Draft for Discussion

The attached technical requirements for continuous monitoring and cloud boundary defense serve as a proposed path forward for implementing federal information systems and cloud cybersecurity.

This draft is for discussion purposes only. Under a separate process at a later date, comments regarding technical requirements will be requested from industry.

The release of these draft requirements does not constitute an invitation for bids or a request for proposal, and is not a commitment by the U.S. Government to enter into any acquisition for any products or services. No solicitation document exists at this time.

These draft requirements are subject to change.

Continuous Monitoring
Performance Work Statements

1 Performance Work Statement (PWS) for Tools Supporting the Hardware[1] Inventory Management Function

This PWS describes the objectives of continuous monitoring and risk scoring for tools2 providing diagnostics for supporting hardware inventory management; the mission need for this function; the operational assumptions and operational concept guiding the adoption of this function; and the operational and functional tool requirements.

1.1 Function Statement of Objectives (SOO)

The **objective of the hardware inventory management function** is to discover and remove unauthorized or unmanaged hardware on a network. Since unauthorized hardware is unmanaged, it is likely vulnerable and will be exploited as a pivot to other assets if not removed or managed.[3]

1.2 Function Mission Needs Statement (MNS)

To perform this function, federal departments and agencies (D/As) need processes, supported by automated reporting and analysis tools, for the ability to:

HWAM-MNS-1:[4] Create, operate, and maintain an authorized hardware inventory baseline, unique identifiers for hardware, and other properties such as the manager of the hardware.

1. The process for generating the authorized hardware inventory baseline must be established, operated, and maintained in environments that are already in operation, using D/A-defined business rules.
2. It should not be assumed that D/A property management functions will significantly assist the process for generating the authorized hardware inventory baseline, but where property management systems are available, they should be considered as sources of input for the authorized hardware inventory baseline.
3. The authorized hardware inventory baseline generated by this process must be complete, accurate, and timely.

HWAM-MNS-2: Create, operate, and maintain the actual inventory of authorized and unmanaged hardware in near-real time, along with information needed to assess the risk to and physically locate the hardware.

1. This inventory should be updated regularly with automated hardware discovery processes and tool(s).
2. The actual inventory data generated by this process must be complete, accurate, and timely.

HWAM-MNS-3: Determine the difference between the authorized hardware inventory baseline and the actual hardware inventory. Differences include both missing and extra devices.

HWAM-MNS-4: Assign risk to each difference (between the authorized hardware inventory baseline and the actual hardware inventory) based on relevant factors.

---

[1] The terms hardware and hardware devices always refer to both physical and virtual "devices" herein. Unless specifically stated otherwise, the terms refer to either IP addressable devices and/or USB devices, but not other devices.

[2] Tools are also referred to as products herein.

[3] SANS Institute, *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)*, Version 3.1, October 3, 2011. (http://www.sans.org/critical-security-controls/)

[4] Mission Needs Statement requirements for hardware asset management have the naming convention: HWAM-MNS-*(unique ID)*

HWAM-MNS-5: Assign the hardware for management and disposition (i.e., authorization to connect to or be removed from the network) manually or automatically, according to D/A-defined business rules.
HWAM-MNS-6: When differences between the authorized hardware inventory baseline and the actual hardware inventory are detected, then:[5]

1. when the difference identifies unauthorized hardware devices, either remove or authorize such hardware promptly, and
2. when the difference indicates authorized hardware that is missing in operation, bring the hardware back into operation promptly, record its non-operational status (with rationale), or de-authorize the hardware.

1.3 Function Operational Assumptions and Constraints

At a minimum, these inventories must cover addressable network hardware (as defined in FY2012 CIO FISMA reporting guidance) and should cover Universal Serial Bus (USB) removable hardware. The process for establishing the authorized hardware inventory and the actual hardware inventory is needed by both small and large D/As, ranging from several hundred users to millions of users. Large D/As may have multiple enclaves and may want to operate the hardware inventory at the enclave level. Ultimately the government seeks to summarize the data up to and including the federal level, which includes all civilian executive D/As.

It is assumed that such a hardware inventory management function must be largely automated to be effective, timely, and efficient. The authorized hardware inventory baseline is established through some process involving actual inventory data and business rules that allow assignment of default responsibility. Data in the authorized hardware inventory baseline should be validated continuously through automated hardware discovery. Manual processes, such as assigning hardware to the baseline, are expected to integrate with and be supported by automated processes.

1.4 Illustration of Function Operational Concept

The government has identified the following technical approaches and/or operational concepts in the market as acceptable ways to meet the objectives of the hardware inventory management tools. The government is open to other innovative, effective, and efficient ways of achieving these objectives, but offers these suggestions to help clarify the objectives and some of the issues to be addressed.

1. Creating the initial authorized hardware inventory baseline by building on existing inventories and business rules to create default (approximate) assignment, such as:
    a. property systems,
    b. tools such as Active Directory and /or Cisco Works,
    c. Internet Protocol (IP) range assignment to specific managers/Local Area Networks (LANs), and
    d. naming conventions.
2. Maintaining and updating the authorized hardware inventory baseline to include supporting a business process to assign unassigned hardware, reassigning mis-assigned hardware, and changing the state from unauthorized to authorized:
    a. when responsibility changes,
    b. before new hardware is added, or
    c. when people identify exceptions to default assignment.

The capability to maintain and update the authorized inventory needs to allow for decentralized administration of hardware authorization, using appropriate access and audit controls to ensure that only

[5] This mission need is part of the hardware asset management function, but not required for tools supporting this function. However, the purpose of the tool is to find the differences described here, so that they can be addressed.

authorized personnel can modify authorized inventories and only for assets for which they are accountable.

3. Obtaining the actual hardware inventory through:
    a. Active methods such as:
        i. IP scanning,
        ii. switch interrogation, and
        iii. traceroute.
    b. Passive methods such as:
        i. switch reporting triggered by events like hardware connecting/disconnecting,
        ii. Dynamic Host Configuration Protocol (DHCP) device reporting, and
        iii. packet inspection.
4. Computing differences between the authorized hardware inventory baseline and the actual hardware inventory by ensuring that there are compatible identifiers in place to enable a set comparison between the authorized hardware inventory baseline and actual hardware inventory, avoiding false positives and false negatives.
5. Meeting Security Content Automation Protocol (SCAP) and relational requirements for interoperability of reporting (dashboard, query, etc.).
    a. If the tool doesn't have a relational database (DB), extract the data to a provided relational DB.
    b. If the tool doesn't support SCAP, use a program provided by the government to convert the relational data to SCAP.
    c. If the tool only supports SCAP, use a tool provided by the government to convert the SCAP data to a relational DB.

1.5 Operational[6] and Functional[7] Requirements for Hardware Inventory Management Tools

In this document, the terms must, shall, should, and may are degree modifiers that indicate the the importance of compliance mandated by the requirement. The following conventions are used:

- Must – Compliance with the requirement in its stated form is mandatory.
- Shall – Compliance with the requirement is mandatory unless an explicit contractual waiver is granted by the contracting agency.
- Should – Compliance with the requirement is highly valued and may be mandatory in the future but is not mandatory now.
- May – Compliance with the requirement is optional. The requirement is a desireable additional feature that may be used by contracting agencies to determine best value to the government.

Where requirements of different degree of compliance are nested, the top level degree applies to the top level requirement, and the lower level modifiers indicate the degrees of compliance that apply to the lower level nested requirements.

The contractor shall provide tool(s) that enable the D/A to identify and track authorized and unauthorized hardware within the network in an efficient, accurate, complete, and timely manner.

HWAM-OP-1: Know the Desired State.
The product [must] record which hardware devices (physical and virtual) are authorized to be on the network, and who (by individual, access group, or organization) manages each device. (Implements HWAM-MNS-1.)

[6] Operational requirements for hardware asset management have the naming convention: HWAM-OP-HWAM-*(unique ID)*

[7] Functional requirements for hardware asset management have the naming convention: HWAM-F-(OP-ID).*(unique ID)*

1. This data will be used to know who is responsible for the following kinds of security attributes to each device (including but not limited to):
    a. installed software,
    b. device and installed software configuration,
    c. installed software vulnerability management (patching), and
    d. maintenance of required network boundary controls (where applicable) including (but not limited to):
        i. appropriate connection of the device to the network, and
        ii. appropriate encryption of device data stores and/or data set over connections.
2. This data will identify devices that are not being managed (unauthorized devices), and which are thus likely to be more easily controlled by attackers and used as a pivot point to attack the rest of the network.
    a. This data needs to be timely enough to find and take action on unauthorized devices significantly faster than attackers can find and exploit the devices. find and exploit the unauthorized software. In this context, "significantly faster" means creating a high probability (notionally ninety percent or greater) that unauthorized software will be discovered by the tool before an attacker would be expected to find and exploit it.
3. Ideally this data needs to be complete enough to cover all devices on the network. While identifying absolutely every hardware device on the network is practically impossible, the government's objective is to minimize uncovered hardware devices.
4. While it would be desirable to cover standalone devices, there does not seem to be a feasible automated way to do this in practice. Solutions are sought but not required.

The product is required to satisfy the following functional requirements to the degree specified to support HWAM-OP-1:

HWAM-F-1.1: Document and record authorized hardware inventory information, including, but not limited to the following key elements:

a. [must] Data to enable people to easily identify the device on the network. This data will include:
    i. [must] device type (e.g., router, workstation, firewall, printer) to help predict appropriate device behavior,
    ii. [must] device connections to help determine whether unauthorized connections exist,
    iii. [must] IP address,
    iv. [must] physical location,
    v. [shall] MAC address,
    vi. [may] machine name,
    vii. [may] manufacturer,
    viii. [may] model, and
    ix. [may] serial number.
b. [must] Data to enable the system to match "authorized" devices to actual devices. The data used may vary by vendor.
c. [must] Data to describe the impact of a compromise to the system as an impact score on a scale to be defined by the government.
d. [must] Data to record who is responsible for the device, including but not limited to the service provider: (Implements HWAM-MNS-5.)
    i. organization,
    ii. location, and
    iii. contact information.
e. [must] Operational status:
    i. to be added,
    ii. active,
    iii. disposed, and

iv. inactive (not-disposed) including:
- in-transit,
- missing, and
- other.

f. [may] Property management information:
i. property barcode (a.k.a. asset tag),
ii. property owner, organization, location, and contact information,
iii. property user, organization, location, and contact information;
iv. acquisition date, and
v. most recent physical inventory date.

HWAM-F-1.2: [must] Allow manual or batch creation of authorized device data.

a. Users [must] be able to manually:
i. create device records,
ii. update device record, and
iii. delete device records.
b. The system [must] record and process decision rules (decision support) to assign device attributes based on:
i. [shall] data collected from the actual inventory system,
ii. [shall] data received from other sources (such as device LDAP systems and property management systems). For example, this might include assigning responsibility by OUs from Active Directory,
iii. [shall] rules provided by the D/A (such as IP range assignments), and
iv. [may] other methods offered by the vendor to automate populating the authorized inventory.

HWAM-F-1.3: [may] Support other property management functions:

a. [may] Permit authorized users to perform manual entry for recording of disconnected or isolated hardware.
b. [may] Offer other property management support capabilities.

HWAM-OP-2: Know the Actual State.

The product [must] discover hardware devices (physical or virtual) actually on the network, whether authorized or not, and whether configured to cooperate with detection or not. (Implements HWAM-MNS-2.)

1. This data will ultimately be used for comparison to the authorized inventory described above to identify differences between the actual and authorized inventory, including but not limited to:
   a. authorized devices which are not on the network, and
   b. unauthorized (and/or unmanaged) devices which are on the network.
2. For this to be achieved, the means used to discover actual inventory [must] not require that the devices are configured to report correctly. This is because unauthorized devices are likely to be poorly configured, and in some cases may be configured to obscure their presence.
   a. Given this, it [may] be necessary to use a combination of both passive and active detection techniques to provide a reliable enumeration of all devices.
3. For this to be achieved, the actual inventory data collected [must] include data necessary to do the following for both unauthorized and authorized devices:
   a. [must] Reliably match (matching primary keys) the authorized inventory data.
   b. [must] Enable people to locate any identified unauthorized devices on the network. (For example, the authorized device which the unauthorized device uses to connect to the network might be indicated.)

4. For authorized devices which are properly configured, the product [shall] collect significant additional data to automatically fill-in (or validate) the authorized inventory data for these devices.

The product is required to satisfy the following functional requirements to the degree specified to support HWAM-OP-2:

HWAM-F-2.1: [must] Discover authorized (managed) and unauthorized (unmanaged) hardware within the boundaries of the network:

a. [must] without regard to whether or not the hardware is properly configured
b. [must] without requiring knowledge of authentication credentials,
c. [must] significantly faster (as defined above) than attackers can find and exploit unauthorized devices,
d. [must] at user-defined intervals and on demand,
e. [must] detect all IP addressable device types,
f. [must] have a false positive/negative rate below 0.1%,[8]
g. [must] limit the burden put on network resources such that (1) the presence of the scan is not noticeable above background variation in network bandwidth and (2) completeness and timeliness goals in HWAM-OP-1 can be met, and
h. [shall] detect all IP addressable devices,
i. [shall] detect all IP addressable devices,
j. [should] detect all USB devices device types, and
k. [should] detect all USB devices.

HWAM-F-2.2: [must] Collect appropriate data to match actual to authorized inventory such that the mapping is:

a. [must] reliable (repeatable), such that the same test run on the same network state produces the same results,
b. [must] valid/accurate (false positive/negative rate below 0.1%),
c. [must] timely (as defined above) ,
d. [must] record when hardware devices are detected and when they were authorized or unauthorized, to enable accurate identification of risks by associating risk conditions (i.e., the presence of unauthorized hardware or absence of authorized hardware) under asynchronous conditions..

HWAM-F-2.3: [must] Collect adequate data to enable people to locate the hardware devices easily on the network.

a. [must] Provide adequate data to do this.
b. [may] Provide network maps and/or identify connections between devices in table form.
c. [may] Provide other means to achieve this objective.

HWAM-F-2.4: For properly configured devices and with credentials, the product [must] collect additional data to validate data in the actual inventory. The government will evaluate tools on the extent and value of the additional data to both network security (first priority) and operations (second priority).

HWAM-F-2.5: [must] Detect the types of each hardware device, based upon its behavior.

HWAM-F-2.6: [shall] Conduct detection of hardware inventory according to a D/A-defined schedule, on a D/A defined event-driven basis, and on an unscheduled ad hoc basis.

HWAM-F-2.7: [shall] Ensure that only authorized users can schedule detection of actual hardware inventory.

HWAM-F-2.8: [may] Provide, on demand or on a periodic basis, a validation questionnaire to authorized users of hardware for verifying hardware inventory information (i.e., property management information).

[8] A false positive is a report of software assets that do not exist. A false negative is a failure to report actual software that does exist.

HWAM-OP-3: Know the Differences (Between Actual and Desired States) and Automatically Act on the Differences.

The product [must] compute difference between the authorized and actual inventory, so that the differences can be addressed. (Implements HWAM-MNS-3.)

The product is required to satisfy the following functional requirements to the degree specified to support HWAM-OP-3:

HWAM-F-3.1: [must] Identify unauthorized hardware devices (physical and virtual) in the actual hardware inventory.

a. [must] Do this using the data collected under HWAM-OP-1 and HWAM-OP-2.
b. [must] Do this automatically and within ten seconds of detection.

HWAM-F-3.2: For properly configured devices in the authorized inventory, the product:

a. [must] assess and validate as much data in the authorized hardware inventory as technically possible, as indicated by capability demonstrated by available COTS products available on the market.
b. [must] Flag devices in authorized inventory that do not appear present in the actual inventory including date last seen.

HWAM-F-3.3: [must] Trigger e-mail notifications and application programming interface (API) notices to the dashboard:

a. when differences are first found,
b. at set times after found, if not resolved, and
c. when discovered to be resolved.

HWAM-OP-4: Group Items Found for Reporting.

Report authorized and actual hardware devices by category (when such data has been entered manually or detected by the system):

1. This data will be sent to the dashboard, to enable displays of devices and their other attributes, (such as software, configurations, vulnerabilities, and connections) to be reported by categories such as, but not limited to:

a. FIPS and/or CNSSI-1253 impact/security categories,
b. approved classification ceiling,
c. system type (GSS or Major Application),
d. FISMA reportable system,
e. LAN location,
f. supported business organizations,
g. supported business functions, and
h. other categories, to be determined by D/As on an ad hoc basis.

2. The product [must] Record any or all of these categories for each hardware device.
3. The product [must] enforce a user-defined cardinality for each category type (single or multi-valued).
4. The product [must] provide an appropriate interface integrated with the basic inventory screens to allow entering, updating, and deleting these categories.
5. The authorized inventory GUI [must] display unauthorized devices so that they can be authorized and/or have the categories (described in HWAM-OP-4 number 1) applied to them.
6. As described in HWAM-OP-1, there [must] be a mechanism to batch update these attributes with data from other sources.

The product is required to satisfy the following functional requirements to the degree specified to support HWAM-OP-4:

HWAM-F-4.1: The product [must] be configurable to record any number of hierarchical categories (attributes) by which the hardware devices may be described.

a. DHS [must] be able to configure such categories as needed to support dashboard operations and central reporting.
b. The D/A [must] be able to configure additional categories needed to support D/A operational concepts.
c. The configuration of categories [must] support:
    i. limitation of values to defined domain,
    ii. required and optional value, and
    iii. either limitation to single valued attributes or inclusion of multiple values.
d. Provide a GUI interface for the application of these categories integrated into the tool's interface.

HWAM-F-4.2: The product [must] assign any of these categories to each hardware device.

HWAM-OP-5: Interoperate.

Share data with other components (discovery tools, dashboard, network asset systems [e.g., Active Directory and other LDAP-like systems], property management systems, and OCIL questionnaire systems).

1. Data shared will be used, for example, in the following ways:
    a. In all cases, data about assets, authorized and unauthorized will need to be sent to the central dashboard.
    b. When the HWAM tool discovers new hardware, the tools for software inventory, configuration, and vulnerability/patch management [should] be notified to allow them to further assess that hardware.
    c. Data from LDAP tools and property management system [may] be used to prepopulate the authorized inventory.
    d. Data from the actual inventory [may] be used to validate the attributes of authorized devices.
    e. Data from the authorized and actual inventory [may] be used to create questionnaires for hardware managers and/or users to check inventory data.
    f. Data from such checks [may] be fed back into the inventory system to update authorized inventory data.

The product is required to satisfy the following functional requirements to the degree specified to support HWAM-OP-5:

HWAM-F-5.1: Provide the hardware inventory data in a standard interface (i.e., communicate to the central dashboard and other components).

a. [should] Using XML based SCAP standard parameters, the product:
    i. [must] use a relational data structure,
    ii. [should] use NIST-specified open standards to express and communicate hardware inventory information such as: Asset Summary Report (ASR) protocol (an emerging specification); Asset Identification (AI) protocol, version 1.1 or later; or Common Platform Enumeration (CPE™) version 2.3 or later,
        - Data describing HWCI/SWCI[9] [should] use the CPE™ version 2.3 or later standard.
        - If it uses CPE™, at a minimum it [should] contain the following structure: cpe:/ {part} : {vendor} : {product} : {version} : {update} : {edition} : {language} : {sw_edition} : {target_sw} : {target_hw} : {other}

[9] References to Software Configuration Items (SWCI) have been included in Hardware Inventory Management functions. Some attributes of Hardware may include Operating System or other SWCI.

iii. [should] process hardware inventory data and distribute them using the CPE™ standard version 2.3 or later,
iv. [may] permit authorized users to create D/A-specific CPE™ definitions, and
v. [may] process and distribute questionnaire responses using the OCIL standard version 2.0 or later.

HWAM-F-5.2: Receive relevant hardware inventory data in a standard interface (i.e., communicate to the central dashboard and other components):

a. [must] using a relational data structure, and
b. [should] using XML-based SCAP standard parameters (as described above).

HWAM-OP-6: Scale.

The product is required to satisfy the following functional requirements to support operations at the scale of federal networks:

HWAM-F-6.1: [must] Scale to federal networks (networks with over 1,000,000 devices) while maintaining adequate timeliness, completeness, and accuracy, as defined above.

HWAM-OP-7: Secure Data Collected.

The tools [shall] adequately protect tool components and data during collection, storage, and transmission to other sources.

The product is required to satisfy the following functional requirements to the degree specified to support HWAM-OP-7:

HWAM-F-7.1: Data [must] be encrypted with adequate methods while in motion (to prevent network sniffers from collecting the inventory data) and while at rest (to prevent exfiltration from data stores).

HWAM-F-7.2: [must] Provide access controls for system functions that supports both centralized and decentralized:

a. administration of the tools,
b. scheduling detection,
c. viewing of the data,
d. transmission of the data, and
e. other functions described herein.

HWAM-F-7.3: [must] Operate within a suitable generic enclave (firewall, etc.) to be designed by the integration contractor.

HWAM-F-7.4: [must] Provide supply chain verification for tool components, such as, but not limited to, digital fingerprints for each software file used in the system, tied to specific product versions and patch levels.

HWAM-F-7.5: The product [shall] assign authorized users to hierarchically-defined "groups."

a. The product [shall] control access by user group.
b. The product [shall] control access based on combinations of user groups.

HWAM-OP-8: Additional Capabilities.

The tools [may] support related data analysis and business functional requirements that are not included in the security requirements listed above. These capabilities [should] be reported by the vendor, and will be evaluated to break ties among products relative to security requirements.

The product [may] satisfy the following functional requirements to the degree specified to support HWAM-OP-8:

HWAM-F-8.1: Dashboard/interface capabilities that allows D/As to get better/additional value from the data. For example, this might include:

a. network design,
b. network mapping,
c. trend analysis,; and

d. compliance reporting.

HWAM-F-8.2: Integrated property management functions that might allow D/As to perform property management without purchasing a separate system. For example, this might include:

a. hardware device sub-component (configuration item) tracking,;
b. purchasing/disposal details,
c. maintenance management,
d. license management,and
e. physical inventory preparation/reporting.

HWAM-F-8.3: Assign Risk to the differences found between the authorized and actual inventory. (Implements HWAM-MNS-4, which is normally performed by the central dashboard.)

Detailed guidance on creating hardware inventory that could meet these requirements are available at http://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf. This document shall be considered as advisory only and does not constitute additional operational or functional requirements.

2 Performance Work Statement (PWS) for Tools Supporting the Software Inventory Management Function

This PWS describes the objectives of continuous monitoring and risk scoring for tools providing diagnostics for supporting software inventory management; the mission need for this function; the operational assumptions and operational concept guiding the adoption of this function; and operational and functional tool requirements.

2.1 Function Statement of Objectives (SOO)

The **objective of the software inventory management function** is to discover and remove unauthorized or unmanaged software configuration items (SWCI) in IT assets on a network. Because unauthorized software is unmanaged, it is probably vulnerable to being exploited as a pivot to other IT assets if not removed or managed.[10] In addition, a complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings; malware often exploits vulnerabilities to gain unauthorized access to and tamper with software and configuration settings to propagate itself throughout the enterprise.

2.2 Function Mission Needs Statement (MNS)

To perform this function, processes are needed to:

SWAM-MNS-1:[11] Create, operate, and maintain an authorized software inventory, unique identifiers for software, and other properties such as the manager of the software.

1. The process for generating the authorized software inventory baseline must be established, operated, and maintained in environments that are already in operation, using department and agency (D/A)-defined business rules.
2. It should not be assumed that D/A property management functions will significantly assist the process for generating the authorized software inventory baseline, but where property management systems are available, they should be considered as sources of input for the authorized software inventory baseline.
3. The authorized software inventory baseline generated by this process must be complete, accurate, and timely.

SWAM-MNS-2: Create, operate, and maintain the actual inventory of authorized and unauthorized SWCIs in near-real time, along with information needed to assess the risk to and physically locate the SWCIs.

1. This inventory should be updated regularly with automated software discovery processes and tool(s).
2. The actual inventory data generated by this process must be complete, accurate, and timely.

SWAM-MNS-3: Determine the difference between the authorized software inventory baseline and the actual software inventory.

SWAM-MNS-4: Assign risk to each difference (between the authorized software inventory baseline and the actual software inventory) based on relevant factors.

SWAM-MNS-5: Assign the software for management and disposition (i.e., authorization for software to operate on, or be removed from, the network) manually or automatically, according to D/A-defined business rules.

SWAM-MNS-6: Fix or disposition software when differences between the authorized software inventory baseline and the actual software inventory are detected.[12]

---

[10] SANS Institute, *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)*, Version 3.1, October 3, 2011. (http://www.sans.org/critical-security-controls/)

[11] Mission Needs Statement requirements for software inventory management have the naming convention: SWAM-MNS-*(unique ID)*

2.3 Function Operational Assumptions and Constraints

At a minimum, these inventories must cover addressable network assets (as defined in the FY2012 CIO FISMA reporting guidance). The process for establishing the authorized software inventory and the actual software inventory is needed by both small and large D/As, ranging from several hundred users to millions of users. Large D/As may have multiple enclaves and may want to operate the software inventory at the enclave level. Ultimately the government seeks to summarize the data up to and including the federal level, which includes all civilian executive D/As.

It is assumed that such a software inventory management function must be largely automated to be effective, timely, and efficient. The authorized software inventory baseline is established through some process involving actual inventory data and business rules that determine assignment of default responsibility. Data in the authorized software inventory baseline should be validated continuously through automated software discovery. Manual processes, such as assigning software to the baseline, are expected to integrate with and be supported by automated processes.

In the specification below, the following definitions are used:

1) A Software Component is an individual executable file. A single software component may be part of more than one software product.
2) A Software Product (also referred to as a SWCI) is a set of all software component files within a specific software release at the vendor, name, version, and update level of detail.

2.4 Illustration of Functional Operational Concept

The government has identified the following technical approaches and operational concepts in the market as acceptable ways to meet the objectives of software inventory management. The government is open to other innovative, effective, and efficient ways of achieving these objectives, but offers these suggestions to help clarify the objectives and some of the issues to be addressed.

1. Creating the initial authorized software inventory baseline by building on existing inventories and business rules to create default (approximate) assignment, such as:
    a. Configuration Management Database (CMDB) Systems,
    b. add-remove-programs like utilities,
    c. registry entries, or
    d. naming conventions.
2. Updating the authorized software inventory baseline to include supporting a business process to assign unassigned software, reassigning mis-assigned software, and changing the state from unauthorized to authorized:
    a. when responsibility changes,
    b. before new software is added, or
    c. when people identify exceptions to default assignment.

The capability to maintain and update the authorized inventory needs to enable decentralized administration of software authorization, using appropriate access and audit controls to ensure that only authorized personnel can modify authorized inventories and only for software for which they are accountable.

3. Obtaining the actual software inventory through:
    a. Active methods, such as:
        i. agent-based software inventory management, and
        ii. systematic search through all disk files.
    b. Passive methods, such as

[12] This mission need is part of the software inventory management function, but not required for tools supporting this function.

i. Nmap-based or Nmap-like passive scans (e.g., port listening/packet sniffing).

4. Identifying software components at the executable level (exe, dll, etc.) and:
    a. Identify the software components by their digital fingerprint, name, and location.
    b. Determine whether the software component has been altered (based on changed fingerprint).
    c. Correlate the individual software component to the larger software product(s), version(s), and update level(s) of which it is part.
    d. Identify any software component that is missing from or extra to a software product.
    e. Identify software products that are not listed in a registry.
    f. Identity executables hidden in other file types.
5. Computing differences between the authorized software inventory baseline and the actual software inventory by ensuring that there are compatible identifiers in place to enable a set comparison between the authorized software inventory baseline and actual software inventory, avoiding false positives and false negatives.
6. Meeting Security Content Automation Protocol (SCAP) and relational requirements for interoperability of reporting (dashboard, query, etc.).
    a. If the tool doesn't make asset inventory data available in a relational database (DB), extract the data to a provided relational DB.
    b. If the tool doesn't make asset inventory data available in SCAP format, use a program provided by the government to convert the relational data to SCAP format.
    c. If the tool only makes asset inventory data available in SCAP format, use a tool provided by the government to convert the SCAP format data to relational DB.

1.5 Operational[13] and Functional[14] Requirements for Software Inventory Management Tools

In this document, the terms must, shall, should, and may are degree modifiers that indicate the the importance of compliance mandated by the requirement. The following conventions are used:

- Must – Compliance with the requirement in its stated form is mandatory.
- Shall – Compliance with the requirement is mandatory unless an explicit contractual waiver is granted by the contracting agency.
- Should – Compliance with the requirement is highly valued and may be mandatory in the future but is not mandatory now.
- May – Compliance with the requirement is optional. The requirement is a desireable additional feature that may be used by contracting agencies to determine best value to the government.

Where requirements of different degree of compliance are nested, the top level degree applies to the top level requirement, and the lower level modifiers indicate the degrees of compliance that apply to the lower level nested requirements.

The contractor shall provide tool(s) that enable the D/A to identify and track authorized and unauthorized software within the network in an efficient, accurate, complete, and timely manner.

SWAM-OP-1: Know the Desired State.

[13] Operational requirements for software inventory management have the naming convention: SWAM-SWAM-OP-*(unique ID)*

[14] Functional requirements for software inventory management have the naming convention: SWAM-F-[OP-ID].*(unique ID)*

The tool [must] record which software products and components on each hardware device (physical and virtual) are authorized to be on the device, and who (by individual, access group, or organization) manages each software product or component. (Implements SWAM-MNS-1.)

1. The software needs to be identified at the following levels of abstraction:
    a. Common Platform Enumeration (CPE™)-level:
        i. vendor,
        ii. software product,
        iii. version, and
        iv. patch level.
    b. Executable-level software components:
        i. which CPE™-level software the executable corresponds to, and
        ii. whether the executable is the correct version for the CPE™-level software.
2. This data is intended to be used to:
    a. Know who is responsible for the following kinds of security attributes to each software product or component (including but not limited to):
        i. installation/removal,
        ii. vulnerability management (patching),
        iii. correct configuration on the software, and
        iv. access controls.
    b. Identify software that is not being managed (unauthorized software), and that is thus likely to be more easily controlled by attackers and used as a pivot point to attack the rest of the network.
    c. Find and take action on unauthorized software within three days after the introduction of unauthorized software products or components; the action must be timely enough to do so significantly faster than attackers can find and exploit the unauthorized software. In this context, "significantly faster" means creating a high probability (notionally ninety percent or greater) that unauthorized software will be discovered by the tool before an attacker would be expected to find and exploit it.
3. Ideally this data needs to be complete enough to cover all software on the network. While identifying absolutely every software product and component on each device on the network is practically impossible, the government's objective is to minimize uncovered software.

The tool is required to satisfy the following functional requirements to the degree specified to support SWAM-OP-1:

SWAM-F-1: Record software inventory information, including, but not limited to the following key elements:

1. [must] Data to enable administrators to easily identify the software products and components on the network. The data that must, shall, or may be included in this inventory information are:
    a) [must] software product name,
    b) [must] software version number,
    c) [must] software patch level,
    d) [shall] an appropriate unique host device ID to link to hardware inventory,
    e) [shall] software component (exe, dll, etc.) file path/name,
    f) [shall] software vendor,
    g) [shall] software component digital fingerprint(s) (authorized and actual), and
    h) [may] other identifying characteristics included in CPE™.
2. [must] Data to enable the tool to match "authorized" software products and components to actual software products and components discovered. The data used may vary by software products and components.
3. [must] Data to describe the impact of a compromise to the software product as an impact score on a scale to be defined by the government.

4. [must] Data to record who, by name or organization, is responsible for the management of the software product on the host and the condition of software product on the host: (Implements SWAM-MNS-5.)
    a. organization,
    b. location,
    c. contact information.
5. [must] Operational status:
    a. to be added,
    b. active,
    c. disposed,
    d. inactive (not-disposed) including:
        i. un-installed,
        ii. missing, and
        iii. other.
6. [may] Property management and accounting information associated with each software product:
    a. licenses or keys that support fiscal inventory (a.k.a., software tag),
    b. name, organization, location, and contact information for accountable property custodian,
    c. name, organization, location, and contact information for software license owner/custodian,
    d. date of software product acquisition, and
    e. most recent physical inventory date of software product.

SWAM-F-1.2: [must] Support population of the authorized inventory by any of these methods: manual data entry, automated ingestion of data in the form of batch files, or automated retrieval of individual or bulk data from interconnected data sources.

a. The tool [must] provide users the functionality to manually:
    i. create software records,
    ii. read software records,
    iii. update software records, and
    iv. delete software records.
b. The tool [must] record decision rules and apply such decision rules to assign software attributes to populate data in the authorized inventory based on multiple sources, including:
    i. [shall] data collected from the actual inventory system,
    ii. [shall] data received from other sources (such as device LDAP systems, property management systems). For example, this might include assigning responsibility by OUs from Active Directory,
    iii. [shall] rules provided by the D/A (such as device types or based on users organization), and
    iv. [may] other methods offered by the vendor to automate populating the authorized inventory.

SWAM-F-1.3: [may] Support other property management functions:

a. [may] Permit authorized users to perform manual entry for recording of software, as necessary.
b. [may] Offer other property management support capabilities.

SWAM-F-1.4: [may] Provide, on demand or on a scheduled basis, a periodic validation questionnaire to authorized users of software for verifying software inventory information (i.e., property management information).

SWAM-OP-2: Know the Actual State.

The tool [must] discover software actually on the network, whether authorized or not, and whether configured to cooperate with detection or not. (Implements SWAM-MNS-2.)

1. This data is intended to be used for comparison to the authorized inventory described above to identify differences between the actual and authorized software inventory, including but not limited to:
    a. authorized software that is not on the network, and
    b. unauthorized (and/or unmanaged) software which are on the network.
2. For this to be achieved, the actual inventory data collected [must] include data necessary to do the following for both unauthorized and authorized software products.
    a. [must] Reliably match (matching primary keys) the authorized inventory data.
    b. [must] Enable system and security administrators to find unauthorized software on the network.
3. For authorized software products that are properly configured[15], the tool [shall] collect significant additional data to automatically fill-in (or validate) the authorized inventory data for these software products.
4. This data will also be used to identify:
    a. which vulnerabilities and configuration standards are/are not applicable to the network, because the affected software is/is-not present,
    b. software for which configuration guides and/or vulnerability checks are needed, and
    c. software for which licenses are actively managed.

The tool is required to satisfy the following functional requirements to the degree specified to support SWAM-OP-2:

SWAM-F-2.1: [must] Discover authorized (managed) and unauthorized (unmanaged) software within the boundaries of the inventoried devices (authorized and unauthorized) on the network:

a. [must] Without requiring knowledge of authentication credentials,
b. [must] significantly faster (as defined above) than attackers can find and exploit unauthorized devices or unauthorized software on authorized devices with,
c. [must] at user-defined scheduled intervals and on demand,
d. [must] detect all executable files stored on the target devices,
e. [must] have a false positive/negative rate below 0.1%,[16]
f. [must] limit the burden put on network resources such that (1) the presence of the scan is not noticeable above background variation in network bandwidth and (2) completeness and timeliness goals in SWAM-OP-1 can be met, and
g. [should] detect all executable files in mobile code.[17]

SWAM-F-2.2: [must] Collect data to match actual to authorized inventory such that the mapping:

a. [must] be reliable (repeatable), such that the same test run on the same network state produces the same results,
b. [must] be valid/accurate (false positive/negative rates below 0.1%),
c. [must] be timely,

[15] "Properly" means that the configuration matches a defined desired state for required and authorized software.

[16] A false positive is a report of software assets that do not exist. A false negative is a failure to report actual software that does exist.

[17] Mobile code is software transferred between systems, e.g. transferred across a network or via a USB flash drive, and executed on a local system without explicit installation or execution by the recipient. Source: Wikipedia, http://en.wikipedia.org/wiki/Mobile_code, page last modified on 23 April 2012 at 20:59.

d. [must] record when software products and components are detected and when they were authorized or unauthorized, to enable accurate identification of risks by associating risk conditions (i.e., the presence of unauthorized software or absence of authorized software) under asynchronous conditions.

SWAM-F-2.3: [shall] Assess and validate software products and components on D/A-responsible IT assets according to a D/A-defined schedule, on a D/A defined event-driven basis, and on an unscheduled ad hoc basis.

a. [must] Provide adequate data to locate the software easily on the network.
b. [may] Provide network maps and/or identify connections between devices in table form for the IT assets covered by the data collection.
c. [may] Provide means other than network and connection maps to achieve the objectives described above.

SWAM-F-2.4: For properly configured IT assets and using authenticated access permission to conduct the discovery inventory, the tool [must] collect additional data to validate data in the actual inventory. The government will evaluate tools on the extent and value of the additional data to both network security (first priority) and operations (second priority).

SWAM-F-2.5: [should] Identify types of software products based upon their behavior (e.g., use of ports, protocols, and services characteristic of specific functionality).

SWAM-F-2.6: [shall] Ensure that only authorized users can schedule detection of actual software inventory.

SWAM-OP-3: Know the Differences (Between Actual and Desired States) and Automatically Act on the Differences.

The tool [must] compute the difference between the authorized and actual inventory, so that the differences can be addressed. (Implements SWAM-MNS-3.) The tool [should] have the ability to prevent/reduce damage from and/or execution of blacklisted and/or non-whitelisted software, as configured by the D/A.

The tool is required to satisfy the following functional requirements to the degree specified to support SWAM-OP-3:

SWAM-F-3.1: [must] Identify unauthorized software products, components, and component fingerprints (or equivalent) in the actual software inventory.

a. [must] Do this using the data collected under SWAM-OP-1 and SWAM-OP-2.
b. [must] Do this automatically and within ten seconds of detection.
c. [must] Report date first seen and date last seen, or never seen.

SWAM-F-3.2: For devices in the authorized inventory, the tool [must] assess and validate as much data in the authorized software inventory as technically possible, as indicated by capability demonstrated by available COTS products available on the market.

a. [must] Flag software products, components, and component fingerprints (or equivalent) in authorized inventory that do not appear present in the actual inventory including date last seen.

SWAM-F-3.3: [must] Trigger e-mail notifications and application programming interface (API) notices to the dashboard based on user-defined business rules, to include at a minimum:

a. when differences are first found,
b. at set times after found, if not resolved,
c. when discovered to be resolved.

SWAM-F-3.4: [must] Detect and report malware (including, as configured, all non-whitelisted software, and software not behaving as expected) at a rate comparable to existing anti-virus products, and provide a means for removing malware in time to prevent it from executing. Thus, with this product, the government's need for an anti-virus program should be satisfied.

a. The tool [should] automatically remove detected malware from an infected software product, based upon the best available information.

b. The tool [should] identify and differentiate between the following types of malware: worm, virus, polymorphic virus, stealth virus, Trojan horse, adware, spyware, spam, and tracking cookies.
c. The tool [should] recommended procedures to selectively/manually remove detected malware from an infected software product or component, based upon the best available information.
d. The tool [may] describe discovered malware using the Malware Attributes Enumeration and Characterization (MAEC™), version 2.0 or later. This can include, but is not limited to, information on the specific objects detected, the system state changes performed by the malware, and the version/date of the AV signature database used to perform the detection.
e. The tool [may] describe the attack pattern of discovered malware; if it does, it should use the Common Attack Pattern Enumeration and Classification (CAPEC™), release 1.6 or later.

SWAM-F-3.5: [shall] Provide management and reporting of whitelist changes and software installation actions.

a. [must] Provide reports of newly installed software products and components to allow monitoring of changes to installed software (using digital fingerprints or other equivalent method).
    i. [must] Include changes to software component fingerprint.
    ii. [must] Include changes to software components.
    iii. [must] Include differences between actual software component fingerprint and vendor-approved software component fingerprint.
b. [should] Use labor saving approaches, such as application of approved business logic, to support automated management of the whitelist, such as the following:
    i. whitelist by location (path) with controls on who can install in each path,
    ii. whitelist, by "grandfathering," existing software at a specific time,
    iii. whitelist by "approved" installers (human or system processes), such that software installed by approved installers is added to the approved whitelist.

SWAM-F-3.6: [shall] Block unauthorized software from executing based on an authorized software list specific to each hardware device.

a. [shall] Block non-mobile (i.e., resident) executables.
b. [should] Block mobile executables.

SWAM-OP-4: Group Items Found for Reporting.

Report authorized and actual software products and components by category (when such data has been entered manually or detected by the system):

1. This data is intended to be sent to the dashboard, to enable displays of software products and components and their other attributes (such as impacts, configurations, vulnerabilities, and connections), reported by categories such as, but not limited to:
a. FIPS and/or CNSSI-1253 impact/security categories,
b. approved classification ceiling,
c. system type (GSS or Major Application),
d. FISMA reportable system,
e. LAN/Device/Path location,
f. supported business organizations,
g. supported business functions, and
h. other categories, to be determined by D/As on an ad hoc basis.
2. The tool [must] be record any or all of these categories for each software product and component.

3. The tool [must] enforce a user-defined cardinality for each category type (single or multi-valued).
4. The tool [must] provide an appropriate interface integrated with the basic inventory screens to allow authorized personnel to enter, update and delete these categories.
5. The tool [must] display software products and components so that users can authorize them and/or have the categories (described in SWAM-OP-4 item 1) applied to them.
6. As described in SWAM-OP-1, there [must] be a mechanism to apply updates to these attributes with data from other sources, including batch file changes.

The tool is required to satisfy the following functional requirements to the degree specified to support SWAM-OP-4:

SWAM-F-4.1: The product [must] be configurable to record any number of hierarchical categories (attributes) by which the software products and components may be described.

a. The tool [must] provide the functionality for DHS to configure such categories as needed to support Federal dashboard operations and reporting.
b. The tool [must] provide the functionality for D/As to configure additional categories needed to support D/A operational concepts.
c. The configuration of categories [must] support:
    i. limitation of values to defined domains,
    ii. required and optional values, and
    iii. either limitation to single valued attributes or inclusion of multiple values.
d. The tool [shall] provide a user interface for the application of these categories.

SWAM-F-4.2: The tool [must] assign any of these categories to each software product and component.

a. Software components [must] be able to inherit categories from their parent software product, including inheriting multiple values of categories from multiple parent software products.

SWAM-OP-5: Interoperate.

Share data with other system components (discovery tools, dashboard, network asset systems [e.g., Active Directory and other LDAP-like systems], property management systems, and OCIL questionnaire systems).

1. Data shared is intended to be used, for example, in the following ways:
    a. In all cases, data about software, authorized and unauthorized, will need to be sent to the Federal dashboard and to D/A dashboards and dashboards for bureaus or organizations within D/As, according to D/A-defined requirements.
    b. When the SWAM tool discovers new software, the tools for configuration, and vulnerability/patch management [should] be notified to allow them to further assess that software.
    c. Data from LDAP products and property management system [may] be used to prepopulate the authorized inventory.
    d. Data from the actual inventory [may] be used to validate the attributes of authorized software.
    e. Data from the authorized and actual inventory [may] be used to create questionnaires for software managers and/or users to check inventory data.
    f. Data from the actual asset inventory discovery checks [may] be fed back into the inventory system to update authorized inventory data.

The tool is required to satisfy the following functional requirements to the degree specified to support SWAM-OP-5:

SWAM-F-5.1: Provide the software inventory data to the Federal dashboard and other subsystem or system components in a standard interface.

a. [should] Using XML based SCAP standard parameters, the tool:
    i. [must] use a relational data structure,

ii. [should] use NIST-specified open standards to express and communicate software inventory information such as: Asset Summary Report (ASR) protocol (an emerging specification); Asset Identification (AI) protocol, version 1.1 or later; or CPE™ version 2.3 or later,
    - Data describing HWCI/SWCI[18] [should] use the CPE™ version 2.3 or later standard.
    - If it uses CPE™, at a minimum it [should] contain the following structure: cpe:/ {part} : {vendor} : {product} : {version} : {update} : {edition} : {language} : {sw_edition} : {target_sw} : {target_hw} : {other}

iii. [should] process software inventory data and distribute them using the CPE™ standard version 2.3 or later,

iv. [may] permit authorized users to create D/A-specific CPE™ definitions.

b. [may] Provide the ability to process and distribute questionnaire responses using the OCIL standard version 2.0 or later.

SWAM-F-5.2: Receive and ingest relevant software inventory data from the Federal dashboard and other system or subsystem components in a standard interface:

a. [must] using a relational data structure and
b. [should] using XML-based SCAP standard parameters (as described above).

SWAM-OP-6: Scale.

The tool is required to satisfy the following functional requirements to support operations at the scale of federal networks:

SWAM-F-6.1: [must] Store, process, and provide software inventory data, as described above, for large federal networks (networks with over 1,000,000 devices) while maintaining adequate timeliness, completeness, and accuracy, as defined above.

SWAM-OP-7: Secure Data Collected.

The tool [shall] protect tool components and data during collection, storage, and transmission to other sources.

The tool is required to satisfy the following functional requirements to the degree specified to support SWAM-OP-7:

SWAM-F-7.1: [must] Encrypt data with adequate methods while in motion (to prevent network sniffers from collecting the inventory data) and while at rest (to prevent exfiltration from data stores).

SWAM-F-7.2: [must] Provide access controls for system functions that support centralized and decentralized:

a. administration of the tools,
b. scheduling detection,
c. viewing of authorized and actual inventory data,
d. transmission of authorized and actual inventory data, and
e. other functions described herein.

SWAM-F-7.3: [must] Operate within a generic enclave (protected by a firewall, etc.) and communicate with (send asset inventory data to and receive it from) the central asset inventory system.

SWAM-F-7.4: [must] Provide supply chain verification for tool components, such as, but not limited to, digital fingerprints for each software file used in the system, tied to specific software product versions and patch levels.

[18] References to Hardware Configuration Items (HWCI) have been included in Software Inventory Management functions.

SWAM-F-7.5: The tool [shall] enable administrators to assign authorized users of the asset inventory tool to hierarchically-defined access control "groups."

a. The tool [shall] control access by user group.
b. The tool [shall] control access based on combinations of user groups.

SWAM-OP-8: Additional Capabilities.

The tools [may] support related data analysis and business functional requirements that are not included in the security requirements listed above. These capabilities [should] be reported by the vendor, and will be used by the government to evaluate tools relative to security requirements.

The tool [must] satisfy the following functional requirements to the degree specified to support SWAM-OP-8:

SWAM-F-8.1: [may] Dashboard/interface capabilities that enable D/As to get better/additional value from the data. For example, this might include:

a. network design,
b. network mapping,
c. trend analysis, and
d. compliance reporting.

SWAM-F-8.2: [may] Integrated property management functions that would enable D/As to perform property management without purchasing a separate system. For example, this might include:

a. software device sub-component (configuration item) tracking,
b. purchasing/disposal details,
c. maintenance management,
d. license management, and
e. physical inventory preparation/reporting.

SWAM-F-8.3: [may] Assign risk values to the differences found between authorized software inventory and actual software discovered. (Implements SWAM-MNS-4, which is normally performed by the Federal dashboard but may be performed by the tool.)

Detailed instructions on creating an asset inventory that could meet these requirements are available at http://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf. This document shall be considered as advisory only and does not constitute additional operational or functional requirements.

3 Performance Work Statement (PWS) for Tools Supporting the Configuration Management Function

This PWS describes the objectives of continuous monitoring and risk scoring for tools providing diagnostics for supporting configuration management; the mission need for this function; the operational assumptions and operational concept guiding the adoption of this function; and operational and functional tool requirements.

3.1 Function Statement of Objectives (SOO)

The **objective of the configuration management function** is to reduce misconfiguration of IT assets, including misconfigurations of hardware devices (to include physical, virtual and operating system) and software. Over 80% of known vulnerabilities are attributed to misconfiguration and missing patches.[19] Cyber adversaries often use automated computer attack programs to search for and exploit IT assets with misconfigurations, especially for assets supporting federal agencies, and then pivot to attack other assets.

3.2 Function Mission Needs Statement (MNS)

To perform this function, processes are needed to:

CM-MNS-1:[20] Establish authorized security configuration benchmarks, consisting of the acceptable value(s) for each relevant configurable setting for each IT asset type.

1) Establish a core federal benchmark for hardware devices and software with pre-programmed tests for actual status and a federal system to provide core-scores for risk assessment.
2) Allow departments and agencies (D/As) to adopt the federal benchmark and/or:
   a) Add, modify, and delete non-core configuration settings.
   b) Assign an alternate method to score risk for common and D/A-specific settings for internal D/A use.
3) Develop a federal benchmark tool, pre-programmed test for actual status and a federal system to provide core-scores for risk assessment.

CM-MNS-2: Determine the value of the actual settings within the authorized security configuration benchmark tool.

CM-MNS-3: Assign core (federal) and alternate (D/A) risk scores to each reported deviation based on relevant factors.

CM-MNS-4: Report the difference (deviation, delta) between the authorized security configuration baseline and the actual assessment results (non-compliant settings) along with relevant risk scores.[21] This difference may make the device or software either more or less secure, and the tool should be able to distinguish this difference.

CM-MNS-5: Manage a change control process that documents D/A extensions[22] or exception to the authorized core federal benchmarks.

3.3 Function Operational Assumptions and Constraints

At a minimum, security configuration compliance assessments must cover addressable hardware devices (such as network assets [as defined in the FY2012 CIO FISMA reporting guidance]) and the software typically found on those assets. The range of software to be covered is indicated by the software and

---

[19] GAO-03-1138T, *Effective Patch Management is Critical to Mitigate Software Vulnerabilities*, September 10, 2003. (http://www.gao.gov/products/GAO-03-1138T)

[20] Mission Needs Statement requirements for configuration management have the naming convention: CM-MNS-*(unique ID)*

[21] For performance reasons, scores may be reported once and computed from actual setting values, or may use other methods that achieve the objective of ensuring that the dashboard has both actual values and scores needed to compute results.

[22] An exception is an authorized deviation with the justification for the deviation.

hardware inventory reported under FISMA. The processes for establishing the authorized security configuration baseline and producing actual assessment results are needed by both small and large D/As, ranging from several hundred users to millions of users. Large D/As may have multiple computing enclaves and may want to operate the security configuration compliance assessment at the enclave level. Ultimately, the government seeks to summarize the configuration of IT assets for all federal D/As.

It is assumed that such a configuration management function must be largely automated to be effective, timely, and efficient. The cost of writing tests for settings within specific benchmarks has historically been a barrier to use of such automation. Another barrier has been that tools on the market have not always been able to test all desired settings. Finally, the ability to adapt the baseline automatically to local device conditions using tailorable rules (for example, to add checks or ignore certain checks based on attributes of the device on which installed) has not always been possible, but is highly desireable.

3.4 Illustration of **Function** Operational Concept

The government has identified the following technical approaches and operational concepts in the market as acceptable ways to meet the objectives of the configuration management function. The government is open to other innovative, effective, and efficient ways of achieving these objectives, but offers these suggestions to help clarify the objectives and some of the issues to be addressed.

7. Creating the initial authorized security configuration benchmark by building on existing security configuration benchmarks to create default (approximate) core federal benchmarks. For example, such sources might include:
    a. United States Government Configuration Baseline (USGCB) or Federal Desktop Core Configuration (FDCC), or
    b. D/A-specified security configuration benchmarks (e.g., Defense Information Systems Agency [DISA] Security Technical Implementation Guides [STIGs], D/A Security Content Automation Protocol [SCAP] Content).
8. Maintaining and updating the authorized federal core security configuration benchmarks by establishing a process to:
    a. document rules to modify the benchmark automatically, and
    b. authorize changes to the rules and benchmark.
9. Providing the ability for D/A to add/modify/delete non-core configuration settings of their D/A benchmark.
10. Obtaining actual security configuration settings assessment results via technically accurate and reliable methods.
11. Computing differences between the authorized security configuration benchmark settings and actual security configuration settings. Benchmark settings may be multi-valued, and more than one setting may be acceptable, with a range of risk values associated with different settings. Therefore, reporting simple pass/fail attributes are not sufficient; actual settings must be reported unless the setting can be unambiguously derived from the reported findings.
12. Meeting SCAP and relational database (DB) representational requirements for interoperability of reporting (dashboard, query, etc.).
    a. If the tool doesn't contain a relational DB, efficiently extract the data to a provided relational DB.
    b. If the tool doesn't support SCAP, use a program provided by the government to convert the relational data to SCAP.
    c. If the tool only supports SCAP, use a tool provided by the government to convert the SCAP data to a relational DB.

3.5 Operational[23] and Functional[24] Requirements for Configuration Management Tools

In this document, the terms *must*, *shall*, *should*, and *may* are degree modifiers that indicate the the importance of compliance mandated by the requirement. The following conventions are used:

- Must – Compliance with the requirement in its stated form is mandatory.
- Shall – Compliance with the requirement is mandatory unless an explicit contractual waiver is granted by the contracting agency.
- Should – Compliance with the requirement is highly valued and may be mandatory in the future but is not mandatory now.
- May – Compliance with the requirement is optional. The requirement is a desireable additional feature that may be used by contracting agencies to determine best value to the government.

Where requirements of different degree of compliance are nested, the top level degree applies to the top level requirement, and the lowerlevel modifiers indicate the degrees of compliance that apply to the lower level nested requirements.

CM-OP-1: Know the Desired State.

The tool must provide the ability to create, update, and maintain the security configuration settings benchmarks for target hardware devices and software products. For each hardware device and software product, the tool needs to maintain the federally authorized core benchmark as well as D/A-specific variations that implement D/A policies. In this regard, DHS will represent the federal government by setting up federal benchmarks for consistent cross-agency comparisons. D/As can modify scoring (for internal use). (Implements CM-MNS-1.) The tool is required to satisfy the following functional requirements to the degree specified to support CM-OP-1:

CM-F-1.1: The tool [shall] document authorized security configuration settings within benchmarks for specific software and hardware products.

CM-F-1.2: The tool [must] store, process, and distribute security configuration benchmarks. The tool:

a. [must] document context-specific changes to the centrally specified security configuration benchmarks, based on D/A policies where implemented, product function, compensating controls, etc.
b. [must] Permit authorized users to edit (add, modify, delete, enable, or disable) both core and non-core security configuration benchmark settings . Typically, only DHS will edit the core setting and core scoring parameters, on behalf of the federal government); D/As will edit non-core settings and D/A scoring parameters.
c. [shall] tailor the authorized security configuration settings within a benchmark by applying contextual rules.
d. [shall] Provide traceability of requirements by associating setting checks in a benchmark to relevant identifiers (e.g., CCE™) and mapping checks to accepted sets of security controls, such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Committee on National Security Systems Instruction (CNSSI)-1253, or D/A-defined security controls.[25]

CM-F-1.3: [shall] Permit authorized users to select and compose a set of security configuration benchmarks to establish an authorized security configuration baseline for an (or a group of) IT asset(s).

a. [shall] Permit authorized users to modify and update security configuration benchmarks.

---

[23] Operational requirements for configuration management have the naming convention: CM-OP-*(unique ID)*

[24] Functional requirements for configuration management have the naming convention: CM-F-[OP-ID].*(unique ID)*

[25] NIST SP 800-53, CNSSI-1253, or D/A-defined security controls may be embedded as a <reference> in XCCDF.

b. [may] Permit authorized users to create and modify a risk/vulnerability score for each security configuration setting within a security configuration benchmark. [26]

CM-F-1.4: The tool [shall] track changes in the authorized security configuration baseline by date and authorized user.

a. The tool [may] associate all changes made to the authorized security configuration baseline by an authorized user.
b. The tool [may] permit an authorized user to define the effective period for recorded changes in the authorized security configuration baseline.

CM-F-1.5: The tool [shall] be capable of being maintained to add or tailor configuration checks with a low level of effort, based on these assumptions:

a. 80% of checks will be defined once at the federal level, and
b. 20% of checks will be defined by each D/A (with over 10,000 employees) using the tool.

CM-OP-2: Know the Actual State.

The tool [must] assess the state of security configuration settings of an IT asset with respect to the authorized security configuration baseline. (Implements CM-MNS-2.) This data will ultimately be used for comparison to the authorized security configuration described above to identify differences between the actual and authorized security configuration and their effect on risk.

The tool is required to satisfy the following functional requirements to the degree specified to support CM-OP-2:

CM-F-2.1: The tool [shall] perform configuration assessments on a D/A defined schedule, on a D/A defined event-driven basis, and on an unscheduled ad hoc basis.

CM-F-2.2: The tool will be used to support a wide range of checks, and:

d. [must] be capable of completing all testable checks within a three-day window,
e. [shall] be capable of "automated checking" the vast majority of desired checks,[27]
f. [shall] be capable of completing required checks without excessive manual effort,
g. [must] be capable of returning the actual value of each setting tested, not just pass/fail, and
h. [must] be capable of completing required checks without noticeable impact on network capacity.

CM-F-2.3: The tool [shall] ensure that only authorized users can schedule assessments to detect vulnerabilities and weaknesses with actual values.

CM-F-2.4: The tool [shall] meet the following conditions:

a. [shall] Implement over 90% of the "automated checks" in typical federal benchmarks for common operating systems and applications that have been adopted by typical D/As.[10]
b. [must] Complete a full assessment and reporting of all "automated checks" for all items needing benchmarks at least every three days,
c. [must] Perform the assessment without noticeable impact on network capacity.
d. [must] Return the actual setting value or corresponding score, not just pass/fail status.

CM-OP-3: Know the Differences (Between Actual and Desired States) and Automatically Report the Differences.

The tool [must] identify and report differences between the authorized security configuration benchmark and the actual assessment results, so that the differences can be addressed. (Implements CM-MNS-3.)

[26] The weight values are in the XCCDF content.

[27] Experience with automating checks of government benchmarks has shown that a small number of checks in some benchmarks are not susceptible to automated checking with unambiguous results.

The tool is required to satisfy the following functional requirements to the degree specified to support CM-OP-3:

CM-F-3.1 The tool [shall] enumerate deviations from the authorized security configuration benchmark, including deviations that provide greater protection or reduce risk further than the authorized benchmark.

CM-F-3.2: The tool [shall] provide visibility of configuration deviations of IT assets from the enterprise level to an individual user's area of responsibility (AOR).

CM-F-3.3: The tool [shall] apply D/A business rules to determine responsibility for addressing deviations.[28]

CM-F-3.4: The tool [shall] score (assign a numerical value to) deviations for purposes of computing risk. Scoring includes:

- scores for all possible values of a configuration setting,
- standard federal score for deviations from accepted benchmarks, and
- alternate D/A scores for deviations from accepted benchmarks, where the D/A has adopted a policy that differs from the federal policy.[29]

CM-F-3.5: The tool [shall] assess the security configuration of networked IT assets.

CM-F-3.6: The tool [may] assess the security configuration of non-networked IT assets.

CM-F-3.7: The tool [shall] store assessment results to enable enterprise security posture reporting for a D/A-defined period of time.

CM-OP-4: Group Items Found for Reporting.

The tool is required to satisfy the following functional requirements to support the reporting using D/A-defined reporting groupings:

CM-F-4.1: The tool [shall] report the security configuration compliance posture of IT assets using the authorized security configuration benchmark using D/A-defined reporting groupings identified for hardware and software asset inventory management functions.

CM-OP-5: Interoperate.

Share data with other system components (discovery tools, dashboard, network asset systems [e.g., Active Directory and other LDAP-like systems], configuration management systems, and OCIL questionnaire systems). Data shared is intended to be used, for example, in the following ways:

1. In all cases, data about software, authorized and unauthorized, will need to be sent to the federal dashboard and to D/A dashboards and dashboards for bureaus or organizations within D/As, according to D/A-defined requirements.
2. When the CM tool discovers misconfigured assets, the tools for hardware inventory, software inventory, and vulnerability/patch management [should] be notified to allow them to further assess those assets.

The tool is required to satisfy the following functional requirements to the degree specified to support CM-OP-5:

CM-F-5.1: Receive and provide configuration data (i.e., communicate with the central dashboard and other components) using standard interfaces and formats, where applicable, to the extent that such standards can be applied with acceptable network performance and reasonable data storage limits.

c. [must] Use a relational data structure [to be defined].

[28] Responsibility for an IT asset is part of the hardware and software inventory management function. The responsibility for addressing a specific configuration may be different than the responsibility for the asset itself.

[29] D/As may adopt benchmarks that are more restrictive, less restrictive, or qualitatively different than federal benchmarks. The purpose of computing both scores is to enable comparison within agencies against the D/A's standards and comparison across the federal government.

d. [should] Use XML-based SCAP standard parameters. The tool [may] do this in SCAP version 1.2 or later (i.e., Extensible Configuration Checklist Definition Format [XCCDF], Open Vulnerability Assessment Language [OVAL®], Open Checklist Interactive Language [OCIL], CCE™, and Common Platform Enumeration [CPE™])[30] or other suitable language.
e. [should] Process configuration data and distribute them using the CCE™ standard version 5 or newer.
f. [should] Report assessment results using XCCDF version 1.2 or later XCCDF Results Format Schema.
g. [should] Encapsulate assessment results using Asset Reporting Format (ARF) version 1.1 or later.
h. [should] use NIST-specified open standards such as: Asset Summary Report (ASR) protocol (an emerging specification) or CPE™ version 2.3 or later, to express and communicate configuration information.
    vi. Data describing HWCI/SWCI[31] [should] use the CPE™ version 2.3 or later standard.
    vii. If it uses CPE™, at a minimum it [should] contain the following structure: cpe:/ {part} : {vendor} : {product} : {version} : {update} : {edition} : {language} : {sw_edition} : {target_sw} : {target_hw} : {other}
i. [may] Map CCE™ identifiers to NIST SP 800-53 security controls via the National Vulnerability Database (NVD) CCE™ Reference Data feed.[32]
j. [may] Associate XCCDF-based security configuration checklist checks with a set of OCIL-based security control definitions.[33]
k. [may] Store and distribute operational and management security control descriptions using the OCIL version 2.0 or later standard.[34]

CM-OP-6: Scale.
The tool is required to satisfy the following functional requirements to support operations at the scale of federal networks:
CM-F-6.1: [must] Be capable of storing, processing, and providing hardware inventory data, as described above, for large Federal networks (networks with over 1,000,000 devices) while maintaining adequate timeliness, completeness, and accuracy, as defined above.

CM-OP-7: Secure the Data Collected.
The tool [shall] protect tool components and data during collection, storage, and transmission to other sources.
The tool is required to satisfy the following functional requirements to the degree specified to support CM-OP-7:

---

[30] NIST SP 800-126, Rev 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, September 2011. (http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf)
[31] Hardware Configuration Items and Software Configuration Items
[32] *Common Configuration Enumeration (CCE) Reference Data* (http://nvd.nist.gov/cce.cfm). Note: Currently, the feed is in Beta and it is limited to the USGCB benchmark.
[33] OCIL can be used for functions other than configuration management. For this case, OCIL is being used to capture security controls status that cannot be captured through automation.
[34] As the operational and management class of security controls in NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

CM-F-7.1: [must] Encrypt data with FIPS-compliant encryption modules while in motion (to prevent network sniffers from collecting the inventory data) and while at rest (to prevent exfiltration from data stores).

CM-F-7.2: [must] Provide access controls for system functions that support centralized and decentralized:

f. administration of the tools,
g. scheduling detection,
h. viewing of authorized and actual configuration data,
i. transmission of authorized and actual configuration data, and
j. other functions described herein.

CM-F-7.3: [must] Operate within a generic enclave (e.g., protected by a firewall) with boundaries to be defined separately by each D/A.

CM-F-7.4: [must] Provide supply chain verification for tool components, such as, but not limited to, digital fingerprints for each software file used in the system, tied to specific software product versions and patch levels.

CM-F-7.5: The tool [shall] enable administrators to assign authorized users to hierarchically-defined "groups."

c. The tool [shall] control access by user group.
d. The tool [shall] control access based on combinations of user groups.

CM-OP-8: Additional Capabilities.

The tool [may] support related data analysis and business functional requirements that are not included in the security requirements listed above. These capabilities should be reported by the vendor, and will be used by the government to evaluate tools relative to security requirements.

4 Performance Work Statement (PWS) for Tools Supporting the Vulnerability Management Function

This PWS describes the objectives of continuous monitoring and risk scoring for tools providing diagnostics for supporting vulnerability management; the mission need for this function; the operational assumptions and operational concept guiding the adoption of this function; and operational and functional tool requirements.

4.1 Function Statement of Objectives (SOO)

The **objective of the vulnerability management function** is to discover and support remediation of vulnerabilities in IT assets on a network. Vulnerability management is the management of risks presented by known software weaknesses that are subject to exploitation. The vulnerability management function ensures that mistakes and deficiencies are identified and removed or remediated quickly from operational systems so that they can no longer be exploited. (An information security vulnerability is a deficiency in software that can be directly used by a hacker to gain access to a system or network.)

4.2 Function Mission Needs Statement (MNS)

To perform this function, processes are needed to:

VUL-MNS-1:[35] Discover, identify, and locate known security vulnerabilities.

VUL-MNS-2: Discover, identify, and locate other known software weaknesses in software applications and source code.

VUL-MNS-3: Support the awareness and understanding of potential exposure risks associated with software weaknesses.

4.3 Function Operational Assumptions and Constraints

This process is needed by both small and large departments and agencies (D/As), ranging from several hundred users to millions of users. Large D/As may have multiple enclaves and may want to operate vulnerability management at the enclave level. Ultimately, the government seeks to summarize the data up to and including the federal level, which includes all civilian executive branch D/As.

Tools that enable the vulnerability management function are categorized as:

- vulnerability scanners,
- web application scanners,
- database scanners,
- static source code analyzers,
- static binary code scanners,
- exploitation tools (including penetration test tools).

It is possible that the specialized tools in each category might fail to interoperate. Since interoperability is even more critical for these categories of tools, it is reasonable to anticipate that, in the near future, more rigorous interoperability requirements will appear for tools that access the Common Vulnerability and Exposure identifiers (CVEs®), Common Weakness Enumeration (CWE™), Common Attack Pattern Enumeration and Classification (CAPEC™), and Cyber Observable eXpression (CybOX™).

4.4 Illustration of Function Operational Concept

The government has identified the following technical approaches and operational concepts in the market as acceptable ways to meet the objectives of the vulnerability management function. The government is open to other innovative, effective, and efficient ways of achieving these objectives, but offers these

[35] Mission Needs Statement requirements for vulnerability management have the naming convention: VUL-MNS-*(unique ID)*

suggestions to help clarify the objectives and some of the issues to be addressed. The objectives of the vulnerability management function are achieved by:

1. Maintaining access to the National Vulnerability Database (NVD) and new vulnerabilities that are addressed therein. Specifically, staying informed about vulnerabilities that are applicable to the specific hardware and software present on the subject system or network (i.e., the desired state).
2. Assessing vulnerabilities present on the subject system or network through the use of vulnerability scanning tools or equivalent methods (i.e., the actual state).
3. Ensuring vulnerability scanning tools are scanning against the most current and complete set of known vulnerabilities.
4. Determining the gap between the desired state and the actual state of security (i.e., the findings), and determining appropriate defensive and corrective actions by:
    a. extracting relevant information from tool outputs,
    b. comparing vulnerability scan results with event logs to determine whether vulnerabilities were exploited,
    c. prioritizing vulnerabilities for remediation in accordance with the criticality of the system to the mission and the impact of the exploitation, and
    d. assessing the vulnerability findings on an established and consistent scale of severity.
5. Establishing processes for remediating discovered vulnerabilities by:
    a. prioritizing the vulnerabilities based on severity and impact,
    b. associating vulnerabilities with known patch levels to reduce or eliminate "double counting" of the same risks represented by (1) vulnerabilities present and (2) patches not present,
    c. quickly distributing remediation guidance to those responsible for software and security administration,
    d. quickly distributing patches and fixes, if available,
    e. applying changes (e.g., patching), and
    f. validating changes (e.g., by comparing back-to-back scans).
6. Meeting Security Content Automation Protocol (SCAP) and relational requirements for interoperability of reporting (dashboard, query, etc.).
    a. If the tool doesn't have a relational database (DB), extract the data to a provided relational DB.
    b. If the tool doesn't support SCAP, use a program provided by the government to convert the relational data to SCAP.
    c. If the tool only supports SCAP, use a tool provided by the government to convert the SCAP data to a relational DB.

Most vulnerabilities are defined by the CVEs®, though other detectable vulnerabilities may exist that are not in the CVEs® and for which patching may also be an available remedy. Vulnerabilities identified will typically be remediated through the software inventory management function, through the use of updates, patches, plug-ins, and new releases.

4.5 Operational[36] and Functional[37] Requirements for Vulnerability Management Tools

In this document, the terms *must*, *shall*, *should*, and *may* are degree modifiers that indicate the the importance of compliance mandated by the requirement. The following conventions are used:

- Must – Compliance with the requirement in its stated form is mandatory.

[36] Operational requirements for vulnerability management have the naming convention: VUL-OP-*(unique ID)*

[37] Functional requirements for vulnerability management have the naming convention: VUL-F-(OP-ID).*(unique ID)*

- Shall – Compliance with the requirement is mandatory unless an explicit contractual waiver is granted by the contracting agency.
- Should – Compliance with the requirement is highly valued and may be mandatory in the future but is not mandatory now.
- May – Compliance with the requirement is optional. The requirement is a desireable additional feature that may be used by contracting agencies to determine best value to the government.

Where requirements of different degree of compliance are nested, the top level degree applies to the top level requirement, and the lower level modifiers indicate the degrees of compliance that apply to the lower level nested requirements.

VUL-OP-1: Know the Desired State.

The tool vendor [must] update the tool to be able detect vulnerabilities and weaknesses that have been identified by the government (e.g., CVE®, CWE™). (Implements VUL-MNS-1 and VUL-MNS-2.) The tool is required to satisfy the following functional requirements to the degree specified to support VUL-OP-1:

VUL-F-1.1: [must] keep their tool for detection of actual vulnerabilities and weaknesses in a state such that it provides:

a. Complete coverage of the CVEs®, CWEs™, etc. identified by the National Vulnerability Database, and equivalent from other useful sources. Coverage of Common Platform Enumerations (CPEs™) currently installed on government hardware requires:
    i. >=95% coverage for High rated CVEs® and CWEs™ (or equivalent),
    ii. >=75% coverage for Moderate rated CVEs® and CWEs™ (or equivalent),
    iii. >=50% coverage for Low rated CVEs® and CWEs™ (or equivalent),
    iv. the ability to operate correctly on the vendor-product-versions of all hardware found on federal networks (networks with over 1,000,000 devices).
b. Timely coverage of the same weaknesses and vulnerabilities within:
    i. 1-4 weeks for High-rated vulnerabilities and weaknesses,
    ii. 1-8 weeks for Moderate-rated vulnerabilities and weaknesses,
    iii. 1-16 weeks for Low-rated vulnerabilities and weaknesses.
c. Text for systems administrators to clearly and simply explain how to correct actual vulnerabilities and weaknesses.
    i. This [must] identify affected assets by device, product, and component.
    ii. This [shall] include links to NVD and other public sources.
    iii. This [should] provide a concise summary for those responsible for mitigation to define how to achieve the desired state.
    iv. This [may] include automated mitigation capabilities if they are configurable to allow control of where/when applied.
d. The system [must] help prioritize what to fix first by:
    i. [must] providing scores for each weakness that rates its level of vulnerability independent of attack paths,
    ii. [may] providing a way to assess the vulnerability in the context of attack paths on the network to identify and increase the score at “choke points” through which many attack paths pass.

VUL-OP-2: Know the Actual State.

The tool [must] discover vulnerabilities, weaknesses, etc. actually on the network. Where possible, detection [should] be possible without authentication, but authentication will be accepted as appropriate, if technically necessary (for example, a restricted system enclave is being scanned and either the entire enclave or a sub-enclave requires additional user privilege to allow the scanning tool to properly operate). (Implements VUL-MNS-1 and VUL-MNS-2.) This data will ultimately be used to list vulnerabilities and

weaknesses in a to-do list (equivalent to a Plan of Actions and Milestones) prioritized by vulnerability and/or risk.

The tool is required to satisfy the following functional requirements to the degree specified to support VUL-OP-2:

VUL-F-2.1: [must] Discover actual vulnerabilities and weaknesses on the network:

h. [must] significantly faster than attackers can find and exploit vulnerabilities. For vulnerabilities for which a CVE® or CWE™ exists in the detection tool, the goal is to discover any newly introduced vulnerability no more than 72 hours from its introduction. For existing vulnerabilities for which a CVE® or CWE™ is newly defined, the goal is to discover any vulnerability within 72 hours of incorporating the CVE® or CWE™ in the tool, as described in VUL-F-1.1 b. (above).
i. [must] at frequent user-defined intervals and on demand,
j. [must] detect vulnerabilities and weaknesses on all IP addressable device types,
k. [must] have a false positive/negative rate below 0.1%,[38]
l. [shall] detect vulnerabilities and weaknesses on all IP addressable devices,
m. [should] detect vulnerabilities and weaknesses on all USB device types,
n. [should] detect vulnerabilities and weaknesses on all connected USB devices
o. [must] limit the burden put on network resources, such that (1) the presence of the scan is not noticeable above background variation in network bandwidth and (2) completeness, accuracy, and timeliness goals detailed above can be met.

VUL-F-2.2: [must] Collect appropriate data to map actual vulnerabilities and weaknesses to authorized hardware and software inventory such that the mapping:

e. [must] be reliable (repeatable), such that the same test run on the same network state produces the same results,
f. [must] be valid/accurate (false positive/negative rates below 0.1%),
g. [must] be timely,
h. [must] record when vulnerabilities are first detected and later not detected, to enable association of vulnerabilities to time periods.

VUL-F-2.3: [shall] Conduct system scans to detect vulnerabilities and weaknesses on a D/A defined schedule, on a D/A defined event-driven basis, and on an unscheduled ad hoc basis.

VUL-F-2.4: [shall] Ensure that only authorized users can schedule scans to detect vulnerabilities and weaknesses.

VUL-F-2.5: [shall] Start automated system scans at a prescribed time.

VUL-OP-3: Know the Differences (Between Actual and Desired States).

The presence of a known vulnerability is by definition a deviation from the desired state. Thus this requirement is covered by VUL-OP-2.

VUL-OP-4: Group Items Found for Reporting.

The vulnerabilities will be grouped based on hardware or logical devices on which it is found and sorted by operating system, software, or device enclaves. Thus, the vulnerability data requires no mandatory grouping requirements.

The tool is required to satisfy the following functional requirements to the degree specified to support VUL-OP-4:

VUL-F-4.1: The tool [may] be configured by the vendor to record any number of hierarchical categories (attributes) by which the vulnerabilities and weaknesses may be described and/or grouped.

[38] A false positive is a report of a vulnerability that does not exist. A false negative is a failure to report an actual vulnerability that does exist.

VUL-OP-5: Interoperate.

Share data with other components (discovery tools, dashboard, network asset systems [e.g., Active Directory and other LDAP-like systems], vulnerability management systems, and OCIL questionnaire systems).

2. Data shared is intended to be used, for example, in the following ways:
    g. In all cases, data about assets, authorized and unauthorized will need to be sent to the Federal dashboard and to D/A dashboards and dashboards for bureaus or organizations within D/As, according to D/A-defined requirements.
    h. When the VUL tool discovers new vulnerabilities, the tools for hardware inventory, software inventory, and configuration [should] be notified to allow them to further assess that device and software on which the vulnerability/weakness was found.

The tool is required to satisfy the following functional requirements to the degree specified to support VUL-OP-5:

VUL-F-5.1: Provide the vulnerability data to the Federal dashboard and other subsystem or system components in a standard interface.

l. [should] Using XML based SCAP standard parameters, the tool:
    i. [must] use a relational data structure,
    ii. [should] use NIST-specified open standards to express and communicate vulnerability information such as: Asset Summary Report (ASR) protocol (an emerging specification) or CPE™ version 2.3 or later,
        - Data describing HWCI/SWCI [should] use the CPE™ version 2.3 or later standard.
        - If it uses CPE™, at a minimum it [should] contain the following structure: cpe:/ {part} : {vendor} : {product} : {version} : {update} : {edition} : {language} : {sw_edition} : {target_sw} : {target_hw} : {other}
    iii. [should] process vulnerability data and distribute them using the CVE® standard no more than 60 days old,
    iv. [may] permit authorized users to create D/A-specific CVE® definitions.

VUL-F-5.2: Receive and ingest relevant vulnerability data from the Federal dashboard and other system or subsystem components in a standard interface:

c. [must] using a relational data structure,
d. [should] using XML-based SCAP standard parameters (as described above).

VUL-OP-6: Scale.

The tool is required to satisfy the following functional requirements to support operations at the scale of federal networks:

VUL-F-6.1: [must] Be capable of storing, processing, and providing vulnerability data, as described above for large federal networks (networks with over 1,000,000 devices) while maintaining adequate timeliness, completeness, and accuracy, as defined above.

VUL-OP-7: Secure Data Collected.

The tools [shall] adequately protect tool components and data during collection, storage, and transmission to other sources.

The tool is required to satisfy the following functional requirements to the degree specified to support VUL-OP-7:

VUL-F-7.1: [must] Encrypt data with adequate methods while in motion (to prevent network sniffers from collecting the vulnerability data) and while at rest (to prevent exfiltration from data stores).

VUL-F-7.2: [must] Provide access controls for system functions that support centralized and decentralized:

k. administration of the tools,
l. scheduling detection,
m. viewing of vulnerability data,
n. transmission of vulnerability data,
o. other functions described herein.

VUL-F-7.3: [must] Operate within a generic enclave (protected by a firewall, etc.) and communicate with (send asset vulnerability data to and receive it from) the central asset inventory system.

VUL-F-7.4: [must] Provide supply chain verification for tool components, such as, but not limited to, digital fingerprints for each software file used in the system, tied to specific product versions and patch levels.

VUL-F-7.5: The tool [shall] enable administrators to assign authorized users of the tool to hierarchically-defined access control "groups."

e. The tool [shall] control access by user group.
f. The tool [shall] control access based on combinations of user groups.

VUL-OP-8: Additional Capabilities.

The tools [may] support related data analysis and business functional requirements that are not included in the security requirements listed above. These capabilities [should] be reported by the vendor, and will be used by the government to evaluate toolsrelative to security requirements. Other capabilities include, but are not limited to the following:

The tool [may] satisfy the following functional requirements to the degree specified to support VUL-OP-8:

VUL-F-8.1: Dashboard/interface capabilities that enable D/As to get better/additional value from the data. For example, this [may] include:

e. network design,
f. network mapping,
g. trend analysis,
h. compliance reporting.

5 Glossary

Term	Definition	
Access control	Control of information flow between a subject (e.g., users, program, process, or device, etc.) and an object (e.g., data object, file, program, process, or device).	Department of Homeland Security (DHS) Federal Network Security (FNS) Branch, Situational Awareness Incident Response (SAIR) Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 156.[39]
Accuracy	A high level of confidence that the number of false positives (assets that are not present but appear in inventory) and false negatives (assets that are present but do not appear not in inventory) is negligible.	DHS FNS
Area of Responsibility (AOR)	A pre-defined logical grouping of information technology (IT) assets assigned to an organization for which it has the operational responsibility for meeting the security objectives specified by the department or agency (D/A).	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 76.
Assessment Summary Results (ASR)	An Extensible Markup Language (XML) schema designed to provide a structured language for exchanging summarized assessment results data between assessment tools, asset databases, and other products that manage asset information.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 156.
Asset Identification (AI)	A standard structure for describing configuration items within an IT asset. It is a part of ARF.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 156.
Asset Reporting Format (ARF)	A data model to express the transport format of information about assets, and the relationships between assets and reports.	National Institute of Standards and Technology (NIST), The Asset Reporting Format (2012). http://scap.nist.gov/specifications/arf/
Assurance	In information security, the level (or degree) of confidence that an IT asset has met its security requirements or the authorized security configuration baseline, based on evidence provided through an automated security configuration compliance assessment.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 56.
Authorized user	An authenticated subject (i.e., tool user) with assigned permission to perform a set of specified operations within the tool.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 157.

[39] The SAIR Tier III product performance requirements were vetted by government and industry partners through the development, release, and response of the SAIR Tier III Request for Information (RFI), RFI-OPO-12-0001.

Cardinal number	A number denoting quantity but not order in a set.	Collins English Dictionary – Complete and Unabridged, "Cardinal Number" (HarperCollins Publishers, 2003) retrieved from The Free Dictionary by Farlex, Inc. http://www.thefreedictionary.com/cardinal+number
Cardinality	The number of elements in a set or group (considered as a property of that grouping). If the upper limit of the cardinality constraint is 1, the attribute is single, otherwise it is multi-valued.	WordNet 3.0, "Cardinality" (Princeton University, 2012) retrieved from The Free Dictionary by Farlex, Inc. http://www.thefreedictionary.com/cardinality Loucopoulos, P. (Ed.), Lecture Notes in Computer Science: Entity-Relationship Approach (Germany: Springer-Verlag Berlin Heidelberg, 1994), 281.
Chart Type	A method for illustrating data in pictures or images (e.g., bar chart, pie chart, line chart, radar chart, scatterplot).	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 77.
Common Attack Pattern Enumeration and Classification (CAPEC™)	A publically available, community-developed catalog of common attack patterns along with a comprehensive schema and classification taxonomy.	The MITRE Corporation, Common Attack Pattern Enumeration and Classification (2012). http://capec.mitre.org/
Common Configuration Enumeration (CCE™)	The standard nomenclature and dictionary of software misconfigurations. It facilitates fast and accurate correlation of configuration data across multiple information sources and tools.	DHS National Cyber Security Division (NCSD) and NIST, Common Configuration Enumeration Reference Data (2012). http://nvd.nist.gov/cce.cfm
Common Platform Enumeration (CPE™)	A standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.	The MITRE Corporation, Common Platform Enumeration (2012). http://cpe.mitre.org/
Common Vulnerabilities and Exposures (CVE®)	A dictionary of common names (i.e., CVE® Identifiers) for publicly known information security vulnerabilities.	DHS NCSD and The MITRE Corporation, About CVE (2012). http://cve.mitre.org/about/index.html
Common Vulnerability Scoring System (CVSS)	An open framework for communicating the characteristics and impacts of IT vulnerabilities.	DHS NCSD and NIST, NVD Common Vulnerability Scoring System Support v2. http://nvd.nist.gov/cvss.cfm
Common Weakness Enumeration (CWE™)	Provides a unified, measurable set of software weaknesses… [that enables] discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as… understanding and management of software weaknesses related to	DHS NCSD and The MITRE Corporation, Common Weakness Enumeration (2012). http://cwe.mitre.org/

	architecture and design.	
Common Weakness Scoring System (CWSS™)	A mechanism for scoring weaknesses in a consistent, flexible, open manner while accommodating context for the various business domains.	DHS NCSD and The MITRE Corporation, Common Weakness Scoring System (2011). http://cwe.mitre.org/cwss/
Completeness	Including in the authorized and actual inventory all devices of the types which a tool is intended to detect.	DHS FNS
Component	Individual executable files within a software product. These executables may be part of several software products at once.	DHS FNS
Configuration items	Can be hardware, virtual machine, and software (HWCI, VMCI, and SWCI).	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 6.
Configuration management function	Identify, locate, and report misconfiguration of, and missing patches in, IT assets.	DHS FNS
Cyber Observable eXpression (CybOX™)	A standardized language for encoding and communicating high-fidelity information about cyber observables, whether dynamic events or stateful measures that are observable in the operational cyber domain.	DHS NCSD and The MITRE Corporation, About CybOX (2012). http://cybox.mitre.org/about/index.html
Dashboard	A visual display of important information needed to achieve enterprise security posture awareness; which fits entirely on a single computer screen allowing it to be monitored at a glance.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 75.
Data Type	In terms of dashboards and reports, there are two data types: 1. Quantitative, where measurements are expressed in numerical terms (e.g., numbers or percentage), and 2. Qualitative, where measurements are expressed in quality or character (e.g., security category, degree of compliance).	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 76.
Extensible Configuration Checklist Data Format (XCCDF)	A specification language for writing security checklists, benchmarks, and related kinds of documents (i.e., Security Technical Implementation Guides [STIGs], Center for Internet Security [CIS] benchmarks). XCCDF also reports the security checklist evaluation results.	NIST, XCCDF – The Extensible Configuration Checklist Description Format (2012). http://scap.nist.gov/specifications/xccdf/
Frequency	Expressed in time, i.e., monthly, weekly, daily, hourly, and near real-time.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 77.
Functional requirements	The necessary task, action or activity that must be accomplished. Functional (what has to be done) requirements identified in requirements analysis will be used as the top level functions for functional analysis.	DoD Systems Management College, Systems Engineering Fundamentals (Virginia: Defense Acquisition University Press, 2001), 36.

General Support System (GSS)	An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.	Office of Management and Budget (OMB), Circular No. A-130, Memorandum for Heads of Executive Departments and Establishments (1996). http://www.whitehouse.gov/omb/circulars_a130
Hardware inventory management function	Discover and remove unauthorized or unmanaged hardware on a network.	DHS FNS
Information assets	D/A-own or responsible data that are stored, processed, and distributed by IT assets.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 69.
Information security continuous monitoring (ISCM)	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 11.
Information technology (IT) asset	A computing device; it can be a personal computer (PC), server, laptop, mobile device, network equipment, or an appliance.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 72.
IT asset inventory	A complete list of IT assets along with their asset inventory attributes such as property management information and configuration items.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 142.
IT asset inventory baseline	A D/A-established IT asset inventory. An IT asset inventory baseline enables the D/A to identify unauthorized IT assets in its trusted operating environment.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 142.
Lightweight Asset Summary Results (LASR)	An XML schema designed to provide a summary of assessment results to CyberScope.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 155.
Major Application (MA)	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.	OMB, Circular No. A-130, Memorandum for Heads of Executive Departments and Establishments (1996). http://www.whitehouse.gov/omb/circulars_a130
Malware	Malicious software intended to damage or disable IT assets (e.g., computing or networking devices) and compromise information assets.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 69.
Malware Attribute Enumeration and	A standardized language for encoding and communicating high-fidelity information about detected	DHS NCSD and The MITRE Corporation, Malware Attribute

Characterization (MAEC™)	malware based upon attributes such as behaviors, artifacts, and attack patterns.	Enumeration and Characterization (2012). http://maec.mitre.org/
Malware detection and reporting	The ability to discover, identify, characterize, and describe detected malware using a standard language to support a D/A's incident response process.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 8.
May	Compliance is optional, and failure to satisfy the requirement does not require an explicit contractual waiver. Examples are functions that may enhance usability, reliability, interoperability, or quality, etc. (Solutions meeting these requirements will be considered as providing additional value above other required features and functions. Acquiring agencies have wide latitude in determining the relative value of optional requirements in meeting their needs.)	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 10.
Measurement	The quantitative and qualitative units that are the basis for assessing or appraising the security configuration compliance posture.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 76-77.
Must	Compliance with the requirement in its stated form is mandated and cannot be waived contractually by D/As. Examples include government regulations, industry standards, and minimal operational need. (Solutions not meeting these requirements will not be considered acceptable.)	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 10.
Ongoing Security Authorization	A subset of Risk Management Framework (RMF) steps where the system security posture baseline is established through the initial round of full RFM steps. ISCM supports the ongoing security authorization process by continuously assessing, monitoring, and measuring *changes* in system security posture baseline after the system is authorized and in operation.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 141.
Open Checklist Interactive Language (OCIL)	A framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions.	NIST, Security Content Automation Protocol (2012). http://scap.nist.gov/specifications/ocil/
Open Vulnerability Assessment Language (OVAL®)	Standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment.	DHS NCSD and The MITRE Corporation, OVAL Language Overview (2012). http://oval.mitre.org/language/about/overview.html
Operational requirements	Operational requirements will define the basic need and, at a minimum, answer the questions posed [below]: • Operational distribution or deployment: Where will the system be used? • *Mission profile or scenario*: How will the system accomplish its mission	DoD Systems Management College, Systems Engineering Fundamentals (Virginia: Defense Acquisition University Press, 2001), 35.

	objective? • *Performance and related parameters*: What are the critical system parameters to accomplish the mission? • *Utilization environments*: How are the various system components to be used? • *Effectiveness requirements*: How effective or efficient must the system be in performing its mission? • *Operational life cycle*: How long will the system be in use by the user? • *Environment*: What environments will the system be expected to operate in an effective manner?	
Performance requirements	The extent to which a mission or function must be executed; generally measured in terms of quantity, quality, coverage, timeliness or readiness. During requirements analysis, performance (how well does it have to be done) requirements will be interactively developed across all identified functions based on system life cycle factors; and characterized in terms of the degree of certainty in their estimate, the degree of criticality to system success, and their relationship to other requirements.	DoD Systems Management College, Systems Engineering Fundamentals (Virginia: Defense Acquisition University Press, 2001), 36.
Portal Function	A system function that acts as a "conduit" to additional data. This is usually associated to human-computer interaction (HCI).	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 77.
Property management information	A system of data that describes the ownership of IT assets.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 28.
Report	A document that provides data records to support security analysis as well as the diagnoses of vulnerabilities and/or sources of potential exposure.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 75.
Risk Management Framework (RMF)	A common framework that consists of six major steps – categorize, select, implement, assess, authorize, and monitor – that are executed throughout a system life cycle.	NIST, NIST Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach, Rev. 1 (2010). http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
Shall	Compliance with the requirements is required unless an explicit contractual waiver is granted by the contracting agency. Examples include statements that are explicit in	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous

	an agency-provided requirement specification or relate to an agreed-to principle or constraint. (Solutions not meeting these requirements will be considered acceptable only if the requirement is explicitly waived by the acquiring agency.)	Monitoring, v 1.2 (FedBizOpps.gov, 2011), 10.
Should	Compliance with the requirement is not mandatory, and failure to satisfy the requirement does not require an explicit contractual waiver. Vendors and/or agencies may have valid reasons to choose not to implement the requirement, but the full implication must be understood and evaluated. The "should" requirements are designed to promulgate government's operational needs in the near future. (Solutions meeting these requirements will be considered as suitable for meeting future requirements and providing additional value. Acquiring agencies have wide latitude in determining the relative value of non-mandatory requirements in meeting their needs.)	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 10.
Situational awareness analysis and reporting (SAA&R) function	Collect, associate, compile, and report metrics that provide authorized personnel awareness of D/A security posture in terms of IT security governance and operational effectiveness.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 75.
Software	Any executable file(s) (including configuration files that contain metadata that alters how an executable file functions). It includes both software products and components.	DHS FNS
Software product	SWCI at the vendor, name, version, and update level of detail, including all configuration items within that release.	DHS FNS
Software Assurance Findings Expression Schema (SAFES)	A unified schema that will support the full range of software assurance activities in a consistent and automatable fashion by providing a common mechanism (structure and content) for all tools, analysis services and analysis practices in the software assurance field to report, integrate and analyze findings in a consistent fashion.	Barnum, S., The MITRE Corporation, Software Assurance Findings Expression Schema (SAFES) Overview (2012). http://www.mitre.org/work/tech_papers/2012/11_3671/
Software inventory management function	Discover and remove unauthorized or unmanaged SWCI in IT assets on a network.	DHS FNS
Component	Individual executable files within a software product. Sometimes these executables may be part of several software products at once.	DHS FNS
System interface	The point of interaction or communication between two functional system entities.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 155.
Timeliness	The high level of confidence that the data in the authorized and actual inventory reflect the most recent changes that can be feasibly detected, that is, rapid cycles for updating the data sets, and negligible delay between an physical change and the change in the data	DHS FNS

	reported, even across large, complex, and heterogeneous network infrastructures, without interfering with or degrading normal network operations.	
Trusted communication	A data communication path with the ability to protect confidentiality and integrity of data-in-transit.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 52.
Unauthorized hardware	Hardware that is not in the authorized inventory, or is in that inventory, but is not assigned to a service organization/POC for management, or is in that inventory, but is behaving in a way inconsistent with the authorized asset (for example, a workstation acting like a switch), or is a device establishing an unauthorized external/internal connection.	DHS FNS
Vulnerability	A state (or condition) which renders an IT asset vulnerable to exploitation or attack by a threat agent (or cyber adversary).	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 7.
Vulnerability management	The management of risks presented by known software weaknesses that are subject to exploitation.	DHS FNS
Vulnerability management function	Discover and support remediation of vulnerabilities in IT assets on a network.	DHS FNS
Weaknesses	Both bugs, which are implementation-level software problems, and flaws, which are design-level software problems.	DHS FNS, SAIR Tier III Product Performance Requirements for Information Security Continuous Monitoring, v 1.2 (FedBizOpps.gov, 2011), 7.

1475

1476 **6 Acronyms**

1477

Acronym	Term
AD	Active Directory
AOR	Area of Responsibility
API	Application Programming Interface
ARF	Asset Reporting Format
ASR	Asset Summary Results
AV	Anti-Virus
CAG	Consensus Audit Guidelines
CAESARS	Continuous Asset Evaluation, Situational Awareness, and Risk Scoring
CAESARS FE	CAESARS Framework Extension
CAPEC™	Common Attack Pattern Enumeration and Classification
CCE™	Common Configuration Enumeration
CCSS	Common Configuration Scoring System
CERT	Computer Emergency Response Team
CI	Configuration Item
CIO	Chief Information Officer
CIS	Center for Internet Security
CMDB	Configuration Management Database
CNSSI	Committee on National Security Systems Instruction
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CPE™	Common Platform Enumeration
CVE®	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE™	Common Weakness Enumeration
CWSS™	Common Weakness Scoring System
CybOX™	Cyber Observable eXpression
D/A	Departments/Agencies
DB	Database
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDI	DoD Instruction
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standard
FISMA	Federal Information System Management Act
FNS	Federal Network Security
FY	Fiscal Year
GSS	General Support System
GUI	Graphical User Interface
HWCI	Hardware Configuration Item
ID	Identifier

IP	Internet Protocol
IR	Interagency Report
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
IT	Information Technology
LAN	Local Area Network
LASR	Lightweight Asset Summary Results
LDAP	Lightweight Directory Access Protocol
MA	Major Application
MAC	Media Access Control
MAEC™	Malware Attribute Enumeration and Characterization
MNS	Mission Needs Statement
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OCIL	Open Checklist Interactive Language
OMB	Office of Management and Budget
OU	Organizational Unit
OVAL®	Open Vulnerability Assessment Language
PC	Personal Computer
PWS	Performance Work Statement
RBD	Risk-Based Decision
RMF	Risk Management Framework
SAA&R	Situational Awareness Analysis and Reporting
SAFES	Software Assurance Findings Expression Schema
SAIR	Situational Awareness Incident Response
SCAP	Security Content Automation Protocol
SCM	Security Configuration Management
SDLC	Systems Development Life Cycle
SELC	Systems Engineering Life Cycle
SOO	Statement of Objectives
SP	Special Publication
STIG	Security Technical Implementation Guide
SWCI	Software Configuration Item
US-CERT	United States Computer Emergency Response Team
USB	Universal Serial Bus
USG	United States Government
USGCB	United States Government Configuration Baseline
VMCI	Virtual Machine Configuration Item
VUL	Vulnerability
WAN	Wide Area Network
XCCDF	Extensible Configuration Checklist Definition Format
XML	Extensible Markup Language

1478

Cloud Service Provider Proposal Review Process: Fast and Custom Service

I. Fast Lane.

The purpose of the fast lane is to provide quick review and approval for service provider offerings which are equivalent to use-cases which have already been approved. As illustrated in *Figure 1, Fast Lane Process Flow*, this allows the offering to proceed almost immediately to assessment and provisional authorization.

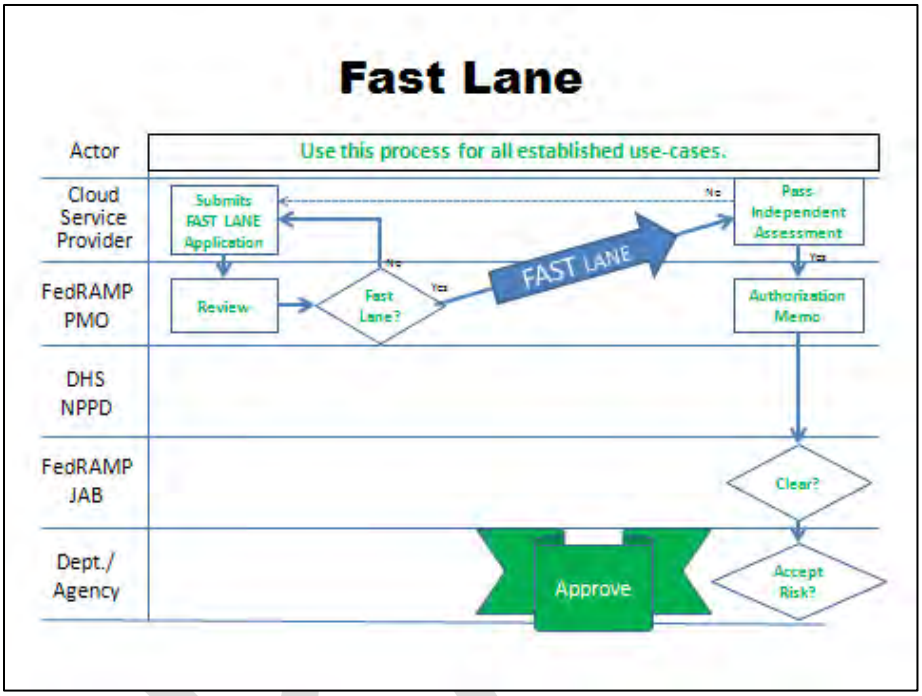

Figure 1: Fast Lane Process Flow

The FedRAMP Program Management Office (PMO) shall maintain a list of preapproved use case scenarios, which will be available to service providers. If service provider offerings are fully consistent with a particular use case, then it can be approved without further review. The Department of Homeland Security (DHS) does not need to review these applications.

If the service provider submits a Fast Lane application, and the FedRAMP PMO determines that it does not meet Fast Lane criteria, the application will be returned to the service provider to prepare for Custom Lane review. Examples of preapproved use cases are as follows:

1. Cloud Service Provider offerings which will be used to contain data/information which is low-impact for confidentiality even if moderate for integrity and high for availability. To use this strategy, the implementing agency must be able to quickly restore the site to its original state if defaced, and over time, experience should show that such defacements are rare.
   The following exceptions would preclude use of this strategy:
   - Inclusion of any sensitive business information on the website;
   - Collection of data which could not be easily restored from backup because of frequent changes; and,
   - Inability of the customer agency to maintain an off-site backup of the information and/or to restore a defaced site quickly enough to meet integrity/availability requirements.

2. Cloud based Intranet Service Providers which provide controls equivalent to the National Institutes of Science and Technology (NIST) special publication 800-53 and Federal Information Processing Standards Publication (FIPS*)* baseline for moderate and high, where the agency can demonstrate to the FedRAMP Joint Advisory Board that there is clear policy and practice in place to prevent classified information from being included in the system.

II. Custom Lane:

The purpose of the custom lane is to provide adequate review and approval for service provider offerings which are new and/or unique use cases which have not already been approved. This allows the FedRAMP program to consider innovative and unusual proposals. Once these use cases are approved they will be added to Fast Lane criteria and used by other providers with an equivalent use case.

Custom Lane proposals received their primary review from DHS who will work with the service providers and the FedRAMP PMO to ensure that approved proposals carefully balance security needs and operational business concerns, including the cost of proposals. The DHS reviewers will consider innovative and effective methods that produce actual security capability, while allowing providers the leeway to innovate to improve security while controlling or reducing costs.

The Custom Lane process submits the DHS review and recommendation to the FedRAMP Joint Advisory Board (JAB) for a provisional-authorization decision whether or not the DHS review determines that the proposal is adequate. It is the responsibility of the FedRAMP JAB to decide for the government whether the risk-based assessment of the offering indicates that the FIPS 199 risk is low enough to grant provisional approval.

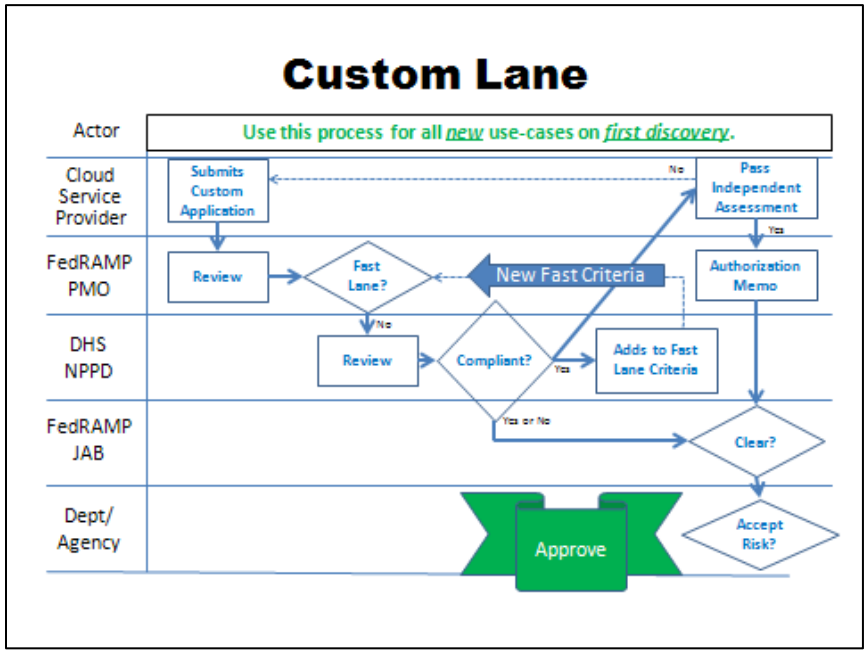

Figure 2: Custom Lane Process Flow

Proposed Phasing of Continuous Monitoring Requirements

Phase 1: First Year of Funding (FY2013 Proposed)

(1) Hardware Asset Management
(2) Software Asset Management and Software White Listing
    - Including Anti-Virus Tools
(3) Vulnerability Management
(4) Configuration Management
(5) Anti-virus (see #2 above)

Note: Implementing each of these areas assumes that normal lifecycle measures are taken within each area from architecture through operational quality control.

Phase 2: Second Year of Funding

(1) Network and Physical Boundary Access Controls Managing Trust in those Granted Access (Personnel Security Clearances)
(2) Managing the Behavior of those Granted Trust (Awareness and Role-based Security Training)
(3) Managing Credential and Authentication
(4) Managing Access Control List for Accounts
(5) Generic Auditing and Monitoring (Part 1 – Establishing Logs)

Note: Within areas 2-5, highest priority goes to users and accounts with higher privileges, and lower priority goes to normal unprivileged user accounts.

Phase 3: Third Year of Funding

(1) Generic Auditing and Monitoring (Part 2 – Establishing Log Analysis and Integration)
(2) Preparing to Respond to Events (Incidents and other Contingencies)
(3) Managing Reponses to Events (Incidents and other Contingencies)
(4) Security Program Level Requirements Policy and Planning
(5) Security Program Level Quality Management
(6) Operations Management

Capability	Class	Function	Short Title	Category	Impact (General)	Points	Points (out of 1000)	Notes
CSP.TM.AU.01	TIC Management	Authentication	User Authentication	Critical	5	50	26.73796791	
CSP.TM.COM.01	TIC Management	Secure Communications	TIC and US-CERT (TS/SCI)	Critical	2	5	2.673796791	
CSP.TM.COM.02	TIC Management	Secure Communications	TIC and Customer	Critical	5	50	26.73796791	
CSP.TM.COM.03	*TIC Management*	*Secure Communications*	*TIC and US-CERT (SECRET)*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TM.DS.01	TIC Management	Data Storage	Storage Capacity	Critical	4	25	13.36898396	
CSP.TM.DS.02	TIC Management	Data Storage	Back up Data	Critical	4	25	13.36898396	
CSP.TM.DS.03	*TIC Management*	*Data Storage*	*Data Ownership*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TM.DS.04	*TIC Management*	*Data Storage*	*Data Attribution & Retrieval*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TM.DS.05	*TIC Management*	*Data Storage*	*DLP*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TM.LOG.01	TIC Management	Logging	NTP Server	Critical	3	15	8.021390374	
CSP.TM.LOG.02	TIC Management	Logging	Time Stamping	Critical	3	15	8.021390374	
CSP.TM.LOG.03	TIC Management	Logging	Session Traceability	Critical	5	50	26.73796791	
CSP.TM.LOG.04	*TIC Management*	*Logging*	*Log Retention*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TM.PC.01	TIC Management	Physical Controls	TIC Facility	Critical	4	25	13.36898396	
CSP.TM.PC.02	TIC Management	Physical Controls	NOC/SOC Facilities	Critical	3	15	8.021390374	
CSP.TM.PC.03	TIC Management	Physical Controls	SCIF Facilities	Critical	2	5	2.673796791	
CSP.TM.PC.04	TIC Management	Physical Controls	Dedicated TIC Spaces	Critical	5	150	80.21390374	
CSP.TM.PC.05	TIC Management	Physical Controls	Facility Resiliency	Critical	3	15	8.021390374	
CSP.TM.PC.06	TIC Management	Physical Controls	Geographic Diversity	Critical	3	15	8.021390374	
CSP.TM.TC.01	TIC Management	TIC Configuration	Route Diversity	Critical	3	15	8.021390374	
CSP.TM.TC.02	TIC Management	TIC Configuration	Least Functionality	Critical	5	50	26.73796791	
CSP.TM.TC.03	TIC Management	TIC Configuration	IPv6	Critical	3	15	8.021390374	
CSP.TM.TC.04	*TIC Management*	*TIC Configuration*	*DNS Authoritative Servers*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TM.TC.05	TIC Management	TIC Configuration	Response Authority	Critical	5	50	26.73796791	
CSP.TM.TC.06	TIC Management	TIC Configuration	TIC staffing	Critical	5	50	26.73796791	
CSP.TM.TC.07	TIC Management	TIC Configuration	Response Access	Critical	5	50	26.73796791	
CSP.TO.MG.01	TIC Oversight	Management	System Inventory	Critical	5	50	26.73796791	
CSP.TO.MG.02	TIC Oversight	Management	Change & Configuration Management	Critical	5	50	26.73796791	
CSP.TO.MG.03	TIC Oversight	Management	Change Communication	Critical	2	5	2.673796791	
CSP.TO.MG.04	*TIC Oversight*	*Management*	*Contingency Planning*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.MG.05	TIC Oversight	Management	TSP	Critical	3	15	8.021390374	
CSP.TO.MG.06	TIC Oversight	Management	Maintenance Scheduling	Critical	5	50	26.73796791	
CSP.TO.MG.07	*TIC Oversight*	*Management*	*Network Inventory*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.MG.08	*TIC Oversight*	*Management*	*SLA*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.MG.09	*TIC Oversight*	*Management*	*Exception Process*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.MG.10	*TIC Oversight*	*Management*	*Tailored Security Policies*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.MG.11	*TIC Oversight*	*Management*	*Tailored Communications*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.MON.01	TIC Oversight	Monitoring/Audit	Situational Awareness	Critical	5	50	26.73796791	
CSP.TO.MON.02	TIC Oversight	Monitoring/Audit	Vulnerability Scanning	Critical	3	15	8.021390374	
CSP.TO.MON.03	TIC Oversight	Monitoring/Audit	Audit Access	Critical	3	15	8.021390374	
CSP.TO.MON.04	*TIC Oversight*	*Monitoring/Audit*	*Log Sharing*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.MON.05	*TIC Oversight*	*Monitoring/Audit*	*Operational Exercises*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.REP.01	*TIC Oversight*	*Reporting*	*Customer Service Metrics*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.REP.02	*TIC Oversight*	*Reporting*	*Operational Metrics*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.REP.03	*TIC Oversight*	*Reporting*	*Customer Notification*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.REP.04	TIC Oversight	Reporting	Incident Reporting	Critical	5	50	26.73796791	
CSP.TO.RES.01	TIC Oversight	Response	Response Timeframe	Critical	3	15	8.021390374	
CSP.TO.RES.02	*TIC Oversight*	*Response*	*Response Guidance*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.RES.03	TIC Oversight	Response	Denial of Service Response	Critical	4	25	13.36898396	
CSP.TS.CF.01	TIC Services	Content Filtering	Application Layer Filtering	Critical	5	50	26.73796791	
CSP.TS.CF.02	TIC Services	Content Filtering	Web Session Filtering	Critical	4	25	13.36898396	
CSP.TS.CF.03	*TIC Services*	*Content Filtering*	*Web Firewall*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.04	TIC Services	Content Filtering	Mail Filtering	Critical	5	50	26.73796791	
CSP.TS.CF.05	TIC Services	Content Filtering	Agency Specific Mail Filters	Critical	5	50	26.73796791	
CSP.TS.CF.06	TIC Services	Content Filtering	Mail Forgery Detection	Critical	5	50	26.73796791	
CSP.TS.CF.07	*TIC Services*	*Content Filtering*	*Digitally Signing Mail*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.08	*TIC Services*	*Content Filtering*	*Mail Quarantine*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.09	*TIC Services*	*Content Filtering*	*Crypto-graphically authenicated protocols*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.10	TIC Services	Content Filtering	Reducing Cleartext	Critical	5	50	26.73796791	
CSP.TS.CF.11	TIC Services	Content Filtering	Encrypted Traffic Inspection	Critical	3	15	8.021390374	
CSP.TS.CF.12	*TIC Services*	*Content Filtering*	*User Authentication*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.13	TIC Services	Content Filtering	DNS Filtering	Critical	4	25	13.36898396	
CSP.TS.INS.01	TIC Services	Inspection	NCPS	Critical	5	150	80.21390374	
CSP.TS.INS.02	TIC Services	Inspection	IDS/NIDS	Critical	3	15	8.021390374	
CSP.TS.PF.01	TIC Services	Packet Filtering	Secure all TIC traffic	Critical	5	50	26.73796791	
CSP.TS.PF.02	TIC Services	Packet Filtering	Default Deny	Critical	5	50	26.73796791	

CSP.TS.PF.03	TIC Services	Packet Filtering	Stateless Filtering	Critical	4	25	13.36898396	
CSP.TS.PF.04	TIC Services	Packet Filtering	Stateful Filtering	Critical	4	25	13.36898396	
CSP.TS.PF.05	TIC Services	Packet Filtering	Filter by Source Address	Critical	2	5	2.673796791	
CSP.TS.PF.06	TIC Services	Packet Filtering	Asymmetric Routing	Critical	2	5	2.673796791	
CSP.TS.PF.07	*TIC Services*	*Packet Filtering*	*H.323*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TS.RA.01	TIC Services	Remote Access	Agency-User Remote Access	Critical	5	50	26.73796791	
CSP.TS.RA.02	TIC Services	Remote Access	External Dedicated Access	Critical	5	150	80.21390374	
CSP.TS.RA.03	*TIC Services*	*Remote Access*	*Extranet Dedicated Access*	*Recommended*				*Recommended Capabilities are not Required*
						1870	1000	

Capability	Class	Function	Short Title	Category	Impact (General)	Points	Points (out of 1000)	Notes
CSP.TM.AU.01	TIC Management	Authentication	User Authentication	Critical	5	50	26.73796791	
CSP.TM.COM.01	TIC Management	Secure Communications	TIC and US-CERT (TS/SCI)	Critical	2	5	2.673796791	
CSP.TM.COM.02	TIC Management	Secure Communications	TIC and Customer	Critical	5	50	26.73796791	
CSP.TM.COM.03	*TIC Management*	*Secure Communications*	*TIC and US-CERT (SECRET)*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TM.DS.01	TIC Management	Data Storage	Storage Capacity	Critical	4	25	13.36898396	
CSP.TM.DS.02	TIC Management	Data Storage	Back up Data	Critical	4	25	13.36898396	
CSP.TM.DS.03	*TIC Management*	*Data Storage*	*Data Ownership*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TM.DS.04	*TIC Management*	*Data Storage*	*Data Attribution & Retrieval*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TM.DS.05	*TIC Management*	*Data Storage*	*DLP*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TM.LOG.01	TIC Management	Logging	NTP Server	Critical	3	15	8.021390374	
CSP.TM.LOG.02	TIC Management	Logging	Time Stamping	Critical	3	15	8.021390374	
CSP.TM.LOG.03	TIC Management	Logging	Session Traceability	Critical	5	50	26.73796791	
CSP.TM.LOG.04	*TIC Management*	*Logging*	*Log Retention*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TM.PC.01	TIC Management	Physical Controls	TIC Facility	Critical	4	25	13.36898396	
CSP.TM.PC.02	TIC Management	Physical Controls	NOC/SOC Facilities	Critical	3	15	8.021390374	
CSP.TM.PC.03	TIC Management	Physical Controls	SCIF Facilities	Critical	2	5	2.673796791	
CSP.TM.PC.04	TIC Management	Physical Controls	Dedicated TIC Spaces	Critical	5	150	80.21390374	
CSP.TM.PC.05	TIC Management	Physical Controls	Facility Resiliency	Critical	3	15	8.021390374	
CSP.TM.PC.06	TIC Management	Physical Controls	Geographic Diversity	Critical	3	15	8.021390374	
CSP.TM.TC.01	TIC Management	TIC Configuration	Route Diversity	Critical	3	15	8.021390374	
CSP.TM.TC.02	TIC Management	TIC Configuration	Least Functionality	Critical	5	50	26.73796791	
CSP.TM.TC.03	TIC Management	TIC Configuration	IPv6	Critical	3	15	8.021390374	
CSP.TM.TC.04	*TIC Management*	*TIC Configuration*	*DNS Authoritative Servers*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TM.TC.05	TIC Management	TIC Configuration	Response Authority	Critical	5	50	26.73796791	
CSP.TM.TC.06	TIC Management	TIC Configuration	TIC staffing	Critical	5	50	26.73796791	
CSP.TM.TC.07	TIC Management	TIC Configuration	Response Access	Critical	5	50	26.73796791	
CSP.TO.MG.01	TIC Oversight	Management	System Inventory	Critical	5	50	26.73796791	
CSP.TO.MG.02	TIC Oversight	Management	Change & Configuration Management	Critical	5	50	26.73796791	
CSP.TO.MG.03	TIC Oversight	Management	Change Communication	Critical	2	5	2.673796791	
CSP.TO.MG.04	*TIC Oversight*	*Management*	*Contingency Planning*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.MG.05	TIC Oversight	Management	TSP	Critical	3	15	8.021390374	
CSP.TO.MG.06	TIC Oversight	Management	Maintenance Scheduling	Critical	5	50	26.73796791	
CSP.TO.MG.07	*TIC Oversight*	*Management*	*Network Inventory*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.MG.08	*TIC Oversight*	*Management*	*SLA*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.MG.09	*TIC Oversight*	*Management*	*Exception Process*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.MG.10	*TIC Oversight*	*Management*	*Tailored Security Policies*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.MG.11	*TIC Oversight*	*Management*	*Tailored Communications*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.MON.01	TIC Oversight	Monitoring/Audit	Situational Awareness	Critical	5	50	26.73796791	
CSP.TO.MON.02	TIC Oversight	Monitoring/Audit	Vulnerability Scanning	Critical	3	15	8.021390374	
CSP.TO.MON.03	TIC Oversight	Monitoring/Audit	Audit Access	Critical	3	15	8.021390374	
CSP.TO.MON.04	*TIC Oversight*	*Monitoring/Audit*	*Log Sharing*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.MON.05	*TIC Oversight*	*Monitoring/Audit*	*Operational Exercises*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.REP.01	*TIC Oversight*	*Reporting*	*Customer Service Metrics*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.REP.02	*TIC Oversight*	*Reporting*	*Operational Metrics*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.REP.03	*TIC Oversight*	*Reporting*	*Customer Notification*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TO.REP.04	TIC Oversight	Reporting	Incident Reporting	Critical	5	50	26.73796791	
CSP.TO.RES.01	TIC Oversight	Response	Response Timeframe	Critical	3	15	8.021390374	
CSP.TO.RES.02	*TIC Oversight*	*Response*	*Response Guidance*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TO.RES.03	TIC Oversight	Response	Denial of Service Response	Critical	4	25	13.36898396	
CSP.TS.CF.01	TIC Services	Content Filtering	Application Layer Filtering	Critical	5	50	26.73796791	
CSP.TS.CF.02	TIC Services	Content Filtering	Web Session Filtering	Critical	4	25	13.36898396	
CSP.TS.CF.03	*TIC Services*	*Content Filtering*	*Web Firewall*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.04	TIC Services	Content Filtering	Mail Filtering	Critical	5	50	26.73796791	
CSP.TS.CF.05	TIC Services	Content Filtering	Agency Specific Mail Filters	Critical	5	50	26.73796791	
CSP.TS.CF.06	TIC Services	Content Filtering	Mail Forgery Detection	Critical	5	50	26.73796791	
CSP.TS.CF.07	*TIC Services*	*Content Filtering*	*Digitally Signing Mail*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.08	*TIC Services*	*Content Filtering*	*Mail Quarantine*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.09	*TIC Services*	*Content Filtering*	*Crypto-graphically authenicated protocols*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.10	TIC Services	Content Filtering	Reducing Cleartext	Critical	5	50	26.73796791	
CSP.TS.CF.11	TIC Services	Content Filtering	Encrypted Traffic Inspection	Critical	3	15	8.021390374	
CSP.TS.CF.12	*TIC Services*	*Content Filtering*	*User Authentication*	*Recommended*				*Recommended Capabilities are not Required*
CSP.TS.CF.13	TIC Services	Content Filtering	DNS Filtering	Critical	4	25	13.36898396	
CSP.TS.INS.01	TIC Services	Inspection	NCPS	Critical	5	150	80.21390374	
CSP.TS.INS.02	TIC Services	Inspection	IDS/NIDS	Critical	3	15	8.021390374	
CSP.TS.PF.01	TIC Services	Packet Filtering	Secure all TIC traffic	Critical	5	50	26.73796791	
CSP.TS.PF.02	TIC Services	Packet Filtering	Default Deny	Critical	5	50	26.73796791	

CSP.TS.PF.03	TIC Services	Packet Filtering	Stateless Filtering	Critical	4	25	13.36898396	
CSP.TS.PF.04	TIC Services	Packet Filtering	Stateful Filtering	Critical	4	25	13.36898396	
CSP.TS.PF.05	TIC Services	Packet Filtering	Filter by Source Address	Critical	2	5	2.673796791	
CSP.TS.PF.06	TIC Services	Packet Filtering	Asymmetric Routing	Critical	2	5	2.673796791	
CSP.TS.PF.07	*TIC Services*	*Packet Filtering*	*H.323*	*N/A - See Notes*				*N/A to Cloud and/or Covered by Contract Requirements*
CSP.TS.RA.01	TIC Services	Remote Access	Agency-User Remote Access	Critical	5	50	26.73796791	
CSP.TS.RA.02	TIC Services	Remote Access	External Dedicated Access	Critical	5	150	80.21390374	
CSP.TS.RA.03	*TIC Services*	*Remote Access*	*Extranet Dedicated Access*	*Recommended*				*Recommended Capabilities are not Required*
						1870	1000	

Boundary Defense for the Cloud
Critical Technical Capabilities
Assessment Workbook
CSP 1.0

Homeland Security

Revision History

Date	Name	Revision
10MAY2012	A. Cooper J. Downing B. Kennedy	Initial release of workbook template

Table of Contents

Summary of Changes

This workbook is a working draft adaptation of the CCV TIC 2.0 Capabilities Assessment workbook. Of the 74 TIC 2.0 Required Capabilities:

- The 14 Recommended /Optional Capabilities were removed
- An additional 11 Capabilities that will be met through other FedRAMP requirements and/or standard customer contract clauses were also removed
- The remaining 49 Required Capabilities identified as applicable to Cloud Providers are documented in this workbook

Capability #CSP.TM.AU.01 (Critical)			
CSP systems and components that support government customer instances comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199). Administrative access to government customer instance devices requires multi-factor authentication (OMB M-11-11).			
Clarification			
Multi-factor authentication is required for high impact systems in order to reduce the threat of unauthorized people from making changes to critical infrastructure. Multi-factor Authentication is defined as using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multi-factor authentication must be performed at the device level (not just access-coded entry into the room where the devices are located) for all administrative users.			
Team Guidance			
Multi-factor authentication to gain access to the console or administrative level equivalent (administrative GUI or web interface) of the device is required. A multi-factor authentication device on a server room door is not a valid substitute for implementing multi-factor authentication on the device. (e.g., remote administration may be possible).			
Examples of Evidence Sought			
- Demonstration of multi-factor authentication to access a CSP device - Audit logs showing which authentication devices methods were used to gain access to a device (this includes audit logs for console machines, and if access is via any remote devices those remote systems are also are capturing audit logs to demonstrate multi-factor authentication)			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	❒	❒	
The CSP uses multi-factor authentication for network and local access to privileged accounts on CSP devices.	❒	❒	
The CSP: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; OR (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator	❒	❒	

Factors used for authentication to access privileged accounts must be separate and independent of the information system being accessed.		❒	❒	
The CSP uses replay-resistant authentication mechanisms for privileged accounts.		❒	❒	
Institutional				
The CSP has defined policies or guidance for maintaining multi-factor authentication for CSP components.		❒	❒	
The CSP has defined processes in place to ensure that the authorized list of users is current and maintained according to organizational guidelines.		❒	❒	
The CSP has staff practices in place to ensure only those who have access to the multi-factor devices are administrating the devices. (For example, an authorized user allows the use of their account by an unauthorized individual)		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.COM.01 (Critical)

The CSP has a minimum of three qualified people with TOP SECRET/SCI clearance available within 2 hours, 24x7x365, with authority to report, acknowledge and initiate action based on TOP SECRET/SCI-level information, including tear line information, with US-CERT.

Authorized personnel with TOP SECRET/SCI clearances have 24x7x365 access to an ICD 705-accredited Sensitive Compartment Information Facility (SCIF) including the following TOP SECRET/SCI communications channels:
- Secure telephone (STE/STU) and card authorized for TOP SECRET/SCI
- Secure FAX machine

Typically personnel with appropriate clearances to handled classified information will include at least the Senior NOC/SOC manager, Chief Information Security Officer (CISO), and Chief Information Officer (CIO), and other personnel as determined by the agency. The SCIF may be shared with another agency and should be within 30 minutes of the CSP management location, during normal conditions, in order for authorized personnel to exchange classified information, evaluate the recommendations, initiate the response and report operational status with US-CERT within two hours of the notification.

Clarification

The intent is at least one qualified person with TS/SCI clearance is always available (on-call, including weekends and holidays) to exchange classified communications within 2 hours. It is acceptable for uncleared personnel to escalate the incident to on-call TS/SCI personnel.
CSPs must have the personnel and equipment to receive and act upon information disseminated from any agency and from US-CERT at the TS/SCI level.
The CSP must be able to describe the SCIF and TS/SCI communication channels, and demonstrate the equipment supporting the communication channels within the SCIF during the on-site CSP assessment.

Team Guidance

The top-secret-level personnel have a total of 2 hours to get to the CSP management location and from there to the ICD 705 accredited SCIF.
The responding personnel must have immediate access to a person with the authority to initiate changes to the CSP infrastructure and configuration including limiting or terminating external connections based on the information received.

The SCIF does not need to be co-located, physically adjacent, or adjoined to the CSP management location.
The intent is to validate the CSP can communicate with US-CERT at the TS/SCI level.
Note: A regular closed area does not constitute a SCIF for handling TS/SCI materials.

Examples of Evidence Sought

The CSP can demonstrate:
- at least one person on the SOC staff is cleared at the TS/SCI level, and that this individual has been indoctrinated for unescorted SCIF access and handling procedures for SCI
- it has access to the SCIF within 30 minutes, including an escorted visit to the SCIF by a qualified/cleared member of the SOC team
- the SCIF has communications equipment capable of handling information up to, and including the TS/SCI level. This can include JWICS terminals, phones accredited for TS/SCI, etc.

The CSP can provide: - a C+A letter stating that its SCIF is compliant with DCID 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities					
Scoring Criteria					
		Yes	No	Evidence	
Technical					
The CSP has a minimum of three qualified people with TOP SECRET/SCI clearance available within 2 hours, 24x7x365, with authority to report, acknowledge and initiate action based on TOP SECRET/SCI-level information, including tear line information, with US-CERT.		❒	❒		
Authorized personnel with TOP SECRET/SCI clearances have 24x7x365 access to an ICD 705-accredited Sensitive Compartment Information Facility (SCIF).		❒	❒		
A Secure telephone (STE/STU) and card authorized for TOP SECRET/SCI is available for use in the SCIF.		❒	❒		
A Secure FAX machine is available within the SCIF.		❒	❒		
The SCIF is located within 30 minutes of the CSP management location (during normal conditions).					
Institutional					
The CSP has defined policies or guidance in place specifying access to and operations of the SCIF.		❒	❒		
The CSP has defined processes in place to specify how to access the SCIF, operate the equipment, and communicate with US-CERT.		❒	❒		
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒		
The CSP has the appropriate tools in place to perform this capability.		❒	❒		
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TM.COM.02 (Critical)

The CSP secures and authenticates the administrative communications (i.e. customer service) between the CSP and each government customer instance.

Clarification

All CSPs are encouraged to have secure communications.
CSPs must have secure mechanisms that can be used between the CSP and each government customer instance so that the CSP (particularly the SOC) can conduct secure, confidential, and authenticated exchange of information.

NOTE: This will be a required capability for all CSPs, and they will also need ability to conduct secure communications at SECRET (or higher)

Team Guidance

For example, methods may include, but not limited to, using HTTPS for administrative web sites, calling back the client at a pre-authorized telephone number to confirm changes, cryptographically signing e-mail messages or similar processes. This does not require ordinary business communications between the CSP and client use classified communication channels; but CSPs and clients may agree to use additional security and authentication requirements.

This capability focuses on the ability of the CSP to provide customer service information and/or communication to its subscriber(s) in a secure method (a customer service portal over HTTPS, HSDN, access to US-CERT SECRET level website, etc.).

Examples of Evidence Sought

The CSP can demonstrate:
- how it meets secure electronic communication requirements—this can include a set of customer specific requirements and an explanation of how the specific requirements are met
- required hardware and/or software in use
- required configuration in place
- sample communications that verify specific requirements are being met
- a demonstration of sending of secure communications

CSP can provide:
- customer specific SLA
- documented policies on secure communications with customers
- documented procedures that describe the process for collecting and implementing individual customer agencies' secure electronic communication requirements
- QA test/audit reports of secure communications

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP provides secure electronic communication to its current customers that meet customer requirements.	❒	❒	

The CSP has an operational definition of "administrative communications"		❒	❒	
The CSP secures and authenticates the administrative communications between the CSP and each government customer instance.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place to manage customer agencies' secure electronic communication requirements		❒	❒	
The CSP has defined processes in place for collecting and implementing customer agencies' secure electronic communication requirements.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.DS.01 (Critical)			
Each government customer instance must be able to perform real-time header and content capture of all inbound and outbound traffic for administrative, legal, audit or other operational purposes. The CSP has storage capacity to retain at least 24 hours of data generated at full CSP operating capacity. The CSP is able to selectively filter and store a subset of inbound and outbound traffic.			
Clarification			
Full CSP operating capacity is the sum of all external connection bandwidth.			
Team Guidance			
The total storage requirement is calculated as follows, where T is the total external bandwidth provided by the CSP: T Mb/s * 86400 s/day * = P Mb/day P Mb/day / 8 = Q MB/day Q MB/day / 1,000,000 ~= Y TB/day. The CSP needs adequate data storage for Y TB/day.			
Examples of Evidence Sought			
The CSP can demonstrate: - The process for reviewing header and packet capture for up to 24 hours. - The total and utilized storage capacity through the storage system management interface. - The process of responding to reaching packet capture storage system threshold or failure. - The process for selectively filtering and storing a subset of inbound and outbound traffic. The CSP can provide: An Audit and Accountability Policy that: - Specifies the amount of storage required to retain real time header and packet capture for 24 hours. - Specifies that alerts should be sent in the event of a packet capture storage system failure or reaching capacity thresholds. - Process and procedures for responding to packet capture storage system alerts. - Specifies thresholds for packet capture storage system capacity alerts. - Specifies the packet capture storage system must have the ability to selectively filter and store a subset of inbound and outbound traffic. - The amount of simultaneous bandwidth per second for external connections – e.g. 600 mb/s.			
Scoring Criteria			
	Yes	No	Evidence
Technical			

The CSP has the ability to and is able to demonstrate it can selectively filter and store a subset of inbound or and outbound traffic.		❒	❒	
The CSP has storage capacity to retain at least 24 hours of data inbound and outbound network traffic, including both packet headers and content, generated at full CSP operating capacity.		❒	❒	
Institutional				
The CSP has the appropriately trained, credentialed personnel in place to recognize and respond to storage system capacity thresholds or failures.		❒	❒	
The CSP has the tools in place to detect storage system capacity thresholds or failures and alert the appropriate personnel.		❒	❒	
The CSP has defined policies or guidance in place to specify storage capacity to retain at least 24 hours of data generated at full CSP operating capacity.		❒	❒	
The CSP has defined policies or guidance in place to specify the ability to selectively filter and store a subset of inbound or outbound traffic.		❒	❒	
The CSP has defined processes in place that specify how to maintain at least 24 hours of data generated at full CSP operating capacity.		❒	❒	
The CSP has defined processes in place that specify how to selectively filter and store a subset of inbound or outbound traffic.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.DS.02 (Critical)
In the event of a CSP system failure or compromise, the CSP has the capability to restore operations to a previous clean state. Backups of configurations and data are maintained off-site in accordance with the CSP continuity of operations plan.
Clarification
The intent is to keep backup data long enough to support restoration and continuity of operations. It does not create longer data retention requirements. The CSP must have the resources in place to be able to restore a system to a previously functioning state in case of a system failure or to reconstitute it in the event of an outage or catastrophe. All backup data (i.e., logs, system state information, and user data) is to be maintained for a stipulated period of time for historical and forensic reconstruction of any event. This applies to all data collected or created by the CSP, NOC, and SOC systems.
Team Guidance
Assessment teams should look for a backup policy and ensure the department and/or agency is following it. Individuals handling backup data must be credentialed or cleared commensurate with the contents of the backups (e.g., if backup data is classified as Top Secret, individuals must have the equivalent credentials). This capability can also be accomplished by mirroring data at another facility; however, the CSP must be able to reconstitute the systems in the event of an outage. The type of medium used for the backups is irrelevant.
Examples of Evidence Sought
The CSP can demonstrate: - what is backed up (such as configurations for the CSP devices or appliances, OS storage, incident data (tracking system), and log files - agency back-up policy or requirements that are being followed - what offsite storage facility is used - secure transfer of data including the backup timeframe (i.e., personnel who transport the data must possess the same security credentials as the on-site personnel) - regular testing of off-site backups The CSP can provide: - evidence of 5 years of data stored off-site - clearly defined backup policy and restoration procedure to recover data or reconstitute systems in the event of an outage - supporting documentation for testing off-site backups (e.g., test plan, test results) that is consistent with NIST standards - QA test/audit reports of off-site storage of backup data
Scoring Criteria

		Yes	No	Evidence
Technical				
The CSP can reconstitute the CSP and associated systems in the event of a system failure or catastrophe in accordance with agency/customer defined policy/guidance.		❒	❒	
The CSP backup data is handled only by individuals cleared commensurate with the contents of the backups.		❒	❒	
The CSP maintains backups of configurations and data off-site in accordance with the CSP continuity of operations plan.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place that specifies the frequency of backups and duration of backup data retention.		❒	❒	
The CSP has defined processes in place to specify how to perform backup and restore activities.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to support offsite storage of backup data.		❒	❒	
The CSP has the appropriate tools in place to support offsite storage of backup data.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.LOG.01 (Critical)

Each government customer instance has a Network Time Protocol (NTP) Stratum 1 system as a stable Primary Reference Time Server (PRTS) synchronized within 0.25 seconds relative to Coordinated Universal Time (UTC). The primary synchronization method is an out-of-band NIST/USNO national reference time source (Stratum 0) such as the Global Positioning System (GPS) or WWV radio clock.

Clarification

All CSPs must have access to a Stratum 1 server time synchronized for aggregation and collaboration of services in its own data center.

Team Guidance

Appendix C/F:
- The Stratum 0 reference clock must be an out-of-band connection to a source such as the Global Positioning System (GPS) satellite clocks; WWVB, WWV, and WWVH radio reference clocks; or private connection to UTC(NIST) and UTC(USNO) master clocks. An out-of-band Stratum 0 time source is required in the event the CSP external connections, including the Internet, are disrupted.

The Stratum 1 server must be owned by the CSP; it does not have to be within the CSP infrastructure layer.
The Stratum 1 server cannot be accessed across the Internet.
The connection to the Stratum 1 must be through a trusted connection.
It is acceptable for the device to receive its time indirectly from a Stratum 3 or 2 that receives its time from the Stratum 1 server within the organization.
If the CSP is using at least NTP v3 (v4 preferred) and getting its time from Stratum 1 within the infrastructure, this is also acceptable.

Examples of Evidence Sought

The CSP can demonstrate (or show):
- tracing the provision of time to the CSP devices
- actual configurations in CSP devices and appliances showing where the time is obtained
- the console login to Stratum 1 device
- how it maintains and updates this service
- the physical location of the Stratum 1 device
- the actual Stratum 1 device in an operational state

The CSP can provide:
- network diagrams showing the use and location of the Stratum 1 server
- QA test/audit reports of Stratum 1 device in use/connected

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP uses Stratum 1 time services for all CSP devices within the CSP, NOC, and SOC.	❒	❒	

The CSP has the appropriately trained personnel in place to manage the Stratum 1 time services.		❒	❒	
Each CSP has its own Network Time Protocol (NTP) Stratum 1 system as a stable Primary Reference Time Server (PRTS) at the CSP location.		❒	❒	
The Stratum 1 system is synchronized within 0.25 seconds relative to Coordinated Universal Time (UTC).		❒	❒	
The primary synchronization method is an out-of-band NIST/USNO national reference time source (Stratum 0) such as the Global Positioning System (GPS) or WWV radio clock.		❒	❒	
CSP PRTS use cryptographic authentication with external network time servers and between internal primary reference time servers.		❒	❒	
The CSP must maintain a log of time changes and synchronization events, and alert the CSP operator when clock accuracy limits are exceeded or may be exceeded due to loss of synchronization with UTC time sources.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place to require the use of Stratum 1 time services.		❒	❒	
The CSP has defined processes in place to specify how to use and manage Stratum 1 time services.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriate tools in place to support using the Stratum 1 time services.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.LOG.02 (Critical)			
All government customer instance event recording clocks are synchronized to within 3 seconds relative to Coordinated Universal Time (UTC). All CSP log timestamps include the date and time, with at least to-the-second granularity. Log timestamps that do not use Coordinated Universal Time (UTC) include a clearly marked time zone designation. The intent is to facilitate incident analysis between CSPs and CSP networks and devices.			
Clarification			
The intent is to facilitate incident analysis between CSPs and CSP networks and devices. There is clear marking of the time zone information displayed in the timestamp.			
Team Guidance			
It is recommended that the difference be to within 0.5 seconds of UTC. This capability is focused only on the existence of timestamps with clear time zone markings and whether or not they are consistently applied across the organization. The time stamp zone must accurately reflect the time zone of the collection device (regardless of where the logs are being displayed).			
Examples of Evidence Sought			
The CSP can demonstrate: - how time zone designations are marked in the timestamp - an example of standardized timestamps in logs and data during CSP infrastructure tool demonstrations The CSP can provide: - documents, logs, screen captures, and configuration files that clearly show timestamps are in use and standardized - documents, logs, screen captures, and configuration files that clearly show timestamps not adhering to the standard are clearly marked with the appropriate time zone - documented procedure for properly time stamping information - QA test/audit reports of how time stamps are used			
Scoring Criteria			
	Yes	No	Evidence
Technical			
All government customer instance event recording clocks are synchronized to within 3 seconds relative to Coordinated Universal Time (UTC).	❒	❒	
All CSP log timestamps include the date and time, with at least to-the-second granularity.	❒	❒	

Log timestamps should adhere to UTC. Those that do not use Coordinated Universal Time (UTC) must be clearly marked with the time zone designation.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place to specify the consistent, accurate use of time stamps.		❒	❒	
The CSP has a documented process in place that specifies how to properly time stamp information.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.LOG.03 (Critical)			
The CSP provides online access to at least 7 days of session traceability and audit ability by capturing and storing logs / files from installed CSP equipment including, but not limited to: firewalls, routers, servers, and other designated devices. The CSP maintains the logs needed to establish an audit trail of administrator, user, and transaction activity and sufficiently reconstructs security-relevant events occurring on, performed by, and passing through CSP systems and components. Note: This capability is intended for immediate, online access in order to trace session connections and analyze security-relevant events. In addition, CSP.TM.LOG.04 requires retaining logs for an additional period of time either online or offline.			
Clarification			
The CSP must maintain the ability for incident analysis and forensic analysis by capturing and storing 7 days of logs and files from installed CSP Portal equipment, such as firewalls, routers, servers, and other designated devices required to establish an audit trail of administrator, user, and transaction activity. This information should be sufficient to reconstruct security-relevant events occurring on, performed by, or passing through the equipment.			
Team Guidance			
NCPS (Einstein) is not part of this requirement, and cannot be used by CSP to 'meet' it.			
Examples of Evidence Sought			
The CSP can demonstrate: - the tools used to collect session data (rolling PCAP off a router, log aggregation, etc.) - the data storage process and tools used to aggregate the data, such as an SEIM tool - the use of existing tools to pull up session data from 7 days ago The CSP can provide: - a trace of network activity from the previous week - system logs captured from CSP devices from the previous week and explain how they would be used to reconstitute sessions - QA test/audit reports of session traces			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP maintains 7 days of history online and 5 years offline/offsite.	❒	❒	
The CSP can demonstrate that it is able to extract a session trace for an event or incident from stored logs.	❒	❒	
The CSP maintains the logs needed to establish an audit	❒	❒	

trail of administrator, user, and transaction activity and can sufficiently reconstruct security-relevant events occurring on, performed by, and passing through CSP systems and components.				
The CSP captures, stores, and provides online access to logs and files from installed CSP equipment for a minimum of seven days.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place to specify that session data must be captured, stored, and able to be quickly reconstructed.		❒	❒	
The CSP has defined processes in place to specify how to capture, store, and reconstruct session data.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained personnel in place to support capturing, storing, and reconstructing session data.		❒	❒	
The CSP has the appropriate tools in place to support capturing, storing, and reconstructing session data.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.PC.01 (Critical)			
The government customer instances comply with NIST SP 800-53 physical security controls for high impact systems (FIPS 199).			
Clarification			
The CSP equipment stack is considered a “high impact” system under FIPS 199 and NIST SP 800-53. Therefore the facility housing the CSP equipment stack must meet the physical and environmental protection (PE) security controls required to protect high impact systems listed in NIST SP 800-53.			
Team Guidance			
The indicators provided are derived directly from NIST SP800-53. For any indicator that contains multiple requirements, all requirements must be satisfied for the indicator to be considered met.			
Examples of Evidence Sought			
The CSP can demonstrate: - what safeguards are in place to clear personnel for unescorted access to CSP spaces, and ensure such personnel are able to access only spaces commensurate with the sensitivity of the contents of the space based on their clearance - that manual or electronic logs are archived and/or stored and periodically reviewed - sensitivity levels for CSP physical spaces based on the contents of those spaces and who has access - compliance with NIST SP 800-53 Physical Security Controls for FIPS 199 high-impact systems to regulate access to the CSP, NOC, and SOC by CSP employees, contractors, vendors, and visitors - physical tiered access controls (e.g., roving guards, fences, man traps, security checkpoints) for each location - how it meets the NIST SP 800-53 high impact level physical security controls (i.e., direct observation by the team) The CSP can provide: - documentation of the definitions of sensitivity levels - manual and electronic logs showing what is recorded for unescorted personnel - the policy for granting personnel with unescorted access to CSP spaces - provide procedures for obtaining badges, the badging process (i.e., granting, maintaining, and terminating access), how to access CSP spaces, how background checks are performed, and how “piggybacking” is prevented - QA test/audit reports of access to CSP spaces - documented policies describing tiered physical access - documented procedures for managing tiered physical access - QA test/audit reports of physical access controls - appropriate C+A letters showing its certification at the high impact level for the CSP spaces and equipment, if it has undergone C+A testing for NIST SP 800-53 compliance			
Scoring Criteria			
	Yes	No	Evidence

Technical			
The CSP develops, disseminates, and reviews/updates policies and procedures. (PE-1 Physical and Environmental Protection Policies and Procedures)	❒	❒	
The CSP develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); issues authorization credentials; reviews and approves the access list and authorization credentials; removing from the access list personnel no longer requiring access. (PE-2 Physical Access Authorizations)	❒	❒	
The CSP enforces physical access authorizations for all physical access points; verifies individual access authorizations before granting access to the facility; controls entry to the facility containing the information system using physical access devices and/or guards; controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; secures keys, combinations, and other physical access devices; inventories physical access devices; changes combinations and keys according to defined policies and when keys are lost, combinations are compromised, or individuals are transferred or terminated. (PE-3 Physical Access Control)	❒	❒	
The CSP controls physical access to information system distribution and transmission lines within organizational facilities. (PE-4 Access Control for Transmission Medium)	❒	❒	
The CSP controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. (PE-5 Access Control for Output Devices)	❒	❒	
The CSP monitors physical access to the information system to detect and respond to physical security incidents, reviews physical access logs, and coordinates results of reviews and investigations with the organization's incident response capability. (PE-6 Monitoring Physical Access)	❒	❒	
The CSP controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. (PE-7 Visitor Control)	❒	❒	
The CSP maintains visitor access records to the facility	❒	❒	

where the information system resides (except for those areas within the facility officially designated as publicly accessible); and reviews visitor access records. (PE-8 Access Records)			
The CSP protects power equipment and power cabling for the information system from damage and destruction. (PE-9 Power Equipment and Power Cabling)	❒	❒	
The CSP provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. (PE-11 Emergency Power)	❒	❒	
The CSP employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. (PE-12 Emergency Lighting)	❒	❒	
The CSP employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. (PE-13 Fire Protection)	❒	❒	
The CSP maintains temperature and humidity levels within the facility where the information system resides; and monitors temperature and humidity levels. (PE-14 Temperature and Humidity Controls)	❒	❒	
The CSP protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. (PE-15 Water Damage Protection)	❒	❒	
The CSP authorizes, monitors, and controls equipment entering and exiting the facility and maintains records of those items. (PE-16 Delivery and Removal)	❒	❒	
The CSP employs information system security controls at alternate work sites; assesses as feasible, the effectiveness of security controls at alternate work sites; and provides a means for employees to communicate with information security personnel in case of security incidents or problems. (PE-17 Alternate Work Site)	❒	❒	
The CSP positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. (PE-18 Location of Information System Components)	❒	❒	

The CSP provides the capability of shutting off power to the information system or individual system components in emergency situations and protects the emergency power shutoff capability from unauthorized activation. Emergency shutoff capabilities must be placed in a location which is safe and easy to access by authorized personnel. (PE-10 Emergency Shutoff)		❒	❒	
Institutional				
The CSP has defined policies or guidance for unescorted and escorted access to CSP spaces.		❒	❒	
The CSP has defined procedures in place for escorting uncleared personnel through CSP spaces when they have a need to enter a sensitive CSP space.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to manage and audit physical access and physical access controls.		❒	❒	
The CSP has the appropriate tools in place to manage and audit physical access controls.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.PC.02 (Critical)			
The CSP management locations, such as a Network Operations Center (NOC) and a Security Operations Center (SOC), comply with NIST SP 800-53 physical security controls for medium impact systems (FIPS 199).			
Clarification			
The systems within both the NOC and SOC are considered “medium impact” systems under FIPS 199 and NIST SP 800-53. Therefore the areas dedicated to NOC and SOC functions must meet the physical and environmental protection (PE) security controls required to protect medium impact systems listed in NIST SP 800-53.			
Team Guidance			
The indicators provided are derived directly from NIST SP800-53. For any indicator that contains multiple requirements, all requirements must be satisfied for the indicator to be considered met.			
Examples of Evidence Sought			
The CSP can demonstrate: - what safeguards are in place to clear personnel for unescorted access to CSP spaces, and ensure such personnel are able to access only spaces commensurate with the sensitivity of the contents of the space based on their clearance - that manual or electronic logs are archived and/or stored and periodically reviewed - sensitivity levels for CSP physical spaces based on the contents of those spaces and who has access - compliance with NIST SP 800-53 Physical Security Controls for FIPS 199 high-impact systems to regulate access to the CSP, NOC, and SOC by CSP employees, contractors, vendors, and visitors - physical tiered access controls (e.g., roving guards, fences, man traps, security checkpoints) for each location - how it meets the NIST SP 800-53 high impact level physical security controls (i.e., direct observation by the team) The CSP can provide: - documentation of the definitions of sensitivity levels - manual and electronic logs showing what is recorded for unescorted personnel - the policy for granting personnel with unescorted access to CSP spaces - provide procedures for obtaining badges, the badging process (i.e., granting, maintaining, and terminating access), how to access CSP spaces, how background checks are performed, and how “piggybacking” is prevented - QA test/audit reports of access to CSP spaces - documented policies describing tiered physical access - documented procedures for managing tiered physical access - QA test/audit reports of physical access controls - appropriate C+A letters showing its certification at the high impact level for the CSP spaces and equipment, if it has undergone C+A testing for NIST SP 800-53 compliance			
Scoring Criteria			
	Yes	No	Evidence

Technical			
TM.PC.02.01 - The CSP develops, disseminates, and reviews/updates policies and procedures. (PE-1 Physical and Environmental Protection Policies and Procedures)	❒	❒	
TM.PC.02.02 - The CSP develops and keeps current a list of personnel with authorized access to the areas where the information system resides (except for those areas within the facility officially designated as publicly accessible); issues authorization credentials; reviews and approves the access list and authorization credentials; removing from the access list personnel no longer requiring access. (PE-2 Physical Access Authorizations)	❒	❒	
TM.PC.02.03 - The CSP enforces physical access authorizations for all physical access points; verifies individual access authorizations before granting access to the facility; controls entry to the areas containing the information system using physical access devices and/or guards; controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; secures keys, combinations, and other physical access devices; inventories physical access devices; changes combinations and keys according to agency policy and when keys are lost, combinations are compromised, or individuals are transferred or terminated. (PE-3 Physical Access Control)	❒	❒	
TM.PC.02.04 - The CSP controls physical access to information system distribution and transmission lines within organizational facilities. (PE-4 Access Control for Transmission Medium)	❒	❒	
TM.PC.02.05 - The CSP controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. (PE-5 Access Control for Output Devices)	❒	❒	
The CSP monitors physical access to the information system to detect and respond to physical security incidents; reviews physical access logs; and coordinates results of reviews and investigations with the organization's incident response capability. (PE-6 Monitoring Physical Access)	❒	❒	
The CSP controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. (PE-7 Visitor Control)	❒	❒	

The CSP maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and reviews visitor access records. (PE-8 Access Records)	❒	❒	
The CSP protects power equipment and power cabling for the information system from damage and destruction. (PE-9 Power Equipment and Power Cabling)	❒	❒	
The CSP provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. (PE-11 Emergency Power)	❒	❒	
The CSP employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. (PE-12 Emergency Lighting)	❒	❒	
The CSP employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. (PE-13 Fire Protection)	❒	❒	
The CSP maintains temperature and humidity levels within the facility where the information system resides; and monitors temperature and humidity levels. (PE-14 Temperature and Humidity Controls)	❒	❒	
The CSP protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. (PE-15 Water Damage Protection)	❒	❒	
The CSP authorizes, monitors, and controls entering and exiting the facility and maintains records of those items. (PE-16 Delivery and Removal)	❒	❒	
The CSP employs information system security controls at alternate work sites; assesses as feasible, the effectiveness of security controls at alternate work sites; and provides a means for employees to communicate with information security personnel in case of security incidents or problems.(PE-17 Alternate Work Site)	❒	❒	
The CSP positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. (PE-18 Location of Information System Components)	❒	❒	

The CSP provides the capability of shutting off power to the information system or individual system components in emergency situations and protects the emergency power shutoff capability from unauthorized activation. Emergency shutoff capabilities must be placed in a location which is safe and easy to access by authorized personnel. (PE-10 Emergency Shutoff)		❒	❒	
Institutional				
The CSP has defined policies or guidance for unescorted and escorted access to CSP spaces.		❒	❒	
The CSP has defined procedures in place for escorting uncleared personnel through CSP spaces when they have a need to enter a sensitive CSP space.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to manage and audit physical access and physical access controls.		❒	❒	
The CSP has the appropriate tools in place to manage and audit physical access controls.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.PC.03 (Critical)			
The CSP maintains access to an accredited Sensitive Compartment Information Facility (SCIF) that complies with ICD 705, “Sensitive Compartmented Information Facilities.”			
Clarification			
The intent of this capability is to ensure that the CSP has, and maintains access to, a Sensitive Compartment Information facility which houses the equipment specified in TM.COM.01.			
Team Guidance			
The Fed Lead is responsible for verification of the location and agency access to the SCIF. Note: A regular closed area does not constitute a SCIF for handling TS/SCI materials. DCID 6/9 Access to a SCIF requires authorization to use it.			
Examples of Evidence Sought			
The CSP can demonstrate: - at least one person on the SOC staff is cleared at the TS/SCI level, and that this individual has been indoctrinated for unescorted SCIF access and handling procedures for SCI - it has access to the SCIF within 30 minutes, including an escorted visit to the SCIF by a qualified/cleared member of the SOC team - the SCIF has communications equipment capable of handling information up to, and including the TS/SCI level. This can include JWICS terminals, phones accredited for TS/SCI, etc. The CSP can provide: - a C+A letter stating that its SCIF is compliant with DCID 6/9 Physical Security Standards for Sensitive Compartmented Information Facilities			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP maintains access to an accredited Sensitive Compartment Information Facility (SCIF) that complies with ICD 705, "Sensitive Compartmented Information Facilities."	❒	❒	
Institutional			
The CSP has defined policies or guidance in place specifying access to and operations of the SCIF.	❒	❒	
The CSP has defined processes in place to specify how to	❒	❒	

access the SCIF, operate the equipment, and communicate with US-CERT.					
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒		
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TM.PC.04 (Critical)

The government customer instances and CSP management functions, such as NOC/SOC, are located in spaces dedicated for exclusive use or support of the U.S. Government. The space is secured by physical access controls to ensure that CSP systems and components are accessible only by authorized personnel. Examples of dedicated spaces include, but are not limited to: secured racks, cages, rooms, and buildings.

Clarification

The intent of this capability is to establish that the facility or areas housing the CSP systems (CSP, NOC, SOC) are either owned by the federal government, or leased under a GSA approved lease agreement for the sole use of the Federal Government.

Team Guidance

The second portion of this capability that references physical control is already covered under capabilities CSP.TM.PC.01 and CSP.TM.PC.02. Because of this, no indicators have been included to cover this portion of the capability.

Examples of dedicated spaces include, but are not limited to: secured racks, cages, rooms, and buildings. The CSP might not reside in a facility that it owns. The intent of this capability is to ensure the CSP can control the facility and the facility is not co-located with other organizations which may put its operation at risk.
The CSP may rent, own, or lease the facility.

Examples of Evidence Sought

The CSP can demonstrate:
- logical and/or physical separation of CSP systems and infrastructure from non-CSP systems and infrastructure

The CSP can provide:
- documentation that the NOC, SOC, and CSP locations all reside in either a government owned, government-contracted, or GSA-approved facility
-must provide evidence that it's NOC, SOC, and CSP locations all reside in facilities controlled by the CSP
- A copy of its deed or current lease agreement (with any rental costs/fees omitted) is acceptable evidence to corroborate this.

Scoring Criteria

	Yes	No	Evidence
Technical			
The government customer instances and CSP management functions, such as NOC/SOC, are located in spaces dedicated for exclusive use or support of the U.S.	❒	❒	

Government.				
Institutional				
The CSP has defined policies or guidance in place to ensure continued dedication of the facilities to the CSP.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.PC.05 (Critical)
The government customer instance is equipped for uninterrupted operations for at least 24 hours in the event of a power outage, and conforms to specific physical standards including, but not limited to: - Electrical systems meet or exceed the building, operating and maintenance standards as specified by the GSA Public Buildings Service Standards, PBS-100. - CSP systems and components are connected to uninterruptable power in order to maintain mission and business-essential functions including, but not limited to: CSP systems, support systems and powered telecommunications facilities, including at the DEMARC or MPOE. - Uninterruptable power systems, HVAC and lighting are connected to an on-site, automatic, standby/emergency generator capable of operating continuously (without refueling) for at least 24 hours.
Clarification
Each government customer instance must have at least 24 hours of emergency power available, without the need for external intervention (such as refueling). Emergency power must be provided in a way such that there is no interruption of power to government customer instance facilities and systems during the loss of main power. (ex: Uninterruptible Power Supply fed by a diesel generator) It is permissible for a CSP Management Location (NOC, SOC,) to relocate command and control functions to a continuity of operation (COOP) location instead of providing the required emergency power.
Team Guidance
DEMARC: Telecommunications point of demarcation. This references the equipment installed by a network vendor to provide telecommunication services to the CSP. MPOE: Multiple Points of Entry. This references that there may be one or more points of demarcation within the CSP facility.
Examples of Evidence Sought
The CSP can demonstrate: - UPSs' and generators' physical locations, and verify that the UPSs are capable of accommodating the power load until the generators take over - the UPSs and generators are periodically tested for readiness and the results documented - specially marked UPS outlets used to power critical components during power outages The CSP can provide: - long term contracts in place for replenishment fuel for generators - service contracts for maintenance and repair of UPSs and generators are consistent with CONOPS/SLA requirements - documented testing process and schedules for tests - QA test/audit reports of UPS and generator operations - documented uptime requirements from either its parent organization or its customers - DR/COOP plan for the CSP infrastructure, detailing uptime requirements and how they are met - QA test/audit reports stating that it meets the uptime requirements
Scoring Criteria

	Yes	No	Evidence
Technical			
The government customer instance is equipped for uninterrupted operations for at least 24 hours in the event of a power outage, and conforms to specific physical standards including, but not limited to: Electrical systems meet or exceed the building, operating, and maintenance standards as specified by the GSA Public Buildings Service standards, PBS-100.	❒	❒	
The government customer instance is equipped for uninterrupted operations for at least 24 hours in the event of a power outage, and conforms to specific physical standards including, but not limited to: CSP systems and components are connected to uninterruptable power in order to maintain mission and business-essential functions including, but not limited to: CSP systems, support systems and powered telecommunications facilities, including at the DEMARC or MPOE.	❒	❒	
The government customer instance is equipped for uninterrupted operations for at least 24 hours in the event of a power outage, and conforms to specific physical standards including, but not limited to: Uninterruptable power systems, HVAC and lighting are connected to an on-site, automatic, standby/emergency generator capable of operating continuously (without refueling) for at least 24 hours.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place that specify uninterrupted power availability for 24 hours (or longer, as governed by an SLA) in the event of a power failure.	❒	❒	
The CSP has defined processes in place to specify how to test and maintain uninterrupted power availability for 24 hours (or longer, as governed by an SLA) in the event of a power failure.	❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.	❒	❒	
The CSP has the appropriately trained personnel in place to test and maintain uninterrupted power availability.	❒	❒	
The CSP has the appropriate tools in place to monitor actual uptime.	❒	❒	

Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.PC.06 (Critical)					
The CSP has geographic separation between its government customer instances, with at least 10 miles separation recommended.					
Clarification					
Intent is to establish geographic diversity such that approved agency CSP sites will not be impacted by the same event. Assessment criteria should document the minimum separation between government customer instances.					
Team Guidance					
Collect the exact distance between government customer instances as part of data collection.					
Scoring Criteria					
		Yes	No	Evidence	
Technical					
The CSP has geographic separation between its government customer instances, with at least 10 miles separation.		❒	❒		
Institutional					
The CSP has defined policies in place or guidance specifying the requirements for physical separation of government customer instances.		❒	❒		
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TM.TC.01 (Critical)			
The government customer instance follows the National Communications System (NCS) recommendations for Route Diversity, including at least two physically separate points of entry at the government customer instance and physically separate cabling paths to an external telecommunications provider or Internet provider facility.			
Clarification			
It is not required that the CSP subscribe to services from two separate providers to satisfy this requirement. The intent of this capability is to ensure that the CSP has two separate connections to the internet, and that those connections take geographically diverse paths from the CSP location to two separate internet points of presence (POPs). Further, the demarcation points for the two separate connections must reside in geographically distant points within the CSP facility. (e.g. opposite sides of the facility) It is important that one single cut cable or conduit cannot take the CSP facility offline.			
Team Guidance			
Route diversity is defined as "communications routing between two points over more than one geographic or physical path, with no points in common." http://www.ncs.gov/rdp/.			
Examples of Evidence Sought			
The CSP can demonstrate: - at a minimum, two physically separate telecommunication paths will service the CSP facility or facilities from two separate POPs - telco conduit into CSP and cross connects to DEMARC - router configurations that verify two circuits are listed - the points of entry are geographically diverse in relationship to the building or facility where the CSP is located The CSP can provide: - network diagrams for diverse paths and circuit IDs - a route diversity study, if available, to confirm diverse routes exist - QA test/audit reports of segregation/isolation of routes			
Scoring Criteria			
	Yes	No	Evidence
Technical			
Each communications circuit used by the CSP at the government customer instance enters the facility at a separate location.	❒	❒	
Each communications circuit used by the CSP at the	❒	❒	

government customer instance takes a geographically separate route from the CSP facility to the telecommunications provider.				
Institutional				
The CSP has defined policies or guidance in place that call for physically diverse MPOE and separate POPs.		❒	❒	
The CSP has defined processes in place that specify how to monitor the status of the MPOE and POPs.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.TC.02 (Critical)			
CSP systems and components in the government customer instance are configured according to the principal of "least functionality," in that they provide only essential capabilities and specifically prohibit or restrict the use of non-essential functions, ports, protocols, and/or services.			
Clarification			
Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). The functions and services provided by organizational information systems, or individual components of information systems, should be carefully reviewed to determine which functions and services are candidates for elimination. (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing)			
Team Guidance			
The assessment of this capability is to verify that the CSP only allows authorized ports and protocols. Additionally, where possible the CSP operates critical services on separate devices/servers.			
Examples of Evidence Sought			
- Change Management meeting minutes indicating the elimination of services on devices - Configuration Management Plan outlining the services permitted on various devices - Multiple Scan results showing documenting a progressive reduction in the amount of services/ports open on a given device (lists from US-CERT can provide suggested ports or services that might be blocked and how CSP addresses those suggestions) - Firewall configuration			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP reviews the information system on a periodic basis (at least yearly) to identify and eliminate unnecessary functions, ports, protocols, and/or services. This review is done by management and can utilize input from (for example) US-CERT notifications.	❒	❒	
The CSP performs regular scans of the information system to document functions, ports, protocols, and/or services. The scans identify not only which ports/protocols are being used, but can highlight whether any unauthorized ports/protocols are being used.	❒	❒	
Host based firewalls or port filtering tools are applied to CSP equipment that supports such capabilities and are	❒	❒	

configured by default to deny all traffic except for traffic that has been explicitly approved by the CSP.				
Institutional				
The CSP has defined policies or guidance in place to document changes to the information system.		❒	❒	
The CSP has defined processes in place to specify how to monitor and filter unnecessary ports, protocols, and/or services, both inbound and outbound.		❒	❒	
The CSP has a process in place to track and manage the implementation of ports, protocols, and services.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.TC.03 (Critical)			
All CSP systems and components of the government customer instance support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22 and Federal CIO memorandum “Transition to IPv6.” - The CSP supports both IPv4 and IPv6 addresses and can transit both native IPv4 and native IPv6 traffic (i.e. dual-stack) between external connections and agency internal networks. The CSP may also support other IPv6 transit methods such as tunneling or translation. - The CSP ensures that the government customer instance systems implement IPv6 capabilities (native, tunneling or translation), without compromising IPv4 capabilities or security. IPv6 security capabilities should achieve at least functional parity with IPv4 security capabilities.			
Team Guidance			
Because of the limitations on the IPv4 address space, OMB has mandated that agencies begin to build their IPv6 infrastructure and implement plans to migrate to IPv6 (IPv6 supports 2^128 addresses whereas IPv4 supports only 2^32). This capability essentially is validating whether or not the CSP has made progress towards migrating to IPv6 support. It is also important to note here that we are concerned primarily with routers, switches, and firewalls when talking about IPv6, since this is a network layer (layer 3) protocol.			
Examples of Evidence Sought			
Packet capture showing IPv6 running on the backbone in one of the acceptable configurations. Security policies specifically referencing IPv6 configuration. Firewall/IDS rules that include IPv6 addressing (may or may not be applicable depending on configuration)			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP backbone supports and operationally carries IPv6 traffic in either a pure IPv6 mode or a dual-stack configuration.	❒	❒	
All CSP component equipment and appliances support use of the IPv6 protocol.	❒	❒	
The CSP has a documented security policy that demonstrates an IPv6 security policy that is, at a minimum, equivalent in security posture to existing IPv4 security policies and controls, and addresses IPv6-specific security issues.	❒	❒	
The CSP has documentation of its IPv6 network equivalent to its IPv4 documentation, including network diagrams,	❒	❒	

planning / architecture documents, and configuration management.				
Institutional				
The CSP has defined processes in place to specify how to monitor and support IPv6 operations and the CSP IPv6 infrastructure.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.TC.05 (Critical)
The CSP maintains normal delegations and devolution of authority to ensure essential incident response performance to a no-notice event. This includes, but is not limited to, terminating, limiting, or modifying access to external connections, including to the Internet, based on documented criteria, including when advised by US-CERT.
Clarification
The intent is on-scene personnel are authorized and capable of initiating essential response actions based on the severity of the event until escalation personnel arrive (including if the escalation personnel fail to respond). Waiting for, or lack of response by, escalation personnel should not prevent essential response by on-scene personnel. The CSP must have in place the right staff (i.e., SOC and/or NOC personnel), with the appropriate authority to take action in response to threats, vulnerabilities, and attacks, within appropriate timeframes, including emergency situations.
Team Guidance
A "no-notice" event refers originally to the National Continuity and Response Plan which mentioned earthquakes, bombs and the like. For here, it refers to things like launched DDOS attacks and other events for which you get no advance notice. This capability focuses on having people ready to take action. There must be a qualified person on duty within the SOC facility that is authorized take action to coordinate or escalate emergency response. If the response requires a call to the NOC (or someone else) to shut down or modify network access, then the NOC must have around-the-clock coverage by someone who also has the authority to take the action. Escalation procedures must be able to occur with enough speed that required action is not stalled while waiting for approvals. The CSP must be able to respond in near real time to requests from US-CERT to take emergency actions. This could include requests to take off a network segment, apply filters based on specified

criteria, or provide information as needed.
The CSP must ensure that there is not a long lag time between crisis and action and that someone ultimately does not take action because they could not reach anyone in the contact list to approve a response action.

Capability specific definitions:
- Appropriate training/qualifications: authority to shut down or modify network access in emergency situations

Examples of Evidence Sought

The CSP can demonstrate:
- how emergency requests from US-CERT would be handled
- how shifts are covered and what authority the staff has to shut down or modify network access in the event of an emergency
- a sample incident where emergency action had to be taken and explain what was done, and by whom, to validate that emergency response can occur in a timely fashion

The CSP can provide:
- any authorization it has been designated to take emergency action (policy, procedure, or management memo)
- its escalation and emergency response procedures, and explain how emergency requests from US-CERT would be handled
- guidelines and procedures outlining:
--the process to be followed to make requested changes
-- the type of notification that is required to be sent to others (users, management, subscribers, US-CERT, etc.)
-- the type of documentation required for the changes made
- QA test/audit reports of emergency response procedures

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP maintains a policy or process that defines the hierarchy of delegated authority to ensure essential incident response performance to a no-notice event.	❒	❒	
The CSP maintains a policy or process that defines essential incident response performance for at least coordinating and escalating emergency issues, and terminating, limiting or modifying access to external connections, including to the Internet, based on documented criteria.	❒	❒	
The CSP takes appropriate action regarding incident response issues when it receives guidance or advice from US-CERT.	❒	❒	

Scoring	Compliant (all Yes boxes	❒	Non-compliant (if any No box	❒

	above are checked)		above is checked)	

Capability #CSP.TM.TC.06 (Critical)

The CSP management location, such as a Network Operations Center (NOC) and/or Security Operations Center (SOC), is staffed 24x7. On-scene personnel are qualified and authorized to initiate appropriate technical responses, including when external access is disrupted.

Clarification

The CSP management location, such as a Network Operations Center (NOC) and/or Security Operations Center (SOC), should be staffed 24x7 with personnel qualified and authorized to take action in response to threats, vulnerabilities, and attacks, within appropriate timeframes, including emergency situations.

Team Guidance

This capability focuses on whether the CSP has a 24x7 management location capable of responding to technical events.
A management location that is capable of recognizing and reacting to events requires personnel with appropriate training, skills, and certifications.
If the response requires a call to the NOC (or someone else) to shut down or modify network access, then the NOC must have around-the-clock coverage by someone who also has the authority to take the action. Escalation procedures must be able to occur with enough speed that required action is not stalled while waiting for approvals.
The CSP must be able to respond in near real time to requests from US-CERT to take emergency actions. This could include requests to take off a network segment, apply filters based on specified criteria, or provide information as needed.
The CSP must ensure that there is not a long lag time between crisis and action and that someone ultimately does not take action because they could not reach anyone in the contact list to approve a response action.
The management location staff must be able to take appropriate actions once given direction.

Capability specific definitions:
Appropriate training/credentials: Information security technical training, skills, abilities, and access to necessary resources to recognize and respond to network security incidents and emergencies and, optionally, have certifications if required by the CSP.
Authority to shut down or modify network access in emergency situations
Appropriate tools: 24x7: around the clock (24 hours a day, 7 days a week, 365 [or 366] days a year).
Remote access or Physical Access to CSP stack equipment.

Examples of Evidence Sought

The CSP can demonstrate:
-How the management location is structured, staffed, organized, and authorized for operation
-The basic process for detecting and responding to events, threats, and network attacks
-Detecting
-Triage
-Analysis
-Incident Response
-A sample incident where emergency action had to be taken and explain what was done, and by whom, to validate that emergency response can occur in a timely fashion
-The management location is operational 24x7 with staff authorized to and capable of responding to events

-How emergency requests from US-CERT would be handled

The CSP can provide:
-Incident Response Policy and Procedures
-Explanation as to how emergency requests from US-CERT would be handled
-Guidelines and procedures outlining
-The process to be followed to make requested changes
-The type of notification that is required to be sent to others (users, management, subscribers, US-CERT, etc.)
-The type of documentation required for the changes made
-Shift schedules (showing 24x7 coverage) and/or shift reports
-Job descriptions of staff showing skills and abilities required–must be approved positions
-Training plans for staff, and sample training materials
-QA test/audit reports management location staffing

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP has the appropriately trained, credentialed personnel in place to support a minimal of two-person operational staffing requirements.	❒	❒	
The SOC and/or NOC are physically staffed 24x7 with qualified personnel who are authorized to take action to coordinate and escalate emergency issues.	❒	❒	
The SOC and/or NOC have a defined schedule and process in place for maintaining 24x7 operational staffing requirements.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place that specifies a minimal of two-person operational staffing requirements.	❒	❒	
The CSP has defined processes in place to specify how to meet the requirement for a minimum of two-person operational staffing.	❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.	❒	❒	
The CSP has the appropriate tools in place to support management of staffing schedules.	❒	❒	
The CSP has the appropriately trained, credentialed	❒	❒	

personnel in place to recognize and respond to network security incidents and emergencies.				
The CSP has the appropriate tools in place to support recognition and response to network security incidents and emergencies.		❒	❒	
The CSP has defined policies or guidance in place to specify 24x7 staffing.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.TC.07 (Critical)
CSP Operations personnel have 24x7 physical or remote access to CSP management systems that control the government customer instance devices. Using this access, CSP operations personnel can terminate, troubleshoot, or repair external connections, including to the Internet, as directed.
Clarification
The intent of this capability is to ensure that CSP management staff and operations personnel can access CSP management systems from local or remote locations, regardless of when a no-notice event occurs. Further, the capability requires that the local or remote access mechanisms provide the capability to assess and repair damage, or implement defensive measures as necessary.
Team Guidance
The CSP must provide local and remote management access to its operational personnel at all times, in the event that the CSP suffers an internal failure or comes under external threat. Please note that by TM.AU.01, any remote access capability to CSP management devices must utilize two-factor authentication. The CSP must be able to respond in near real time to requests from US-CERT to take emergency actions. This could include requests to take off a network segment, apply filters based on specified criteria, or provide information as needed. Capability specific definitions: - Appropriate training/qualifications: authority to shut down or modify network access in emergency situations
Examples of Evidence Sought
The CSP can demonstrate: - how emergency requests from US-CERT would be handled - how shifts are covered and what authority the staff has to shut down or modify network access in the event of an emergency - a sample incident where emergency action had to be taken and explain what was done, and by whom, to validate that emergency response can occur in a timely fashion The CSP can provide: - any authorization it has been designated to take emergency action (policy, procedure, or management memo) - its escalation and emergency response procedures, and explain how emergency requests from US-CERT would be handled - guidelines and procedures outlining -- the process to be followed to make requested changes -- the type of notification that is required to be sent to others (users, management, subscribers, US-CERT, etc.) -- the type of documentation required for the changes made - QA test/audit reports of emergency response procedures
Scoring Criteria

		Yes	No	Evidence
Technical				
The CSP Operations personnel have 24x7 physical or remote access to CSP management systems that control the Government customer instance devices.		❒	❒	
CSP operations personnel may use this access to terminate, troubleshoot, or repair external connections, including to the Internet, as directed.		❒	❒	
Institutional				
The CSP has defined policies and guidance in place that delegate the authority to take emergency action to qualified SOC staff and specify what constitutes an emergency.		❒	❒	
The CSP has defined processes in place to specify how to modify network access and shut down the network during an emergency with enough speed that required action is not stalled while waiting for approvals.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, qualified personnel in place to take emergency action.		❒	❒	
The CSP has the appropriate tools in place to support emergency actions.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MG.01 (Critical)			
The CSP develops, documents, and maintains a current inventory of all CSP information systems and components, including relevant ownership information.			
Clarification			
In order to ensure the protection of all CSP assets, an up-to-date and complete inventory is required for all CSP components. Additionally, ownership information is needed in order to ensure the proper owner is notified of issues regarding their equipment, including any security vulnerabilities discovered, so that proper action can be taken in a timely matter.			
Team Guidance			
For example, based on NIST guidance, level of granularity includes: who owns it, IP address, asset tag, and operating system with version information.			
Examples of Evidence Sought			
Inventory listing of all CSP equipment indicating the Point of Contact (POC) for each piece of equipment Network diagrams listing all equipment with POC information Current configuration management plan documenting all hardware and POC information			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP can demonstrate that it documents and maintains an inventory of its CSP related information systems. Updates to the inventory are an integral part of the CSP's change management process.	❒	❒	
The CSP can demonstrate that the inventory accurately reflects CSP related information systems.	❒	❒	
The inventory contains the entirety of the CSP's CSP related information systems.	❒	❒	
The inventory contains asset ownership information and a means for identifying by name, position, or role, the individuals owning those components.	❒	❒	
Institutional			
The inventory is available for review and audit by designated organizational officials.	❒	❒	

The CSP has defined policies or guidance in place that specifies development and maintenance of the inventory of its information systems.		❒	❒	
The CSP has defined processes in place ensure the hardware inventory is properly updated when new systems are added or when systems are removed.		❒	❒	
The CSP's Configuration Management Plan/policy includes procedures for documenting the addition or subtraction of equipment from the information system.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MG.02 (Critical)

The CSP follows a formal configuration management and change management process to maintain a proper baseline.

Team Guidance

see TM.TC.02 for related items
This capability deals with two separate but related issues: configuration management and change management. Both must be assessed for how they are handled within the CSP infrastructure.
This will facilitate a more efficient recovery of systems and give some historical context for CSP equipment in the future.
The CSP can demonstrate that this capability could be achieved at an enterprise level, and not because individual device managers enforce it for their own devices.
For CSPs, the CSP must be able to negotiate and handle any customer-specific requirements per SLAs over and above their own organization's baselines.

Examples of Evidence Sought

For configuration management:
The CSP can demonstrate:
- configuration management tools used for each CSP infrastructure component
- the process for restoring a prior configuration setting
- the process for restoring a standard CSP device back to working order, based on the default configuration with all additional modifications made in accordance with its configuration management processes

The CSP can provide:
- an example of multiple configuration versions and baselines from a configuration database for a CSP component
- the configuration management process and responsible personnel
- relevant policies for a formal configuration management process
- documented procedures for performing configuration management activities
- technical details of the implementation, blackout procedures, user notification, versioning systems (e.g., SVN or CVS) being used, or any other procedures relating to configuration management
- QA test/audit reports of configuration management

For change management:
The CSP can demonstrate:
- change management tools
- change request mechanisms
- tracking systems
- databases used for CSP infrastructure component change requests

The CSP can provide:
- the change management process and associated review boards
- relevant policies for a formal change management process
- documented procedures for performing change management activities
- an example of a submitted and completed change request
- evidence of technical review or change control board meetings relating to CSP infrastructure component changes (e.g., Change Control Board [CCB], Configuration Management Board [CMB], or Technical Review Board [TRB])
- technical details of the implementation, blackout procedures, user notification, versioning systems (e.g.,

SVN or CVS) being used, or any other procedures relating to change management - QA test/audit reports of change management					
Scoring Criteria					
		Yes	No	Evidence	
Technical					
The CSP has a formal configuration management process that supports: review, approval, and implementation of changes to the CSP information system configurations.		❒	❒		
The CSP has a formal configuration management process that supports identification and base lining of configuration components.		❒	❒		
The CSP has a formal configuration management process that supports version control of configurations.		❒	❒		
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TO.MG.03 (Critical)
The CSP communicates all changes approved through the formal configuration management and change management processes to customers, as defined in SLAs or other authoritative documents.
Clarification
The intent of this capability is to ensure that all changes to the CSP infrastructure that affect customers and end-users are communicated to those customers/end-users as required by policy or service level agreement.
Team Guidance
This capability is to verify that an open line of communication to customers or subscribing agencies exists where changes being enacted on the network (e.g., shared files being migrated, web proxy being switched from one vendor to another, level 2/3 equipment being moved in the overall network topology, etc.) are relayed to appropriate personnel. The communications should be tailored to the CSP audience in order to make sure only as much relevant information as needed is communicated.
Examples of Evidence Sought
The CSP can explain how information is communicated regarding changes resulting from formal configuration or change management activities. The CSP can demonstrate: - how configuration and change management actions are communicated to customers - communication tools or mechanisms The CSP can provide: - sample communications relating to configuration and change management activities - copies of policies, procedures, or SLAs that define how changes are to be communicated - QA test/audit reports of communications about changes
Scoring Criteria

		Yes	No	Evidence
Technical				
The CSP communicates all changes to relevant personnel based on requirements set forth in SLAs.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MG.05 (Critical)
The CSP has telecommunications service priority (TSP) configured for external connections, including to the Internet, to provide for priority restoration of telecommunication services.
Clarification
The intent is the CSP has pre-arranged priority restoration for its major Internet connections and other mission critical external connections. The CSP must subscribe to TSP restoration of services (for voice and data).
Team Guidance
Focus on CSP systems and not other external connections. If voice and data are over IP, then they need restoration services that will provide that coverage TSP is typically available from whomever the CSP is purchasing its fiber connections. This may go by other names, depending on the telecom provider. Note: Per FNS guidance [2009-11-16], TSP is easy to request. Fill out a form at tsp.ncs.gov.
Examples of Evidence Sought
The CSP can demonstrate: - TSP restoration services it subscribes to - critical CSP circuit IDs and the that TSP codes have been designated on them The CSP can provide: - its primary points of contact designated for TSP restoration services - documented policy on the use of TSP - QA test/audit reports of TSP restoration of services
Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP subscribes to TSP for restoration of voice/data services.	❒	❒	

Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MG.06 (Critical)			
The CSP employs a formal technical review process to schedule, conduct, document, and communicate maintenance and repairs. The CSP maintains maintenance records for CSP systems and components. The intent of this capability is to minimize downtime and operational impact of scheduled maintenance and outages.			
Team Guidance			
There should be a clearly defined, formal process for approving and communicating outages and maintenance activities (both scheduled, non-routine, and emergencies). The timing for communicating these should be defined in appropriate policies, SLAs, or other agreements.			
Examples of Evidence Sought			
The CSP can demonstrate: - communication mechanisms used to announce outages or maintenance windows The CSP can provide: - any policies, procedures, SLAs, or other documentation relating to technical review and formal outage processes - defined schedules for maintenance window timeframes, non-routine maintenance, and emergencies - charters, meeting notes, or documentation about any technical review boards - an example of how regularly scheduled (routine) and non-routine or emergency outages are communicated to customers of the CSP and how any feedback from these outages is handled - sample notifications - QA test/audit reports of outages and maintenance			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP employs a formal technical review process to schedule, conduct, document, and communicate maintenance and repairs.	❒	❒	
The CSP maintains maintenance records for CSP systems and components.	❒	❒	
The CSP has a defined process for handling emergency outages.	❒	❒	
Institutional			
The CSP has defined policies or guidance (or SLAs) in place to specify the need to communicate both scheduled and non-routine outages and maintenance windows.	❒	❒	

The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained personnel in place to communicate outages and maintenance windows to customers.		❒	❒	
The CSP has the appropriate tools in place to support communication of outages and maintenance windows to customers.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MON.01 (Critical)
The CSP maintains situational awareness of the CSP and its supported networks as needed to support customer security requirements. Situational awareness can be achieved by correlating data from multiple sources, multiple vendors, and multiple types of data by using, for example, Security Incident + Event Management (SIEM) tools.
Clarification
The CSP collects, correlates, and analyzes information from a number of different sources, including logs and network sensors, to provide various situational awareness reports. (e.g., dashboard information, graphs).
Team Guidance
Most network devices can be configured to produce a stream of diagnostic data to a number of output locations, including live feeds and locally stored logs. These sources of information can be aggregated by a SIEM tool to allow for event correlation and analysis across the enterprise environment. Analysis can be performed using a number of different commercially available tools and techniques. The result of this analysis is usually a structured set of reports used to indicate the overall health or threat level of the network. For best results, SIEM tools should be able to process data from devices manufactured by a wide variety of vendors. Some sources of diagnostic data are: routers, firewalls, proxy devices, e-mail servers, network based cameras, motion sensors, and intrusion detection systems. These sources may provide the information in different forms, such as log files, e-mail, and SNMP events.
Examples of Evidence Sought
The CSP can demonstrate: - how it correlates and analyzes data from the key CSP infrastructure components (firewalls, syslogs, etc.) - the sources of data - any correlation or SIM tools showing that it accepts multiple sources of data from multiple vendors - how analysis of activity across multiple logs is conducted The CSP can provide: - dashboards and alerts produced by correlation tools - software user documentation or implementation guidance - evidence that staff are trained and can use the correlation tools (training plans, certifications on vendor products, etc.) - documented policies on data correlation and reporting - documented procedures on how to correlate and report on analysis of data - QA test/audit reports of data correlation activities or results CSPs can demonstrate how they collect and implement individual customer agencies' correlation and reporting requirements.

Auto Verification					
No. This capability will not be validated using technical means because it is process driven and cannot easily be tested. This capability is not easily verified in an externally automated fashion.					
Scoring Criteria					
		Yes	No	Evidence	
Technical					
The CSP maintains situational awareness by correlating multiple types of data from multiple sources (e.g., various logs) as needed to support customer security requirements.		❒	❒		
Institutional					
The CSP has defined policies or guidance in place that specifies how correlation of data is conducted.		❒	❒		
The CSP has defined processes in place to specify how to correlate data points from multiple sources and vendors.		❒	❒		
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒		
The CSP has appropriately trained, credentialed personnel in place to support analysis and correlation.		❒	❒		
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TO.MON.02 (Critical)			
At a minimum, the CSP annually conducts and documents a security review of the Government customer instance and undertakes the necessary actions to mitigate risk to an acceptable level (FISMA, FIPS 199 and FIPS 200). Vulnerability scanning of the CSP architecture is a component of the security review.			
Clarification			
The CSP must conduct annual security reviews and document the actions taken during the review. The results should be captured and a plan of action and milestones created to mitigate risk to an acceptable level.			
Team Guidance			
Acceptable levels of risk are defined by the agency and the Designated Approving Authority (DAA). A security review is an assessment of the security posture of organizational systems, networks, and security policies and procedures.			
Examples of Evidence Sought			
The CSP can provide: - A security assessment report that details the findings from the annual security review. - A plan of action and milestones (POA+M) for mitigating the vulnerabilities in the security review. - A signed document from the Designated Approving Authority (DAA) stating that they accept the risk of operation. - A vulnerability scan report that shows the latest scan of all systems in the CSP.			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP conducts an annual security review of the CSP Access Point and related management systems.	❒	❒	
The CSP identifies deficiencies from the security review and undertakes the necessary actions to mitigate the risk.	❒	❒	
The annual security review includes a vulnerability scan of all CSP Access Point and related management systems.	❒	❒	
The CSP Access Point Systems are certified and accredited as high impact systems.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place that	❒	❒	

specifies an annual security review.				
The CSP has defined processes in place to specify how to conduct an annual security review.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MON.03 (Critical)			
The CSP provides access for government authorized auditing of the government customer instance, including all CSP systems and components. Authorized assessment teams are provided access to previous audit results of CSP systems and components, including but not limited to, C+A and DCID documentation.			
Clarification			
Authorized government auditors must be able to access the CSP in order to conduct inspections, validations, audits, etc.			
Examples of Evidence Sought			
The CSP can demonstrate: - what process is followed or defined to provide government auditors access to the CSP locations - how specific agency-mandated auditor access requests are handled The CSP can provide: - examples of visitor access requests and how they are handled - audit reports indicating auditors were granted access Allowing CSP Assessment teams on site and granting access to personnel required for the assessment can be used as a direct observation of compliance with this capability.			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP provides access for government authorized auditing of the Government customer instance, including all CSP systems and components.	❒	❒	
The CSP provides access for authorized assessment teams to previous audit results of CSP systems and components, including but not limited to C+A and DCID documentation.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place to permit access to CSP facilities by government-authorized auditors.	❒	❒	
The CSP has defined processes in place that specifies how to handle government-authorized auditor access to CSP facilities.	❒	❒	

Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.REP.04 (Critical)			
The CSP reports incidents to US-CERT in accordance with federal laws, regulations, and guidance.			
Clarification			
CSPs must follow FISMA/NIST 800-61 guidelines for reporting. (See NIST 800-61 rev1 Appendix J Table 1 for specific reporting requirements)			
Team Guidance			
The CSP should have an Incident Response Policy which defines roles and responsibilities for reporting, and to whom reporting is required. (Per FNS, it is not the CSP's responsibility to "manage" internal agency issues) For CSPs, this is not about what is happening outside the CSP boundary (they might gather the information and pass off to someone in agency to report). CSPs must demonstrate that they have a policy and process for reporting incidents. The CSP may only report to the CISO, who then reports to US-CERT (this is acceptable).			
Examples of Evidence Sought			
The CSP can demonstrate: - A walkthrough of reporting an incident The CSP can provide: - Incident Response Policy that details reporting threats/incidents and events - Incident Response Procedures that detail how to report threats/incidents and events, and associated timeframes - Sample incident reports showing requirements are met			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP reports to US-CERT as required by applicable standards, laws, and regulations.	❒	❒	
Institutional			
The CSP has the appropriately trained, credentialed personnel in place to support reporting of threats, incidents, and events.	❒	❒	
The CSP has the appropriate tools in place to support reporting of threats, incidents, and events.	❒	❒	

The CSP has defined policies or guidance in place that specifies reporting of threats, incidents, and events.		❒	❒	
The CSP has defined processes in place to specify how to report threats, incidents, and events.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.RES.01 (Critical)

The CSP has a documented and operational incident response plan in place that defines actions to be taken during a declared incident. In the event of a declared incident or notification from US-CERT, CSP operations personnel immediately activate incident response plan(s). CSP operations personnel report operational status to US-CERT within two hours and continue to report based on US-CERT direction.

Clarification

This includes delays for personnel with necessary security clearances to respond and access classified communication channels.
The CSP SOC must be staffed by at least two people with the appropriate skills, credentials, and technical capabilities to be able to manage any threat and/or attack on the networks; there should be established parameters for taking action.
The SOC personnel should be able to direct the response, although they might not be the staff performing the response (i.e., response could be performed by an incident response team or the NOC at the direction of the SOC).

Team Guidance

This capability is related to Capability 26 (old 40). The previous capability focuses on whether the CSP has a 24x7 SOC capable of responding. This capability focuses on two-person integrity.
"At all times" requires that two (2) qualified and authorized staff members are required to be on duty in the SOC around the clock (24 hours a day, 7 days a week, 365 [or 366] days a year). Remote access or on-call/pager duty coverage does not meet the around-the-clock requirement.
Two (2) staff must be on duty at each SOC location (two-person integrity).

Appropriate credentials include, but are not limited to, having the required:
- authority
- passwords (to log on to systems, to make changes if needed)
- ability to get into the SCIF (for at least one staff member); this requires security clearances
- training

The SOC staff must be able to take appropriate actions once they are given direction.

If the SOC and NOC share space, the two-person integrity could be satisfied with personnel from the SOC and the NOC – BUT BOTH MUST HAVE THE REQUIRED QUALIFICATIONS , ACCESS, AND AUTHORITY TO PERFORM THE TASKS REQUIRED OF THE SOC (i.e., the NOC staff must be able to do the same tasks as the SOC staff).

Examples of Evidence Sought

The CSP can demonstrate:
- through observation of staff on duty, that two qualified people are physically on duty at all times, within the SOC facility (i.e., not remote)

The CSP can provide:
- shift schedules showing at least two people are physically on duty at all times
- shift reports
- a multi-year workforce plan showing planned resources for at least two people for all shifts
- job descriptions of staff showing skills and abilities required and credentials (e.g., security clearances

required for access into the SCIF)—job descriptions must be for approved positions - training plans for staff and sample training materials - a list of security clearance requirements for SOC functions, and the number of SOC staff per shift who have those clearances per shift - QA test/audit reports of two-person staffing				
Scoring Criteria				
		Yes	No	Evidence
Technical				
The CSP has a documented and operational incident response plan in place that defines actions to be taken during a declared incident.		❒	❒	
The CSP operations personnel can activate incident response plans immediately in response to a declared incident or notification from US-CERT.		❒	❒	
CSP operations personnel report operational status to US-CERT within two hours of the activation of the incident response plan and continue to report based on US-CERT direction.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place that specifies a minimal of two-person operational staffing requirements.		❒	❒	
The CSP has defined processes in place to specify how to meet the requirement for a minimum of two-person operational staffing.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriate tools in place to support management of staffing schedules.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.RES.03 (Critical)

The CSP manages filters, excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks on the organization's internal networks and CSP services. The CSP has agreements with external network operators to reduce the susceptibility and respond to information flooding types of denial of service attacks.

The CSP mitigates the impact on non-targeted CSP clients from a DOS attack on a particular CSP client. This may include diverting information flooding types of denial of service attacks targeting a particular CSP client in order to maintain service to other CSP clients.

Clarification

DoS attacks focused on a particular CSP client have the potential to overwhelm the CSP as a whole, disrupting internet communication for all clients. There are multiple ways to mitigate DoS attacks, including agreements with upstream ISP providers to divert or filter disruptive traffic.

Team Guidance

Both peering and upstream ISPs must be considered.

The bulk of this capability is focused on mitigating the impact of a Denial of Service attack using a combination of service restriction, filtering, and properly configured devices.

The CSP's service provider may also provide on-demand filtering/scrubbing services for DoS attacks which do not require an in-place agreement. It is sufficient for a CSP to know how to activate that service and be authorized by management to do so.

Examples of Evidence Sought

The CSP can demonstrate:
- Restricting service to CSP clients targeted by Denial of Service attacks.
- Filtering of DoS packets using a boundary protection device
- Use of traffic scrubbing to minimize attack effectiveness.

The CSP can provide:
- Agreements with upstream ISPs
- Agreements with peering ISPs

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP has the ability, either alone or in conjunction with peering or upstream ISPs, to mitigate information flooding Denial of Service (DoS) attacks by allocating additional bandwidth, filtering network traffic, redirecting traffic, or other network traffic management techniques.	❒	❒	

Institutional				
The CSP has defined policies or guidance in place that specifies response to denial of service attacks.		❒	❒	
The CSP has defined processes in place to specify how to how to respond to denial of service attacks.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.CF.01 (Critical)

The government customer instance uses a combination of application firewalls (stateful application protocol analysis), application-proxy gateways, and other available technical means to implement inbound and outbound application layer filtering. The CSP will develop and implement a risk-based policy on filtering or proxying new protocols.

Clarification

Anything that can be proxied should be in order to facilitate inspection (HTTP/HTTPS, FTP, SSH, etc.).
Non-proxied traffic must also be able to be scanned and blocked.
Non-proxied traffic must go through a formal and approved exemption process.

Team Guidance

There are a number of methods available to filter inbound and outbound application layer network traffic. Application layer network traffic is defined to mean any traffic transported at layer 4 or above in the OSI network model.

The intent of this capability is to ensure that any network traffic that can be proxied, inspected, and filtered is. Any traffic that cannot be proxied must still be filtered. In the event that an exemption is requested or a new protocol is required, there must be a process in place to analyze the risk inherent in performing the change, and a formal, auditable sign-off process by a Designated Approving Authority.

For indicator TS.CF.01.03, it is possible that the CSP has a policy, but has had no reason to implement it. In this instance, mark this indicator as “Not Applicable”. If a policy does not exist, this indicator must be scored “no”.

Note: Public facing servers belonging to the CSP are not intended to be covered in this capability.

Examples of Evidence Sought

The CSP can demonstrate:
- how it would identify the volume of traffic not being proxied (not limited to web traffic)
- tools, procedures, and services available for performing this activity

The CSP can provide:
- documentation that justifies non-proxied traffic
- documentation that explains the inspection and process to implement a block on non-proxied traffic
- a documented process for handling and approving changes to the types of traffic that are proxied
- QA test/audit reports of non-proxied traffic filters

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP has developed and implemented a risk-based	❒	❒	

policy on filtering or proxying new protocols.				
The CSP has a documented exception-handling process.		❒	❒	
Inbound application layer filtering is implemented by the government customer instance through the use of application firewalls (stateful application protocol analysis), application-proxy gateways, and other available technical means.		❒	❒	
Outbound application layer filtering is implemented by the government customer instance through the use of application firewalls (stateful application protocol analysis), application-proxy gateways, and other available technical means.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.CF.02 (Critical)

The government customer instance filters outbound web sessions from CSP clients based on, but not limited to: web content, active content, destination URL pattern, and IP address. Web filters have the capability of blocking: malware, fake software updates, fake anti-virus offers, phishing offers and botnets/keyloggers calling home.

Clarification

All web requests (using http or https) must be filtered to prevent both malware within the CSP from reporting out or exfiltrating information, and malicious content from being retrieved from web services external to the CSP. This can be achieved by filtering outbound requests before they leave the CSP network, or by filtering the information sent to a CSP client from an external web server in response to a request.

Although it is not strictly a web protocol, the File Transfer Protocol (FTP) is included in this capability, and must be filtered.

Team Guidance

Note: Decryption of HTTPS traffic is not required in this capability.
Note: Both the inbound and outbound traffic associated with an outbound web session must be filtered.

This capability concerns all web sessions, not just proxied web sessions.
Note: There is no Federal policy in place that requires that web sessions be proxied.

For purposes of the indicators for this capability, “malicious content” is defined as any content that is intended to subvert the client system, its users, or the network itself. This includes, but is not limited to malware, fake software updates, fake anti-virus offers, phishing offers, and botnets/keyloggers calling home.

Examples of Evidence Sought

The CSP can demonstrate:
- the tools it uses to filter web traffic
- how exceptions are handled or approved
- how a "bad" URL would be filtered (HTTP/HTTPS)
- how a “bad” IP would be filtered (HTTP/HTTPS)
- how FTP traffic (proxied or not) is scanned and filtered
- bi-directional FTP traffic (proxies or not) being diverted to anti-virus scanners for inspection
- how infected FTP files are blocked, quarantined, logged, and the SOC is notified
- how it filters all web sessions (proxied or non-proxied), including showing how the tools are used
- what criteria is used to filter web sessions
- how "bad" traffic could be filtered
- handling and approving exceptions
- handling requests for adding a specific filter
- handling requests for implementing multiple filters for the same session
- how it would handle such a request from US-CERT

The CSP can provide:

- documented procedures for filtering proxies web sessions, handling exceptions, updates, and maintenance
- sample requests
- documentation of the tools used to perform this activity
- QA test/audit reports of web session filters
- SLAs and/or policies with requirements to filter FTP messages for malware
- Documented procedures for keeping content filter products up-to-date
- QA test/audit reports of FTP traffic filters
- documented procedures for updating or adding filters
- documentation of how exceptions are handled or approved
- QA test/audit reports of web session filtering

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP filters outbound web sessions from CSP clients based on destination URL pattern.	❒	❒	
The CSP filters outbound web sessions from CSP clients based on destination IP address.	❒	❒	
The CSP filters malicious content from outbound web sessions. (see team guidance for definition of malicious content)	❒	❒	
Institutional			
The CSP has defined policies or guidance in place that specify that inbound and outbound HTTP and HTTPS traffic must be filtered.	❒	❒	
The CSP has defined processes in place that specifies how to filter inbound and outbound HTTP and HTTPS traffic.	❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to filter inbound and outbound HTTP and HTTPS traffic.	❒	❒	
The CSP has defined policies or guidance in place that specifies filtering of proxied web sessions must be performed.	❒	❒	

Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.CF.04 (Critical)

The government customer instance performs malware scanning, filters content, and blocks spam-sending servers as specified by NIST 800-45, "Guidelines for Electronic Mail Security," for inbound and outbound mail. These government customer instance protections are in addition to malware scanning and content filtering performed by the agency's mail servers and end-user's host systems.
The CSP takes agency specified actions for potentially malicious or undesirable mail, including at least the following actions: block messages, tag undesirable content, sanitize malicious content, and deliver normally. CSPs tailor their malware and content filtering services for individual agency mail domains.

Clarification

The intent of this capability is to ensure that the CSP is able to filter e-mail based on the CSP's determination that a particular piece of e-mail:

1) is considered to be SPAM
2) contains malware
3) contains objectionable content
4) contains undesirable / inappropriate content

Attributes and content found in the header and body of an e-mail may be used to assist in the determination. In addition, the CSP must be able to block SPAM sending servers from connecting to their mail servers, potentially by using a blacklist.

For the purposes of this capability, SPAM e-mail is defined as an e-mail based advertisement or an unsolicited commercial e-mail. (NIST 800-45)

The CSP must also have:
- a process for incorporating changes in the signatures for identifying and blocking malware.
- a defined schedule for frequency of updates and/or refreshes

Team Guidance

All filtering should be accomplished according to CSP (or agency) security policy. Some attributes of an e-mail message that may be considered when making a determination are:
- mail source or destination

- malicious content
- file attachment types
- message size
- unsigned content
- IP reputation checks
- undesirable active content

Additionally, the CSP may also use a whitelist/blacklist to determine what servers they will accept mail from or send mail to.

CSP must be able to offer these services to all of their customers, and implement customer specific actions and policies as necessary.

These government customer instance protections are in addition to malware scanning and content filtering performed by the agency's mail servers and end-user's host systems.
CSPs should be filtering for all criteria listed in the capability statement.

Capability specific definitions:
Filtering must be done for both inbound and outbound traffic.

The assessment is used to verify that the full capability is implemented, rather than focus on what is actively being filtered.
Note: There is no national filtering policy.

Examples of Evidence Sought

The CSP can demonstrate:
- monitoring and filtering e-mail for these requirements
- the administrative interface for the tools used to execute these functions
- configuration settings that show filtering for these criteria in the production environment
- the corresponding processes, personnel, and tools to perform monitoring and filtering, inbound and outbound
- how it scans SMTP messages for malware and blocks infected messages

The CSP can provide:
- an existing ticket or request to implement or remove a specific filter
- log file evidence showing filtering on each of these criteria, inbound and outbound
- a documented process for incorporating changes in the filtering signatures
- a defined schedule for frequency of updates/refreshes
- QA test/audit reports of email filters

- QA test/audit reports of malware scanning and blocking

Scoring Criteria

	Yes	No	Evidence
Technical			
The filtering of e-mail messages and mail server network connections is being done at the CSP Access Point.	❒	❒	
The CSP has and maintains an e-mail security policy, which defines the circumstances under which an e-mail may be subject to actions other than normal delivery.	❒	❒	
The CSP is capable of performing the following actions in response to the attributes of an e-mail being filtered: block, quarantine, tag content, sanitize content, deliver normally.	❒	❒	
CSPs are able to implement customer specific policies and actions as requested.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place that specifies monitoring and filtering of SMTP messages, both	❒	❒	

inbound and outbound.				
The CSP has defined processes in place to specify how to monitor and filter SMTP messages, both inbound and outbound.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to support monitoring and filtering of SMTP messages, both inbound and outbound.		❒	❒	
The CSP has the appropriate tools in place to support monitoring and filtering of SMTP messages, both inbound and outbound		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.CF.05 (Critical)			
The government customer instance uses an agency-specified custom-processing list with at least the combinations of senders, recipients, network IP addresses or host names. The agency specified custom-processing list has custom CSP malware and content filtering actions. Mail allowed by an agency-specified custom-processing list is still scanned by the CSP for malware or undesirable content and tagged if found. CSPs tailor their malware and content filtering services for individual agency mail domains.			
Clarification			
The intent of this capability is not to show that the CSP is capable of filtering e-mail, but instead to show that they are capable of customizing their e-mail filtering rule sets with agency specific rules. At a minimum, the rule set must support filtering based on combinations of sender, recipient, IP addresses, and host names. In addition, the CSP must be able to implement custom actions in response to agency specified filtering rules. CSPs must be able to implement custom e-mail filtering rules and actions for each of their customer agencies. Customer agency specific rules and actions must not depend on, or be affected by, rules and actions required by other customer agencies.			
Team Guidance			
For this capability, a CSP may not push the responsibility for e-mail filtering down to the customer level. A CSP must possess the capability to filter e-mail using custom rules and actions at the government customer instance. A CSP must have a customer accessible process in place for customers to request changes to the filtering rules and actions.			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The government customer instance uses an agency specified custom-processing list that filters mail based on combinations of sender, recipients, and network IP addresses or host names.	❒	❒	
The government customer instance provides custom email malware and content filtering actions for agency specified custom-processing lists.	❒	❒	
The government customer instance scans email allowed by an agency specified custom-processing list for malware or undesirable content and tags it if found.	❒	❒	

CSPs tailor their email malware and content filtering services for individual agency mail domains.		❒	❒	
Institutional				
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.CF.06 (Critical)

For email received from other agency mail domains known to have domain-level sender authentication (for example Domain Keys Identified Mail or Sender Policy Framework) the government customer instance includes the results of the domain-level sender forgery analysis when determining potentially suspicious or undesirable email. This capability is intended to support domain-level sender authentication, but does not necessarily confirm a particular sender or message is trustworthy. Scoring criteria for this capability will be aligned with the National Strategy for Trusted Identities in Cyberspace (NSTIC). The CSP takes agency specific actions for email determined to be suspicious or undesirable.

Clarification

The CSP must have:
-a process to monitor domain level authentication
-a defined schedule to update the list of domains that use domain level authentication protocols, such as DKIM or SPF
-a default action for each forged mail detected

Examples of Evidence Sought

The CSP can demonstrate:
-how it scans email messages for authenticity given a domain that uses DKIM or SPF
-a list of logged, unauthenticated email messages flagged by DKIM or SPF

The CSP can provide:
-log file evidence showing that it is scanning for mail forgery
-a documented process for incorporating changes to the list of domains that use DKIM or SPF
-a documented schedule for frequency of updates to the list of domains that use DKIM or SPF
-a documented action for each forged mail detected

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP includes domain-level sender forgery analysis when determining potentially suspicious or undesirable mail.	❒	❒	
The CSP takes agency specific actions on the detection of a forged mail	❒	❒	
Institutional			
The CSP has the appropriately trained, credentialed personnel in place to support scanning for mail forgery detection in SMTP messages.	❒	❒	

The CSP has defined policies or guidance in place that specifies domain-level sender forgery analysis.		❒	❒	
The CSP has defined processes in place to specify how to perform domain-level sender forgery analysis.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.CF.10 (Critical)			
The CSP limits and documents the use of unauthenticated, cleartext protocols for CSP management and will phase out such protocols or enable cryptographic authentication where technically and operationally feasible.			
Clarification			
As part of the capability, the CSP must not use clear-text protocols for CSP management. Only cryptographic authenticated protocols should be used for CSP management where technically and operationally feasible. If the system requires the use of a clear-text protocol such as Telnet or FTP, the service must be behind a firewall and documented and maintained. (Over time such protocols will be phased out of production by the CSP).			
Team Guidance			
The assessment of this capability is to determine if the CSP allows unauthenticated or clear-text protocols for CSP management. A CSP can be exempted from this capability in the case of clear-text and unauthenticated protocols that are technically and operationally infeasible to change. However, they must follow several guidelines. Examples of clear-text protocols: FTP, Telnet, HTTP, Rlogin, etc. If a device supports authenticated cryptographic sessions, cleartext management is not permitted. An unencrypted remote session must use VPN and terminate outside the firewall as to not bypass the security architecture. The connection will be proxied at the firewall or via an application proxy. Clear-text protocols are acceptable via a site-to-site VPN between trusted enclaves; however, an Acknowledgement of Risk Letter (AORL) must be in place for the tunnel. Clear-text protocols are acceptable with local and direct physical access, such as use with a console cable or a direct network connection.			
Examples of Evidence Sought			
The CSP can demonstrate: -the use of authentication protocols for CSP management The CSP can provide: -a list of authenticated cryptographic protocols that are used to manage CSP systems -a list of unauthenticated and clear-text protocols that have been granted exceptions -a documentation showing the steps taken by the organization to mitigate risks of unauthenticated and clear-text protocols			
Scoring Criteria			
	Yes	No	Evidence

Technical				
The CSP uses authenticated FIPS 140-2 cryptographic protocols for CSP management where technically and operationally feasible.		❒	❒	
Where operationally infeasible and where cleartext protocols are in use, the CSP must: set a password expiration date no longer than 90 days; ensure the user does not have administrative or root privileges; disable anonymous or guest access to the system.		❒	❒	
The CSP documents any cleartext protocols in use for CSP management.		❒	❒	
The CSP has defined processes in place to specify how to add or transition from an unauthenticated or clear-text protocol to an authenticated and cryptographic protocol.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place that specifies and documents each protocol used for CSP management.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.CF.11 (Critical)			
The CSP has a documented procedure or plan that explains how it inspects and analyzes encrypted traffic. The document includes a description of defensive measures taken to protect CSP clients from malicious content or unauthorized data exfiltration when traffic is encrypted. The government customer instance analyzes all encrypted traffic for suspicious patterns that might indicate malicious activity and logs at least the source, destination and size of the encrypted connections for further analysis.			
Clarification			
This capability does not require the CSP to decrypt encrypted traffic. It only requires the CSP to log information about encrypted traffic, and analyze that information for patterns.			
Team Guidance			
What is important here is whether the CSP is clearly documenting how they handle and log encrypted connections. The source and destination addresses and ports associated with encrypted connections, not the entire encrypted packet, is what must be logged. NOTE: NCPS (Einstein) is not part of this requirement, and cannot be used by CSP to 'meet' it. Documentation MUST be provided.			
Examples of Evidence Sought			
The CSP can demonstrate: -the tools used to collect session data associated with encrypted connections (capture of packet headers from a router, log aggregation, etc.) -the ability to pull up session data associated with encrypted connections The CSP can provide: -clearly documented procedures for how encrypted traffic is handled and logged -network documentation or diagrams that show where encrypted connections terminate			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP has a tool in place to collect session data associated with encrypted connections.	❒	❒	
The CSP identifies encrypted connections and logs information about them. Logs include source, destination, and amount of traffic sent.	❒	❒	
The CSP analyzes the data collected about encrypted	❒	❒	

connections for suspicious activities.				
The CSP has a documented procedure or plan for identifying and analyzing encrypted traffic sessions.		❒	❒	
Institutional				
The CSP has a defined policy or guidance in place that specifies protection of CSP clients from malicious content and prevents unauthorized data exfiltration in encrypted traffic.		❒	❒	
The CSP has defined processes in place that specify how it handles encrypted connections.		❒	❒	
The CSP has defined processes in place that specifies how to log the source/destination of all encrypted connections.		❒	❒	
The CSP has the appropriately trained personnel in place to support capturing and storing session data associated with encrypted connections.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.CF.13 (Critical)

The government customer instance filters DNS queries, and performs validation of DNS Security Extensions (DNSSEC) signed domains, for CSP clients. The CSP configures DNS resolving/recursive (also known as caching) name servers in accordance with, but not limited to, the following recommendations from NIST SP 800-81 Revision 1 (Draft):
1. The CSP deploys separate recursive name servers from authoritative name servers to prevent cache poisoning.
2. The CSP filters DNS queries for known malicious domains.
3. The CSP logs at least the query, answer, and client identifier.

Clarification

This capability is intended to differentiate a CSP's externally accessible Domain Name Servers from its internal domain name servers. CSP clients must use an internal recursive name server for querying domain information, and must not be allowed to go directly to an external domain name server for results. Internal recursive domain name servers should validate DNSSEC information returned as a part of a query prior to passing the information along to the requesting client.

The use of an internal recursive domain name server allows the CSP to filter out requests for known bad domains internally, before they are requested from the internet. This allows the CSP to either send a negative response to the client, or redirect the client to a safe location.

Team Guidance

Note that criteria for filtering DNS queries for known malicious domains are somewhat vague. "Known malicious" domains is clearly subject to the CSP's judgment, and therefore, there is no standard blacklist they should be using. They should merely demonstrate that they can, and are, filtering for known-bad domain names.

Examples of Evidence Sought

Sample log showing a complete client request for information about a given domain, and the response delivered by the name server. Consider obtaining logs from more than one domain name server (if applicable) to verify logging is consistent across servers.
If using a vendor to deploy DNSSEC, vendor documentation of compliance with NIST controls.
DNS architecture showing that the caching non-authoritative servers are deployed separately from the authoritative domain name servers for the zone.

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP deploys caching, non-authoritative name servers to perform recursive queries as required. These servers are separate from the authoritative name servers used to service external requests.	❒	❒	

The CSP performs filtering at the domain name server for queries relating to known-malicious DNS domain names. Queries for known-malicious domains are black-holed or otherwise blocked.		❒	❒	
The CSP logs all DNS queries and answers, including the requesting client.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place to specify DNSSEC operations and management of the CSP DNS infrastructure.		❒	❒	
The CSP has defined processes in place to specify how to monitor and support DNSSEC operations and the CSP DNS infrastructure.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.INS.01 (Critical)			
The government customer instance participates in the National Cyber Protection System (NCPS, operationally known as Einstein).			
Clarification			
Specific support requirements are provided to each CSP as part of the NCPS agreement with DHS. The CSP must participate in version 2 of the NCPS (Einstein) program for compliance with this capability. Participation in this regard means: - The CSP has fully executed all the required agreements (MOU, ISA, etc.) - The NCPS equipment is installed and operating (e.g., collecting network traffic) (Participation in Einstein v1 does not constitute compliance)			
Team Guidance			
The CSP assessment team can obtain information through interviews onsite and visual inspection of the NCPS (Einstein) devices. In addition, the team must confirm compliance with DHS to assure that the agreements have been fully executed (the Federal Government team lead can contact the appropriate DHS individual to obtain this confirmation)			
Examples of Evidence Sought			
The FNS Government Lead can check with the NCSD's Network Security Deployment branch to ensure the CSP's NCPS equipment is fully operational and all agreements have been completed. The Federal Government Lead provides this feedback to the assessment team. The CSP can show: - the location of the NCPS (Einstein) device(s) that are operational and collecting data The CSP can provide: - copies of the signed agreements			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP has all applicable (fully executed) agreements on file with the NCSD and/or US-CERT.	❒	❒	
The NCPS devices are in protected space and only authorized staff have access to the system.	❒	❒	
The DHS NCSD confirms the CSP has a fully operational NCPS v2 or higher appliance installed, configured, and collecting data.	❒	❒	

Institutional				
The CSP has defined policies or guidance in place to specify compliance with installation and operations of the devices.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to support the NCPS devices.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.INS.02 (Critical)			
The government customer instance passes all inbound/outbound network traffic through Network Intrusion Detection Systems (NIDS) configured with custom signatures, including signatures for the application layer. This includes, but is not limited to, critical signatures published by US-CERT.			
Clarification			
The intent is the CSP has its own NIDS capability, and does not solely rely on the NCPS for IDS. The CSP can integrate custom IDS signatures. All traffic passing through the CSP must be inspected by a NIDS.			
Team Guidance			
The CSP must be operating an IDS solution capable of accepting custom signatures from US-CERT, such as SNORT-based signatures. The CSP must have staff with the ability to take action and load custom signatures on its sensors from vendors, US-CERT, etc. The CSP does not need to be able to write custom signatures as long as it has the ability to obtain and implement custom signatures (vendor-provided, US-CERT, etc.). Example: ISS requires an SLA with IBM to be able to obtain and load custom signatures (SNORT). If the CSP is using ISS, it should be able to show the SLA with IBM, if it doesn't have an SLA, the department and/or agency must be able to demonstrate how it is going to accommodate custom signatures.			
Examples of Evidence Sought			
The CSP can demonstrate: -how this capability is performed, the process for receiving, reviewing and updating these signatures, and the update cycle, to ensure signatures are current. - the process for adding custom signatures to the IDS configuration - If it can perform this action in timeframes, as specified by policy or SLA. - testing mechanisms and deployment schedules based on the threat - the tools used to support implementation of custom IDS signatures - what type of NIDS is implemented and how it is used - where and how NIDS devices are strategically placed within the CSP - that all traffic is passed through the NIDS and how analysis is done on this traffic The CSP can provide: - documented policies on handling and implementing IDS signatures - documented procedures for maintaining IDS configuration, signatures, and stability - QA test/audit reports of IDS signature maintenance - policies and procedures for maintaining NIDS configuration, signatures, and stability - QA test/audit reports of NIDS operations and maintenance			
Scoring Criteria			
	Yes	No	Evidence
Technical			

The CSP has deployed a NIDS solution to monitor and filter all network traffic passing through the CSP boundary.		❒	❒	
The NIDS is configured with custom signatures to meet agency needs, including the application-layer signatures and critical signatures published by US-CERT.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place to specify that custom IDS signatures (including those from US-CERT) must be tested and implemented within timeframes specified by policy or defined in SLA.		❒	❒	
The CSP has defined processes in place to specify how to test and implement custom IDS signatures, including those from US-CERT.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to test and implement custom IDS signatures, including those from US-CERT.		❒	❒	
The CSP has the appropriate tools in place to support testing and implementing custom IDS signatures, including those from US-CERT.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.PF.01 (Critical)

All external connections are routed through a government customer instance, scanned and filtered by CSP systems and components according to the CSP's documented policy, which includes critical security policies when published by US-CERT. The definition of "external connection" is in accordance with the CSP Reference Architecture, Appendix A (Definition of External Connection).

Clarification

The intent of this capability is to ensure all external connections are protected by the government customer instance scanning and filtering components. The effectiveness of those components will be validated in other capabilities. This capability should verify that all external connections are documented, protected by government customer instance systems, and the security controls in place are documented in the CSP policy.

Team Guidance

External Connection: A physical or logical connection between information systems, networks, or components of information systems and networks in which one is inside and the other outside of the specific Certification and Accreditation (C+A) boundaries established by the D/A, where:
the D/A does not have control over the application of required security controls or the assessment of security control effectiveness on the outside information system, network, or components of information systems or networks; or
the D/A, notwithstanding control over the application of required security controls or the assessment of security control effectiveness, has specific reason to believe that the external system has a substantially reduced set of security controls or an increased threat posture relative to the internal system; or
the connection could be used to establish a connection with an external system that is not routed through an approved CSP.

Examples of Evidence Sought

The CSP can demonstrate:
-The physical connectivity between all CSP routers that connect or aggregate customer agency networks for external connection.
-The process for detecting unauthorized external connections at the CSP.
-A walkthrough of the change management process for CSP systems and components.

The CSP can provide:
-System and Communications Protection Policy that:
-Details the security controls that compose the CSP access point.
-Defines internal and external boundaries.
-Defines which external networks customer agency traffic will be routed.
-Specifies that all external connections will pass through a CSP access point.
-Specifies all external connections should be scanned and filtered by the CSP systems and components.
-Defines process for detecting unauthorized external connections.
-QA test/audit reports of access points and external connections.
-The routing tables for all CSP routers that connect or aggregate customer agency networks for external connection.
-Configuration files for all CSP routers that connect or aggregate customer agency networks for external connection.
-Change Management Policy that details the process for making changes to any router that connects or

aggregates customer agency networks for external connection.
-Change Management Procedures for making changes to any router that connects or aggregates customer agency networks for external connection.
-An external connections inventory that describes the Capacity of each external connection, the approximate utilization of each external connection and the location (access point) of the external connection.
-Security Assessment and Authorization Policy that documents the interface characteristics, security requirements, and the nature of the information communicated for each external connection.
-High level information system architecture and network diagrams illustrating network security devices between the internal and external networks, the flow of traffic, connection capacity and approximate utilization.

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP routes all external connections through a Government customer instance.	❒	❒	
All external connections are scanned and filtered by Government customer instance systems and components in accordance with CSP and US-CERT documented policies.	❒	❒	
Institutional			
The CSP has the appropriately trained, credentialed personnel in place to ensure all external connections through a CSP access point.	❒	❒	
The CSP has the appropriate tools in place to ensure all external connections through a CSP access point.	❒	❒	
The CSP has defined policies or guidance in place for ensuring all external connections are routed through a CSP access point.	❒	❒	
The CSP has defined processes in place that specify how to ensure all external connections are routed through a CSP access point.	❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.	❒	❒	

Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.PF.02 (Critical)
By default, the government customer instance blocks network protocols, ports, and services. The government customer instance only allows necessary network protocols, ports, or services with a documented mission requirement and approval.
Clarification
By default, a government customer instance must block ALL network protocols and services (both IPv4 and IPv6). Each unblocked port, protocol, or service must be an integral part of a documented mission requirement, and must be authorized by appropriate CSP management personnel.
Team Guidance
What this means is that a CSP must adopt a default-deny policy for IPv4 and IPv6. Any unblocked ports, protocols, or services must be treated as exceptions to this policy, and must be accompanied by a justification and authorization. All firewalls used by the CSP must have an easily observed default deny instruction at the end of the firewall rules chain in the configuration file.
Examples of Evidence Sought
The CSP can demonstrate: - the process and supporting tools in place to handle requests for exceptions - an existing request and explain how it is reviewed, approved, or rejected and how the customer is notified - tools, procedures, and services available for performing this activity The CSP can provide: - a documented process for handling and approving exception list changes - a list of protocols that have been granted exceptions - meeting minutes from any review or change/configuration management boards that review such requests and detail the handling of this activity - a description or documentation detailing any review boards, or change/configuration management boards that handle such requests - any forms or interfaces used by customers or users to request such changes - QA test/audit reports of exception lists for authorized protocols - documentation that explains the inspection and process to implement a block on non-proxied traffic - a documented process for handling and approving changes to the types of traffic that are proxied
Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP perimeter defenses are configured using default-deny configuration rules for ports, protocols, and services.	❒	❒	
Exceptions to the default-deny rules are based strictly on	❒	❒	

documented needs that are tied to mission requirements and are made only after approval by a defined, authorized party.				
Institutional				
The CSP has defined policies or guidance in place that specifies that exception requests for any protocol must be received and managed.		❒	❒	
The CSP has defined processes in place that specifies how to receive and manage exception requests for any protocol.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to receive and manage exception requests for any protocol.		❒	❒	
The CSP has the appropriate tools in place to receive and manage exception requests for any protocol.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.PF.03 (Critical)					
The government customer instance implements stateless filtering of all inbound and outbound connections without being limited by connection state tables of CSP systems and components. Attributes inspected by Stateless Filters include, but are not limited to: - Direction (inbound, outbound, interface) - Source and destination IPv4/IPv6 addresses and network masks - Network protocols (TCP, UDP, ICMP, etc.) - Source and destination port numbers (TCP, UDP) - Message codes (ICMP)					
Team Guidance					
Stateless filtering of network traffic includes all filtering that requires no knowledge of prior network traffic.					
Examples of Evidence Sought					
The CSP can demonstrate: -that it uses stateless filtering to monitor all inbound and outbound connections. -stateless packet filtering The CSP can provide: -access control lists on routers -a documented process for incorporating changes in the identification criteria -a documented schedule for frequency of updates or refreshes -an existing ticket or request to implement or remove a specific filter -a network diagram that shows where stateless filtering exists					
Scoring Criteria					
		Yes	No	Evidence	
Technical					
The government customer instance implements stateless filtering of all inbound and outbound connections.		❒	❒		
Institutional					
The CSP has defined policies or guidance in place that specify stateless filtering.		❒	❒		
The CSP has defined processes in place to specify how to perform stateless filtering.		❒	❒		
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TS.PF.04 (Critical)

By default, the government customer instance blocks unsolicited inbound connections. For authorized outbound connections, the government customer instance implements stateful inspection that tracks the state of all outbound connections and blocks packets which deviate from standard protocol state transitions. Protocols supported by stateful inspection devices include, but are not limited to:
- ICMP (errors matched to original protocol header)
- TCP (using protocol state transitions)
- UDP (using timeouts)
- Other Internet protocols (using timeouts)
- Stateless network filtering attributes

Team Guidance

Stateful inspection tracks the state of all inbound and outbound connections and blocks packets which deviate from standard protocol state transitions.

With today's infrastructure tools and appliances, most firewalls have this function turned on by default. However, the CSP assessment team should make sure that the capability is engaged and operational.

Examples of Evidence Sought

The CSP can demonstrate on in-line networking equipment that can block inbound / outbound traffic:
- a console view of a current state table
- a current running configuration (Cisco IOS uses the " inspect" series of commands)

The CSP can provide:
- printed configuration files from the CSP equipment
- QA test/audit reports of use of stateful packet inspection

Note: No mention of state could mean state is left on; mention of state would most likely indicate a modification or state being turned off

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP filters inbound and outbound connections based on stateful packet inspection.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place requiring stateful packet inspection services.	❒	❒	
The CSP has defined processes in place to specify how to perform stateful packet inspection services.	❒	❒	

The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained personnel in place to manage stateful packet inspection services.		❒	❒	
The CSP has the appropriate tools in place to support stateful packet inspection services.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.PF.05 (Critical)

The government customer instance only permits outbound connections from previously defined CSP clients using Egress Source Address Verification. It is recommended that inbound filtering rules block traffic from packet source addresses assigned to internal networks and special use addresses (IPv4-RFC5735, IPv6-RFC5156).

Clarification

The intent of this capability is to ensure that:

1) Traffic entering the CSP from an external source comes from a known routable IP address space, and not from a non-routable, multicast, or broadcast address space.
2) Traffic leaving the CSP is addressed from a known routable IP address space allocated to the CSP
3) Traffic that is non-routable, multicast, or broadcast is not allowed to leave the CSP.

The non-routable, multicast, and broadcast address ranges for IPv4 and IPv6 are listed in IETF RFCs 5156 and 5735. Please see http://tools.ietf.org for more information.

Team Guidance

From http://merlot.tools.ietf.org/search/rfc3330:

Address Block	Present Use	Reference
0.0.0.0/8	"This" Network	RFC1700, page 4
10.0.0.0/8	Private-Use Networks	RFC1918
14.0.0.0/8	Public-Data Networks	RFC1700, page 181
24.0.0.0/8	Cable Television Networks	--
39.0.0.0/8	Reserved but subject to allocation	RFC1797
127.0.0.0/8	Loopback	RFC1700, page 5
128.0.0.0/16	Reserved but subject to allocation	
169.254.0.0/16	Link Local	
172.16.0.0/12	Private-Use Networks	RFC1918
191.255.0.0/16	Reserved but subject to allocation	
192.0.0.0/24	Reserved but subject to allocation	
192.0.2.0/24	Test-Net	
192.88.99.0/24	6to4 Relay Anycast	RFC3068
192.168.0.0/16	Private-Use Networks	RFC1918
198.18.0.0/15	Network Interconnect Device Benchmark Testing	RFC2544
223.255.255.0/24	Reserved but subject to allocation	
224.0.0.0/4	Multicast	RFC3171
240.0.0.0/4	Reserved for Future Use	RFC1700, page 4
::1/128	Loopback	RFC 4291
::/128	Unspecified Address	RFC4291

::FFFF:0:0/96	IPv4 mapped addresses	RFC4291
::{ipv4-address}/96	IPv4 compatible addresses	RFC4291
fe80::/10	Link Local	RFC4291
fc00::/7	Unique Local Addresses	RFC4193
2001:db8::/32	Documentation Addresses	RFC3849
2002::/16	6to4 Relay Anycast	RFC3849
2001::/32	Teredo addresses	RFC4380
5f00::/8	6bone (first instance)	RFC1897
3ffe::/16	6bone (second instance)	RFC2471
2001:10::/28	ORCHID	RFC4843
::/0	Default Unicast	
ff00::/8	Multicast	RFC4291

Examples of Evidence Sought

The CSP can demonstrate:
- Filtering of inbound connections
- Filtering of outbound connections

The CSP can provide:
- A list of known CSP client IP addresses

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP maintains a list of known CSP client IP addresses.	❒	❒	
The CSP permits outbound connections only from known CSP clients.	❒	❒	
The CSP filters all inbound IPv4 and IPv6 traffic to ensure it comes from a valid, known routable IPv4 or IPv6 address space.	❒	❒	
The CSP filters all outbound IPv4 and IPv6 traffic to ensure it comes from a known routable IPv4 or IPv6 address space allocated to the CSP.	❒	❒	
The CSP filters all inbound and outbound multicast and broadcast IPv4 and IPv6 traffic.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place that specifies filtering of non-CSP addresses.	❒	❒	

The CSP has defined policies or guidance in place that specifies filtering of special use and internal addresses.		❒	❒	
The CSP has defined processes in place to specify how to filter addresses.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.PF.06 (Critical)			
CSP stateful inspection devices correctly process traffic returning through asymmetric routes to a different CSP stateful inspection device; or document how return traffic is always routed to the same CSP stateful inspection device.			
Team Guidance			
For purposes of this capability, a CSP must be able to prove one of two potential ways to satisfy this capability. The first way is to show that inspection devices located in one government customer instance are synchronized with the inspection devices located in all other government customer instances. This is usually accomplished through a network link between the government customer instances that sits behind the entirety of the CSP stack for protection. The second way is to show that replies to traffic that originated at one government customer instance that are sent to a different government customer instance are either re-routed or routed internally back to the correct access point, so that the replication of state information is not necessary.			
Examples of Evidence Sought			
The CSP can provide: -Some form of state table between the government customer instances at the CSP. -Documented policy or procedure for stateful inspection.			
Scoring Criteria			
	Yes	No	Evidence
Technical			
The CSP replicates state information between stateful inspection devices in near-real time to accommodate return traffic that routes back to the CSP through a stateful inspection device other than the one which initiated the session.	❒	❒	
The stateful inspection device, using replicated state information, inspects traffic entering/leaving a Government customer instance regardless of whether or not it originated from a different Government customer instance.	❒	❒	
The CSP re-routes replies to traffic generated at one Government customer instance that are received at a different Government customer instance back to the originating Government customer instance before the traffic transits any Government customer instance security stack.	❒	❒	

Institutional				
The CSP has the appropriate tools to verify, and make changes, to state replication when needed.		❒	❒	
The CSP has defined policies or guidance in place to support replicating state information between CSP security stacks.		❒	❒	
The CSP has defined processes in place to specify how to monitor and filter traffic returned to the infrastructure via an alternate route and alternate CSP.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.RA.01 (Critical)

The government customer instance supports telework/remote access for CSP client authorized staff and users using ad-hoc Virtual Private Networks (VPNs) through external connections, including the Internet. This capability is not intended to include permanent VPN connections for remote branch offices or similar locations. In addition to supporting the requirements of OMB M-06-16, “Protection of Sensitive Agency Information," the following baseline capabilities are supported for telework/remote access at the government customer instance:
1. The VPN connection terminates behind NCPS and full suite of CSP capabilities which means all outbound traffic to/from the VPN users to external connections, including the Internet, can be inspected by NCPS.
2. The VPN connection terminates in front of CSP-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from remote access users to internal networks to be inspected.
3. NIST FIPS 140-2 validated cryptography is used to implement encryption on all VPN connections (see NIST SP 800-46 Rev1).
4. Split tunneling is not allowed (see NIST SP 800-46 Rev1). Any VPN connection that allows split tunneling is considered an external connection, and terminates in front of NCPS.
5. Multi-factor authentication is used (see NIST SP 800-46 Rev1).
6. VPN concentrators and Virtual-Desktop/Application Gateways use hardened appliances maintained as CSP network security boundary devices.
7. If telework/remote clients use Government Furnished Equipment (GFE), the VPN connection may use access at the IP network-level and access through specific Virtual Desktops/Application Gateways.
8. If telework/remote clients use non-GFE, the VPN connection uses only access through specific Virtual Desktops/Application Gateways.

CSP clients may support additional telework/remote access connections for authorized staff and users using equivalent agency-managed security controls at non-government customer instance locations. The agency-level NOC/SOC is responsible for maintaining the inventory of additional telework/remote access connections and coordinating agency-managed security controls.

Because of the difficulty verifying the configuration, sanitizing temporary and permanent data storage, and analyzing possible compromises of non-Government Furnished Equipment, it is the agency’s responsibility to document in accordance with OMB M-07-16 if sensitive data may be accessed remotely using non-GFE, and informing the CSP Access Provider of the appropriate security configuration policies to implement.

Clarification

The intent of this capability is to ensure that the CSP provides access for authorized users to perform their job duties, even when the users are not physically present at a CSP or client agency location. This capability does not include permanent VPN connections to remote offices or external partners – those connections are covered by CSP.TS.RA.02. If the CSP chooses to allow split tunneling for telework/remote access, those connections MUST be treated as external / untrusted connections and terminate in front of the NCPS suite and CSP security stack, and therefore fall under the CSP.TS.RA.02 capability.

Despite the VPN connections terminating behind the NCPS (Einstein) and CSP security stacks, the CSP must filter all traffic from a VPN tunnel through, at a minimum, an Intrusion Detection System and Stateful Packet Inspection capable firewall. Traffic from the VPN destined for the internet MUST be routed through the CSP security stack and NCPS.

Team Guidance

For the CSP.TS.RA capabilities, the terms “in front of” and “behind” are used to describe locations in a CSP’s network relative to the CSP security stack and the NCPS. “In front of” means that the VPN concentrator is located outside the government customer instance’s security boundary, and all traffic to and from the VPN concentrator is subject to the full CSP security stack inspection and logging by NCPS. (A physical analogue to this concept is a bus taking you to a military facility, and dropping you off outside the main gate. You would still have to pass a full inspection of credentials and baggage before being allowed into the facility.)

In contrast, “Behind” means that the VPN concentrator is located inside the CSP security boundary, and thus all traffic to the concentrator is still encrypted when it transits the CSP security stack and NCPS, rendering their protections ineffective. Decrypted traffic is then subject to a smaller set of protections (IDS and firewall at a minimum) before being sent into the CSP’s network. (The corresponding physical analogue to this is if the bus from the prior example takes you through the main gate to the facility without inspection, but drops you off outside a secure building. You must still pass through a smaller security checkpoint to visit the secure building, but it is less intensive than the main checkpoint, and no log of your arrival at the main gate is required.)

The baseline capabilities are generally drawn from NIST SP 800-46 Rev 1. In general, Virtual Private Networks can handle client (user) network traffic in one of two ways. The first method, called “Split Tunneling” only directs data meant for the CSP’s network through the VPN, allowing all other traffic to exit the client (user)’s local network normally. In this mode, the CSP is only aware of traffic meant for its networks, which is a security concern as the client’s (user’s) computer may be compromised through regular internet traffic while connected to the CSP VPN tunnel. Since the VPN connection terminates behind the NCPS and CSP security stack, traffic from a compromised client is not subject to as thorough an inspection and packet capture, which places the CSP and client agency networks at risk.
The second mode is known as a “Full Tunnel”, and directs all network traffic generated by the client’s (user’s) computer through the VPN tunnel, regardless of its eventual destination. In this mode, all traffic generated by the client is visible to the CSP, and can be filtered / logged as appropriate, just as if the client’s (user’s) computer were located on the local network.

It is important to note that if a CSP allows “Split Tunneling” for VPN connections that this capability’s requirements do not apply – apply CSP.TS.RA.02 instead. If “Split tunneling” is allowed, and the VPN concentrator is located behind the CSP security stack, the CSP is NOT compliant for this capability.

Please note that OMB M-06-16 requires a maximum “Idle” timeout of 30 minutes. If the VPN concentrator has not seen any client traffic for 30 minutes, the corresponding tunnel MUST be closed.

See capability CSP.TM.AU.01 for a discussion of multi-factor authentication covering baseline capability #5.
If the remote client/user is not accessing the VPN from government furnished (and managed) equipment, their VPN tunnel traffic must be routed immediately to an application server or virtual desktop environment, and MUST NOT be allowed to access any other portion of the CSP network.

Please note that all devices used as a part of the telework remote access package are subject to the capabilities that govern all other CSP stack devices. If the CSP utilizes a Remote Desktop or Application Gateway, that gateway must also be hardened and maintained as with all other CSP stack devices.

Examples of Evidence Sought

The CSP can demonstrate:
-The process of externally connecting to a remote access VPN with multi-factor authentication.
-The process of configuring access for a remote access VPN user.
-The process for making configuration changes to remote access VPN devices.
-Split Tunneling is not implemented by verifying all remote access VPN traffic is sent through the

encrypted tunnel to CSP before traversing the Internet.

The CSP can provide:
Access Control Policy that:
-Specifies what groups of users are authorized to connect to the remote access VPN.
-Details the process for configuring a remote access VPN user.
-Specifies remote access VPN cryptography will adhere to FIPS 140-2 standards for both cryptographic modules and cryptographic algorithms.
-Details procedures to periodically ensure remote access VPN cryptography will adhere to FIPS 140-2 standards for both cryptographic modules and cryptographic algorithms.
-Specifies Split Tunneling will not be used for any remote access VPN connection.
-Specifies that multi-factor authentication will be used for remote access VPN authentication and that one of the factors is provided by a device separate from the computer gaining access.
-Details the process for multi-factor authentication.
-Specifies that non-GFE must connect only to Virtual Desktops/Application Gateways when remotely accessing the internal network.
-Details the procedures for ensuring non-GFE only connect to Virtual Desktops/Application Gateways when remotely accessing the internal network.
-Specifies remote access VPN sessions will be terminated after 30 minutes of inactivity.
-System and Information Integrity Policy that:
-Specifies that remote access VPN devices will be hardened, maintained, and protected.
-Details how remote access VPN devices will be hardened, maintained, and protected.
-Configuration Management Policy that:
-Specifies configuration management is required for remote access VPN devices.
-Details the process for altering the configuration of remote access VPN devices.
-The manufacturer name, model name, and major firmware release version of all remote access VPN devices.
-The cryptographic algorithm and related IPSEC configuration information (if applicable) – e.g. Diffie Hellman, HMAC – for all remote access VPN connections.
-High level information system architecture and network diagrams illustrating network security devices between the internal and external networks, the location of all remote access VPN devices, and the flow of all remote access VPN traffic.
-Remote access VPN device configuration that enforces a session to terminate after 30 minutes of inactivity.

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP terminates all telework remote access VPN connections behind NCPS and the full suite of CSP capabilities.	❒	❒	
The CSP terminates all telework remote access VPN connections in front of CSP-managed security controls including, but not limited to, a firewall and IDS/IPS.	❒	❒	
The CSP uses FIPS 140-2 validated cryptographic modules and FIPS 140-2 validated cryptographic algorithms to implement encryption on all VPN connections.	❒	❒	

The CSP does not allow split tunneling on any telework remote access VPN connection.		❒	❒	
The CSP enforces multi-factor authentication for all telework remote access VPN connections.		❒	❒	
The CSP requires all non-GFE devices to connect to a specific Virtual Desktop or Application Gateway.		❒	❒	
The CSP enforces a time-out after 30 minutes of inactivity for all remote access connections. (See OMB M-06-16)		❒	❒	
The government customer instance supports telework/remote access for CSP client authorized staff and users using ad-hoc Virtual Private Networks (VPNs) through external connections, including the Internet.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.RA.02 (Critical)

The government customer instance supports dedicated external connections to external partners (e.g., non-CSP federal agencies, externally connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. The following baseline capabilities are supported for external dedicated VPN and private line connections at the government customer instance:
1. The connection terminates in front of NCPS to allow traffic to/from the external connections to be inspected.
2. The connection terminates in front of the full suite of CSP capabilities to allow traffic to/from external connections to be inspected.
3. VPN connections use NIST FIPS 140-2 validated cryptography over shared public networks, including the Internet.
4. Connections terminated in front of NCPS may use split tunneling.

Clarification

The intent of this capability is to ensure that the CSP treats permanent and temporary network connections to external partners as un-trusted connections, regardless of the physical or logical type of connection. All external partner connections must terminate in front of the NCPS, which means that all partner traffic must be decrypted and subject to inspection not only by the NCPS, but the entire CSP security stack as well before it enters the CSP internal network.
In addition to the inspection requirements, this capability also requires that a CSP document all external partner connections, and ensure that those connections have a documented mission requirement and appropriate administrative approval.
As the network traffic to and from external partners is subject to NCPS and the full CSP security suite, split tunneling is allowed, but not required, for partners connecting to the CSP over VPN connections.

Team Guidance

For the purposes of this capability, all connections must terminate “in front of” the NCPS and the full CSP security suite, as defined in the team guidance for CSP.TS.RA.01. The intent of this capability is to ensure that the CSP limits its exposure to potentially malicious traffic coming from partner organizations, and must consciously commit to and document the modifications to the CSP security suite (firewall rules, reverse proxy rules, intrusion detection rules, routing rules, etc.) required to do business with that external partner. In the event that malicious traffic does come from a partner organization, the NCPS and CSP security suite logging mechanisms can then be used to provide methods for analysis and mitigation if necessary.
If external partner organizations use a Virtual Private Network to communicate with the CSP or its clients, that VPN must conform to FIPS 140-2 cryptographic requirements for the protection of data over the VPN tunnel. This is to ensure adequate protection of data while it is in transit between the CSP and the external partner. Unlike capability CSP.TS.RA.01, multi-factor authentication is not required to establish these VPN tunnels.

If the CSP does not have any external connections, then this capability (and all indicators) should be scored as “Not Applicable”.

Examples of Evidence Sought

The CSP can demonstrate:

-The process of configuring a new Permanent, Site-to-Site, VPN connection to external partners.
-The process of configuring a new private line connection to external partners.

The CSP can provide:
Access Control Policy that:
-Specifies Permanent, Site-to-Site VPN cryptography will adhere to FIPS 140-2 standards for both cryptographic modules and cryptographic algorithms.
-Details procedures to periodically ensure Permanent, Site-to-Site VPN cryptography will adhere to FIPS 140-2 standards for both cryptographic modules and cryptographic algorithms.
-High level information system architecture and network diagrams illustrating network security devices between the internal and external networks, the location of all Permanent, Site-to-Site VPN devices and -Private Lines, and the flow of all Permanent, Site-to-Site VPN traffic and Private Lines.
-The manufacturer name, model name, and major firmware release version of all Permanent, Site-to-Site VPN devices.
-The cryptographic algorithm and related IPSEC configuration information – e.g. Diffie Hellman, HMAC – for all Permanent, Site-to-Site VPN connections.

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP terminates dedicated external connections to external partners in front of the full suite of CSP capabilities and NCPS.	❒	❒	
The CSP uses FIPS 140-2 validated cryptographic modules and FIPS 140-2 validated cryptographic algorithms to implement encryption on all Permanent, Site-to-Site VPN connections.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place to support dedicated external connections to external partners.	❒	❒	
The CSP has defined processes in place to specify how to support dedicated external connections to external partners.	❒	❒	
The CSP has staff practices in place to support dedicated external connections to external partners.	❒	❒	

Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Boundary Defense for the Cloud

Transferred Technical Capabilities

Homeland Security

Revision History

Date	Name	Revision
18MAY2012	A. Cooper J. Downing	Initial release of workbook template

Table of Contents

Summary

This workbook is a working draft adaptation of the CCV TIC 2.0 Capabilities Assessment workbook and summarizes 11 of the 74 TIC 2.0 Capabilities that will be met through FedRAMP requirements and/or standard customer contract clauses.

Capability #CSP.TM.DS.03

The government customer instance ensures that each customer agency retains ownership of the data collected by the government customer instance.

Clarification

The government customer instance does not own the data passing through the CSP, it is owned by the originating customer agency.

Data generated by a government customer instance must be afforded the same protections as defined by the agency's System Security Plan (SSP). In order to ensure these protections, the agency must maintain ownership of their data.

Team Guidance

The underlying issue is that the agency does not relinquish total ownership to the CSP, but still owns and is responsible for its data--even though it is managed by the service provider (CSP); therefore the CSP must be able to segregate each customer's data from any other customer's data, and be able to provide each customer with access to their own data, and only their own data.

Examples of Evidence Sought

The CSP can provide:
- Memorandums of Understanding (MOUs) that state data ownership is maintained by the originating agency.
- policies and procedures that prohibit the release of agency data without obtaining the agency's approval.
- policies and procedures to ensure the protection of the agency's data
-confirmation check between CSP's protection strategies and the customer's protection strategy (e.g., to demonstrate that equivalent levels of protection are applied)

Scoring Criteria

	Yes	No	Evidence
Technical			
Access to agency data is restricted to those with a need-to-know.	❒	❒	
Agreements exist between the agency and CSP stating the agency owns the data collected by the CSP.	❒	❒	
Institutional			
The CSP has defined polices or guidance in place to	❒	❒	

ensure the protection of the originating agency's data in accordance with the classification level of that data.					
The CSP has agreements in place to ensure the originating agency maintains ownership of their data.		❒	❒		
The CSP has defined policies or guidance in place that specify who may access agency data.		❒	❒		
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TM.DS.04

The CSP identifies and can retrieve each customer agency's data for the customer agency, without divulging any other agency's data.

Clarification

The intent is the CSP can provide each agency a copy of its own data kept by the CSP, without revealing data from other agencies.
This capability may be met by implementation of either physical or logical separation of client data.

Team Guidance

CSPs must be able to meet the agency's requirements. If the customer requires physical separation they must be able to provide it, regardless of cost. If the customer does not require physical separation, the CSP must still perform this function logically.

Examples of Evidence Sought

The CSP can demonstrate:
- the mechanisms used to physically or logically partition multiple agencies' data

The CSP can provide:
- supporting documentation that covers all stages of segmentation from equipment acquisition through deployment and maintenance
- documented policy describing the processes for partitioning
- documented procedures for handling segmentation of agency data
- examples of current customer SLAs or other requirements specifying what type of segmentation is required, along with how the CSP meets these requirements
- QA test/audit reports of segmentation

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP physically or logically partitions CSP components and data based on client ownership.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place to specify partitioning per SLA and agency requirements.	❒	❒	
The CSP has defined processes in place that specify how to monitor and manage the partitioning of components and data.	❒	❒	

The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained personnel in place to manage or control partitioning of components and data.		❒	❒	
The CSP has the appropriate tools in place to monitor partitioning of components and data.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TM.LOG.04

The CSP follows a documented procedure for log retention and disposal, including, but not limited to, administrative logs, session connection logs, and application transaction logs. Record retention and disposal schedules are in accordance with the National Archives and Records Administration existing General Records Schedules, in particular Schedule 12, “Communications Records” and Schedule 20, “Electronic Records;” or NARA approved agency-specific schedule.

Note: This capability is intended for the management and operation of the CSP itself, and does not require the CSP infer or implement retention policies based on the content of CSP client communications. The originator and recipient of communications through a CSP remain responsible for their own retention and disposal policies.

Clarification

The CSP must retain logs and data according its own internal requirements. The CSP must also retain logs and data owned by or referring to each client agency according to that client agency’s negotiated requirements.

Team Guidance

This capability assesses the CSP against its own log retention policy.

For general guidance on the creation and implementation of a log retention policy, see:

NARA General Records Schedule 24: Information Technology Operations and Management Records. (Administrative Logs)

NARA General Records Schedule 12: Communications Records. (Session connection/Application Transaction Logs)

Capability specific definitions:
- Logs: from the key components or appliances within the CSP, including firewall logs, router logs, proxy logs, IDS, and any logs produced from components in the NOC, SOC, or CSP necessary for event reconstruction

Examples of Evidence Sought

The CSP can demonstrate:
- evidence of the log retention schedule
- how each of the logs from the key CSP infrastructure components (Firewall, Proxy, Mail, IDS, SIM Tool, Network Performance, etc.) are archived and retained, for both on-line accessibility (7 days) and longer term archiving
- how off-site storage for retention of logs is accomplished

The CSP can provide:
- its log retention policy
- QA test/audit reports of log retention

The CSP can provide:
- its log retention policy (normally, 7 days online and 30 days offline)

The CSP can: - demonstrate the ability to collect and manage individual customer agency requirements - demonstrate customized log storage - provide customized retention policies - provide documented procedures and guidance for log data retention					
Scoring Criteria					
		Yes	No	Evidence	
Technical					
The CSP retains logs for 7 days online and 30 days offline. The CSP meets customer requirements in addition to normal CSP requirements (if the customer requires additional coverage).		❒	❒		
The CSP follows a documented procedure for log retention and disposal, including, but not limited to: administrative logs, session connection logs, and application transaction logs.		❒	❒		
Record retention and disposal schedules are in accordance with the National Archives and Records Administration existing General Records Schedules, in particular Schedule 12 "Communications Records" and Schedule 20 "electronic Records;" or NARA approved agency-specific schedule.		❒	❒		
Institutional					
The CSP follows a well-defined and documented data retention policy for archiving logs.		❒	❒		
The CSP has the appropriately trained, credentialed personnel in place to perform this capability.		❒	❒		
The CSP has the appropriate storage devices and media in place to support log retention.		❒	❒		
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TO.MG.08

The CSP provides each customer with a detailed Service Level Agreement.

Team Guidance

Certain parts of SLAs are expected to be fairly consistent, but the CSP must be able to customize the SLAs as needed to meet requirements for different agency subscribers.

Examples of Evidence Sought

The CSP can demonstrate:
- the process for collecting agency subscriber requirements and developing the customized SLA

The CSP can provide:
- completed SLAs for a sampling of customer agencies or bureaus showing how they are customized
- any supporting documentation that describes how this process is performed
- QA test/audit reports of SLA processes

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP has customized SLAs with current customer agencies.	❒	❒	
Institutional			
There is a defined policy and process for developing and periodically reviewing SLA's.	❒	❒	

Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MG.09

The CSP provides an exception request process for individual customers.

Team Guidance

This capability focuses on the CSP's ability to handle requests regarding exceptions to policy or changes to services.
The resolution process may be handled by the same Control Board or Technical Review Board discussed in other capabilities.
SLA is usually for a measurable performance measure and an MOU is usually for a roles and responsibilities document and either may apply here.

Examples of Evidence Sought

The CSP can demonstrate:
- the exemption resolution process for subscribing agencies to follow

The CSP can provide:
- SLAs, MOUs, a Concept of Operations (ConOps), or other documentation for subscribing agencies that describes the exemption resolution process and responsible or relevant personnel
- an example of an exemption resolution that was completed
- meeting minutes from any review board that handles exemption resolution
- QA test/audit reports of exemption resolutions

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP resolves exemptions with its customer agencies per SLAs, MOUs, or other agreements.	❒	❒	
The CSP provides an exception request process for individual customers.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place that specify exemptions must be resolved according to SLAs, MOUs, or other agreements	❒	❒	
The CSP has the appropriately trained personnel to handle exemptions.	❒	❒	

Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MG.10

The CSP accommodates individual customer agencies' security policies and corresponding security controls, as negotiated with the customer.

Team Guidance

Relevant tools might include something that defines what to do for which customer.
The CSP must have a mechanism in place to collect requirements for providing services to meet individual customer security policies.

Examples of Evidence Sought

The CSP can demonstrate:
- how it meets individual customer agencies' security policy requirements—this can include:
- a set of customer-specific requirements
- an explanation of how the specific requirements are met:
  - required hardware and/or software is in place
  - required configuration is in place
  - logging and reports verify that specific requirements are being met
  - evidence of change management/configuration management system to handle customer security requirements

The CSP can provide examples of:
- signed SLAs, MOAs, or various work products such as reports, traffic logs, or other artifacts evidencing support to multiple customers
- a fully executed SLA or other agreement between the CSP and a customer agency that outlines services provided to meet specific security policies and/or requirements
- documented policies requiring implementation of individual customer agencies' security policy requirements
- documented procedures that describe how to manage, collect, and implement individual customer agencies' security policy requirements
- QA test/audit reports of how individual customer agencies security requirements are met.

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP manages, collects, and maintains requirements for individual customer security policies.	❒	❒	
The CSP accommodates individual customer agencies' security policies and corresponding security controls, as negotiated with the customer.	❒	❒	
Institutional			

The CSP has defined policies or guidance in place to specify that it supports security policies unique to its current customer agencies, as defined in SLAs, MOUs, or other documented agreements.		❒	❒	
The CSP has defined processes in place to specify the services provided to individual customer agencies.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to collect and implement requirements for individual customer security policies.		❒	❒	
The CSP has the appropriate tools in place to provide services according to individual customer security policies.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.MG.11

The CSP accommodates tailored communications processes to meet individual customer requirements.

Clarification

Communications between CSP and subscribers (i.e., trouble reporting, status reporting, security incidents, etc.) should be tailored to meet individual subscriber requirements.

Examples of Evidence Sought

The CSP can describe or demonstrate:
- how it meets customer-specific requirements - whether that is via website access to information, e-mail, reports sent through mail, faxed, self encrypting PGP/GPG archive, telephone call, etc.
- how it meets individual customer agencies' communication policy requirements, including the customer specific requirements, e.g.,
-- required hardware and/or software it uses
-- reports that verify that specific requirements are being met

The CSP can provide:
- examples of tailored communications processes, outputs, or reports
- documented policies regarding customer communications
- documented procedures for managing, collecting, and implementing individual customer agencies' communication policy requirements
- QA test/audit reports of customer-specific communication requirements, processes, and reports

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP custom tailors and manages communications processes to meet the needs of subscribing agencies.	❒	❒	
Institutional			
The CSP has defined policies or guidance in place for managing communications requirements to meet the needs of subscribing agencies.	❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.	❒	❒	
The CSP has the appropriately trained personnel in place to support custom tailoring of communications processes.	❒	❒	
The CSP has the appropriate tools in place to support	❒	❒	

custom tailoring of communications processes.					
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)		❒

Capability #CSP.TO.REP.01

The CSP collects customer service metrics about the government customer instance and reports them to its customers, DHS, and/or OMB as required. Examples of customer service metrics include, but are not limited to, performance within SLA provisions, issue identification, issue resolution, customer satisfaction, and quality of service.

Clarification

The CSP must be able to provide customer service metrics and relevant data to its customers, DHS, and/or OMB.

Team Guidance

This capability is specifically related to customer service metrics. The capability to report network operational metrics is covered in CSP.TO.REP.02.

Examples of Evidence Sought

The CSP can demonstrate:
- the types of metrics that are regularly collected, to whom these metrics are provided, and how they are used
- any tools used to collect metrics
- any type of customer dashboards or interfaces that are used to provide the metrics
- how it meets specific metric requests or needs of each subscribing agency
- what types of metrics are provided to subscribing agencies and how they are provided

The CSP can provide:
- sample metric reports
- documented procedures for collecting and providing metrics
- QA test/audit reports of metrics collection and reporting
- SLAs or other documents that describe customer agency metrics requirements and how those are met by the CSP
- sample metrics relating to customer business needs that are being collected and communicated
- tools or mechanisms such as dashboards, portals, or reports that are used to provide metrics
- procedures on how customer metrics are collected, assigned, monitored, or escalated and how any customer feedback on these metrics is handled
- QA test/audit reports of metrics collection and reporting

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP collects customer service metrics about the government customer instance, and reports them to its customers, DHS, and/or OMB as required.	❒	❒	

Institutional				
The CSP has defined policies or guidance to specify what metrics are collected, the frequency of collection, and to whom they are reported.		❒	❒	
The CSP has defined processes in place to specify how to collect metrics, how often, and to report metrics.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained personnel in place to collect and report metrics.		❒	❒	
There are appropriate tools in place to collect and report metrics.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.REP.02

The CSP collects operational metrics about the government customer instance, and reports them to its customers, DHS, and/or OMB as requested. Examples of operational metrics include, but are not limited to, performance within SLA provisions, network activity data (including normal and peak usage), and improvement to customer security posture.

Clarification

The CSP must be able to provide network metrics and relevant data to the extent necessary to study trending and network behavior under times of attack or penetration.

Team Guidance

Examples of operational metrics include, but are not limited to: Performance within SLA provisions, Network activity data (including normal and peak usage), and improvement to customer security posture.
This capability seeks to determine whether the CSP is collecting a set of network and incident metrics that could be informative in the context of incident response.
For example, it would be helpful to know that the volume of incoming traffic on a particular port was highly unusual at the time of attack. Without a baseline set of metrics, the CSP will not be able to make that assessment easily.
- These metrics might include network performance, quality of service, security, and system operations.
- A "report card" of some or all of these metrics might be reported regularly to management and/or subscribing agencies or components.
- Examples of network metrics might include LAN utilization (throughput in Mbps of designated circuits or parts of circuits), traffic (inbound/outbound) traversing specific ports, traffic (inbound/outbound) by sender, typical users and/or IP addresses of specific network resources (e.g., shared folders) and the details of that use, e-mail volume sent and received, and external connections (e.g., VPN) established and terminated, top malware seen or URLs visited.

This capability focuses on whether there is an open line of communication to customers or subscribing agencies about normal and peak network activity (throughput per link, most common protocol and/or port being used, number of web proxy blocks due to inappropriate content, top websites visited, etc.).
This is not necessarily the type of information that would be shared with a CSP's end users.

Examples of Evidence Sought

The CSP can demonstrate:
- the types of metrics that are regularly collected, to whom these metrics are provided, and how they are used
- any tools used to collect metrics
- any type of customer dashboards or interfaces that are used to provide the metrics
- the types of network activity that are regularly collected and to whom any reports are provided
- any tools used to collect network activity
- any type of customer dashboards or interfaces that are used to provide the reports

The CSP can provide:
- sample metric reports
- documented procedures for collecting and providing metrics
- QA test/audit reports of metrics collection and reporting
- sample reports

- documented procedures for collecting and providing network activity - QA test/audit reports of network and peak activity reporting				
Scoring Criteria				
		Yes	No	Evidence
Technical				
The CSP collects operational metrics about the government customer instance and reports them to its customers, DHS, and/or OMB as required, including, but not limited to Performance within SLA provisions, Network activity data (including normal and peak usage), and improvement to customer security posture.		❒	❒	
Institutional				
The CSP has defined policies or guidance to specify what metrics are collected, the frequency of collection, and to whom they are reported.		❒	❒	
The CSP has defined processes in place to specify how to collect metrics, how often, and to report metrics.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained personnel in place to collect and report metrics.		❒	❒	
There are appropriate tools in place to collect and report metrics.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TO.REP.03

The CSP reports threats, alerts, computer security-related incidents, and suspicious activities that affect a subscribing agency to the subscribing agency.

Clarification

The intent is the CSP keeps each client informed about issues involving the client; so clients have similar levels of information as if they operated their own CSPs.
CSPs must follow FISMA/NIST 800-61 guidelines for reporting.
At a minimum, CSPs must be able to provide data to their customers based on reporting requirements outlined in their SLAs. Each agency negotiates with the CSP to determine its reporting requirements.
If customers have additional SLAs in place with the CSPs for custom services, the CSPs should provide copies of those SLAs that describe the additional services and reporting requirements between the CSP and the agency.
NOTE: The capability does not require the list of specific federal laws or regulations regarding reporting requirements (the agency and CSP will work that out through the SLA or MOU).

Team Guidance

The CSP should be detecting incidents and passing that information to the appropriate entities.

Examples of Evidence Sought

The CSP can demonstrate how it handles these requirements via
- a walkthrough of reporting an incident

The CSP can provide:
- documented policies on reporting threats/incidents and events
- documented procedures, matrix, and workflow for how to report and any associated timeframes
- sample reports showing requirements are met
- copies of the SLAs that describe the additional services and reporting requirements
- QA test/audit reports of threat, event, and incident reporting

CSPs can demonstrate how they meet customer requirements by providing:
- documented policies on reporting threats/incidents and events
- documented procedures, matrix, workflow for how to report and any associated timeframes
- sample reports showing requirements are met
- a business model or policy for collecting and implementing requirements
- copies of the SLAs that describe the additional services and reporting requirements
- QA test/audit reports of threat, event, and incident reporting

Scoring Criteria

	Yes	No	Evidence
Technical			
The CSP reports threats, alerts, and computer security related incidents and suspicious activities to the affected	❒	❒	

agency.				
Institutional				
The CSP has defined policies or guidance in place that specifies reporting of threats, incidents, and events.		❒	❒	
The CSP has defined processes in place to specify how to report threats, incidents, and events.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
The CSP has the appropriately trained, credentialed personnel in place to support reporting of threats, incidents, and events.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒

Capability #CSP.TS.PF.07

The government customer instance supports Federal Video Relay Service (FedVRS) for the Deaf (www.gsa.gov/fedrelay) network connections, including but not limited to devices implementing stateful packet filters. Please refer to http://www.fedvrs.us/supports/technical for FedVRS technical requirements. Agencies may document alternative ways to achieve reasonable accommodation for users of FedVRS.

Clarification

Video Relay Service (VRS): A telecommunications relay service that allows people with hearing or speech disabilities who use sign language to communicate with voice telephone users through video equipment. The video link allows the Interpreter (also known as a Communication Assistant (CA) or Video Interpreter (VI) to view and interpret the party's signed conversation and relay the conversation back and forth with a voice caller. The VRS is an Internet-based service that connects the Deaf consumer to an interpreter via a web cam or videophone. However, the hearing person does not see either the Deaf consumer or the interpreter and needs no special equipment other than a regular telephone.

The Federal Relay Service (FedRelay) is a federal government telecommunications service, which enables federal employees who are deaf, hard-of-hearing, deaf/blind, or have speech disabilities equal communication access. The FedRelay is accessible domestically 24 hours a day, 7 days a week, 365 days a year (including federal holidays).

In the event that the CSP has not yet had the need to implement the FedVRS system, it must have a plan in place to do so as soon as it becomes necessary.

Team Guidance

Although the computer and a webcam can be used to deliver video interpreting, there is a growing trend to use both videophones and televisions for the same purpose. In those cases, the TV and the videophone replace the computer and its peripherals but require broadband connections. Many of the VRS service providers give videophones to deaf consumers at no charge.

Port	Function	Outbound Connection
389	Internet Locator Service (ILS)	TCP
522	User Location Service	TCP
1503	T.120	TCP
1720	H.323	TCP
1731	Audio call control	TCP
Dynamic	H.323 call control	TCP
Dynamic	H.323 streaming	Real-Time Transfer Protocol (RTP) over UDP

Examples of Evidence Sought

The CSP can provide:
-a list of authorized Video Relay Service for the Deaf providers
-documented policy or procedures related to Video Relay Service for the Deaf

Scoring Criteria

		Yes	No	Evidence
Technical				
The government customer instance supports the authorized Video Relay Service for the Deaf.		❒	❒	
Institutional				
The CSP has defined policies or guidance in place that specifies supporting Video Relay Service for the Deaf.		❒	❒	
The CSP has defined processes in place to specify how to support Video Relay Service for the Deaf.		❒	❒	
The CSP has staff practices in place to ensure continued adequate staffing of qualified, trained, credentialed personnel.		❒	❒	
Scoring	Compliant (all Yes boxes above are checked)	❒	Non-compliant (if any No box above is checked)	❒