backup when an issue occurred to prove that the backup DNS server works as intended.

Technology specific: Boundary Network Devices

**SC-23: Session Authenticity**

NIST SP 800-53 Objective: The information system protects the authenticity of communications sessions.

Control Translation: This control is to ensure session communications for each component are authentic and have not been altered.

Notes: This control addresses communications protection at the session, versus packet level.

How to test and evaluate: Obtain a screenshot showing the session communication encryption mechanisms to protect the authenticity and CIA (confidentiality, integrity, availability) of the communication between the component and the user/administrator. For web based applications this will probably be HTTPS and for SSH connections this will probably be SSL. The screenshot should show the encryption mechanism used by HTTPS and SSL or the means used by the component (certificate details).

Technology specific: All components

**SC-24: Fail In Known State**

NIST SP 800-53 Objective: The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.

Control Translation: This control is to ensure that in the event of component level failure, the component fails to the last known secure state.

How to test and evaluate: Examine the organizational and component level policies to determine identify the known state the component is to fail. Examine the organizational and component level policies to determine the issues that will cause the component to fail to the known state. Examine the organizational and component level policies to determine the information that must be preserved when failing to the known state. This control is difficult test. We can’t cause the component to fail and test to ensure proper usage. If possible, obtain a ticket to show the actions that occurred when the component failed. Review the contingency plan and incident response tests to determine if this was covered during the last test. Lastly, review the running configurations looking specifically for configuration items that will detail the known state in the event of an issue.

Technology specific: All components

**SC-28: Protection Of Information At Rest**

NIST SP 800-53 Objective: The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].

Control Translation: This control is to ensure that information stored on the component is encrypted.

How to test and evaluate: Examine the organizational and component level policies to determine the information stored on the component that is to be protected (usually with encryption). Utilize the information obtained during SC-13 testing to show the type of encryption used by the component to protect data stored on the component. This is most often hashing such as MD4, SHA1, or some flavor of SHA.

Technology specific: All components

**SC-39: Process Isolation**

NIST SP 800-53 Objective: The information system maintains a separate execution domain for each executing process.

Control Translation: This control is to ensure that each component has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces.

How to test and evaluate: Obtain running configurations from each selected unique component containing the host name and IP address. Use this information to ensure that each unique component as a separate computing space for each process. This will prevent one process negatively impacting another process.

Technology specific: All components