# Configuration Settings Management (CSM) Capability Data Sheet

## Desired State:

- All hardware and software assets are configured according to policy for all in-scope devices
- All authorized hardware and software with security-related configuration settings have a configuration settings specification that defines the policy for that asset type

## Desired State Data Requirements:

| Data Item | Justification |
|---|---|
| Authorized Hardware Inventory to include for every device:<br>• Security-related settings flag<br>• Configuration settings specification(s) to apply<br>  ○ Name<br>  ○ Version(s)<br>  ○ Requirement Option | • To identify what devices to check and what specifications apply<br>• To identify authorized hardware with security-related settings that do not have existing specifications |
| The associated Value for every device attribute[1] | • To prioritize defects associated with devices. |

[1] This value will initially be defined by the D/A fore the SWAM capability. Once the necessary data becomes available, it will be calculated from the value assigned by the D/A to assets.

| Data Item | Justification |
|---|---|
| Organizational Whitelist to include for every authorized software product:<br>• Security-related settings flag<br>• Configuration settings specification(s)[2] to apply<br>  ○ Name<br>  ○ Version(s)<br>  ○ Requirement Option<br><br>If there are different configuration policies for the same software product depending on device attributes, then for that software product in every software profile include:<br>• Configuration settings specification(s) to apply<br>  ○ Name<br>  ○ Version(s)<br>  ○ Requirement Option | • To identify what devices to check and what specifications apply<br>• To identify authorized software products with security-related settings that do not have existing specifications |

[2] Multiple configuration settings specifications can apply to the same authorized software product.

| Data Item | Justification |
|---|---|
| A configuration settings specification for every authorized hardware or software product that has security-related settings to include:<br>• Version<br>• Date<br>• Specification Manager<br>• Authorization Status<br>• Date first authorized<br>• Date last authorized<br>• Date revoked<br>• Expiration Policy<br>• Applicable asset types/attributes[3]<br>• Specification frequency<br>• Configuration setting check identifier (CCE or equivalent)<br><br>For every configuration setting check include:<br>• Check frequency[4]<br>• Associated system attributes<br>• Required/acceptable values<br>• Compliance definition<br>• Results definition | • To detect unauthorized, non-compliant, or out of date configuration settings<br>• To know who to instruct to fix specific risk conditions found;<br>• To assess each person performance in risk management<br>• To ensure that checks are run at required frequency<br>• To determine compliance with each specific configuration settings check<br>• To document what must be collected and stored for a failed configuration settings check |

## Actual State:

- Security-related configuration settings for every hardware and software asset
- Collection mechanisms and/or processes to detect and record/report the Actual State information

### Actual State Data Requirements:

While not explicitly stated below, all Actual State Data elements must have a date/time associated with each collection instance of that element[5].

[3] Use asset type identifiers that are consistant with those used in HWAM and SWAM. Examples include CPE or SWID.

[4] A check frequency only needs to be defined if it differs from the specification frequency.

[5] Collection often occurs in batches, where the sensors collect from a set of devices at once. As long as a date/time can be provided for the data resulting from that collection to a reasonable precision (i.e., ± 1 hour), that is acceptable.

| Data Item | Justification |
|---|---|
| For every in-scope device:<br>• Name and Version of every configurations settings specification that the device is assessed against<br>  ○ List of checks that device is compliant with for specification<br>  ○ List of checks that device was unable to verify compliance with for specification<br>  ○ Results information for every check failed or found non-compliant for specification<br>  ○ How long each failed check has been present on device | • To identify non-compliant, unauthorized, or out-of-date configuration settings<br>• To identify when checks are not run at desired frequency<br>• To accurately report the defect associated with the non-compliant configuration setting and to aid in mitigation<br>• To determine how long device has been non-compliant with check |

## Defects:

A defect is defined as a discrepancy between the actual hardware or software configuration settings to the specification for each in scope device as defined by the D/A's policy. The following are defects for CSM:

| Defect Type | Why is this considered a risk condition? | Typical Mitigation[6] Option 1: | Typical Mitigation Option 2: |
|---|---|---|---|
| Authorized hardware or software does not have security-related settings flag set | Security-related requirements for an organization are not documented or deployed allowing at-risk devices to have continued access to information and systems | If a determination about security-related settings has already been made, record the result | Otherwise, investigate the product, deterimine if there are security-related settings, and record the result |
| Authorized hardware or software has security-related settings but no specification has been developed | Security-related requirements for an organization are not enforced allowing at-risk devices to have continued access to information and systems | Develop the configuration settings specification for the authorized product | If further analysis has determined that there are not any security-related settings, reset the security-related settings flag to "No" |

[6] Risk acceptance is always an option. In the case of Option 1 and Option 2, the risk conditions and scores do not go away. They remain visible to ensure that the organization understands the impact of their risk acceptance decisions over time and in aggregate.

| Defect Type | Why is this considered a risk condition? | Typical Mitigation[6] Option 1: | Typical Mitigation Option 2: |
|---|---|---|---|
| Authorized hardware or software being checked with expired specification | The risk associated with authorization decisions increases with time. Decisions that were acceptable in the past may now be considered too risky | Reauthorize the configuration settings specification | Otherwise, associate products with appropriate authorized specification |
| Device checked with suspended, revoked, or inappropriate configuration settings specification | Known insecure configuration settings are considered compliant or security-related requirements for an organization are not enforced allowing at-risk devices to have continued access to information and systems | Update authorized hardware or software inventory to reflect correct products or device roles for device | Otherwise, suspend or revoke authorization device |
| Device has unauthorized configuration setting | The device is vulnerable to attack due to misconfiguration of the hardware or installed software | Remediate the configuration setting | Otherwise, either update the specification or suspend/revoke the device's authorization |
| An important data element of the Desired State specification is missing | A key piece of information used to score or assign risk is unknown | If the data element is known, record the information | Otherwise, determine or define the data element and record the information |
| Operational configuration setting information has not been provided or updated within a set timeframe<br><br>(Non-reporting for Configuration Settings) | Ability to monitor vulnerable conditions (e.g., defects) is limited | Work with the sensor/collection managers or process owners to troubleshoot/resolve the problem. | Otherwise, revoke or suspend the device's authorization |

## Appendix A - Definitions

| Term | Definition |
|---|---|
| Authorized Hardware Inventory | List of authorized hardware assets for an organization or subnet. |
| Common Configuration Enumeration (CCE) | The Common Configuration Enumeration, or CCE, assigns unique entries (also called CCEs) to configuration guidance statements and configuration controls to improve workflow by facilitating fast and accurate correlation of configuration issues present in disparate domains.[7] |
| Common Platform Enumeration (CPE) | Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.[8] |
| Configuration Setting | A parameter in software that can be modified to change the behavior of the software asset. |
| Configuration Settings Check Frequency | How often a configuration settings check must be verified on operational assets. |
| Configuration Settings Management (CSM) Capability | The CDM capability that ensures inappropriate configuration settings are identified and reset to an appropriate value to minimize exploitation. |
| Configuration Settings Specification Authorization Status | Current state of a configuration settings specification authorization. States can be 'pending', 'authorized, 'suspended', 'expired', or 'revoked'. Different versions of the same specification are authorized separately. |
| Configuration Settings Specification Frequency | How often a configuration settings specification must be checked on operational assets. |
| Compliance Definition | The logic associated with a configuration settings check that expresses how to determine if an asset is compliant with the policy. |
| Defect | A condition where the Desired State specification and the Actual State do not match in a manner that incurs risk to the organization. |
| Device | IP-addressable asset on the network or a non-addressable component (e.g. removable media) able to interact with the D/A's data and resources. |

[7] http://cce.mitre.org/
[8] http://nvd.nist.gov/cpe.cfm

| **Term** | **Definition** |
|---|---|
| Device Attribute | Device attributes are a way to describe a set of labels, values, and hierarchies associated with dimensions or characteristics of a device. The attributes assigned to a device are used to determine the applicability of a defect check, the result domain of a defect check, or create the appropriate desired state specification for a defect check associated with that device. |
| Expiration Policy | The policy that defines the requirements for when an asset's authorization expires. Examples include a piece of software is authorized for use in the enterprise for 2 years or a configuration settings specification is good for 1 year. |
| Hardware Asset Management (HWAM) Capability | The Continuous Diagnostic and Mitigation (CDM) capability that ensure unauthorized and/or unmanaged hardware is removed from the organization's network, or authorized and assigned for management, before it is exploited, compromising confidentiality, integrity, and/or availability. |
| Requirement Option | A way to denote if multiple versions of a configuration settings specification are "Required" or any 1 of the set is "Allowed" for an authorized hardware or software product. A D/A would use the "Allowed" option to support the existence of two acceptable specifications (e.g., during a transition to a new version or allowing systems to use a more restrictive version). |
| Results Definition | The data or information that must be collected and stored for a failed configuration settings check to support accurate and timely reporting and scoring of the associated defect. This information is also necessary to support mitigation of the failed check/defect. |
| Security-related settings flag | An indicator that the D/A has decided that the authorized hardware or software product has security-related configuration settings that need to be defined per policy. |
| Scoring | The process of calculating the risk points for a defect. Identified defects will be "scored" based on the amount of perceived risk they create. The CDM program will be providing a scoring system that is generic across D/As. Each D/A may adapt this with additional D/A specific information to better prioritize defects for action. |
| Software | For CDM, software includes firmware, basic input/output systems (BIOS), operating systems, applications, services, and malware such as rootkits, trojans, viruses, and worms. |
| Software Asset Management (SWAM) capability | The CDM capability that ensures unauthorized and/or unmanaged software is 1) identified, 2) authorized, and 3) assigned for management, or 4) removed before it can be exploited compromising confidentiality, integrity, and availability. |

| **Term** | **Definition** |
|---|---|
| Software product | The level of abstraction by which software is typically licensed, listed in registries during installation, and executed by users. Software products are roughly equivalent to the software identified by the NIST Common Product Enumeration (CPE) codes, and also by the ISO SWIDs. |
| Software profile | A listing of authorized and blacklisted software for a particular device role. |
| Software identification tag (SWID) | Software ID tags provide authoritative identifying information for installed software or other licensable item.[9] |

[9] ISO/IEC 19770-2: Software identification tag