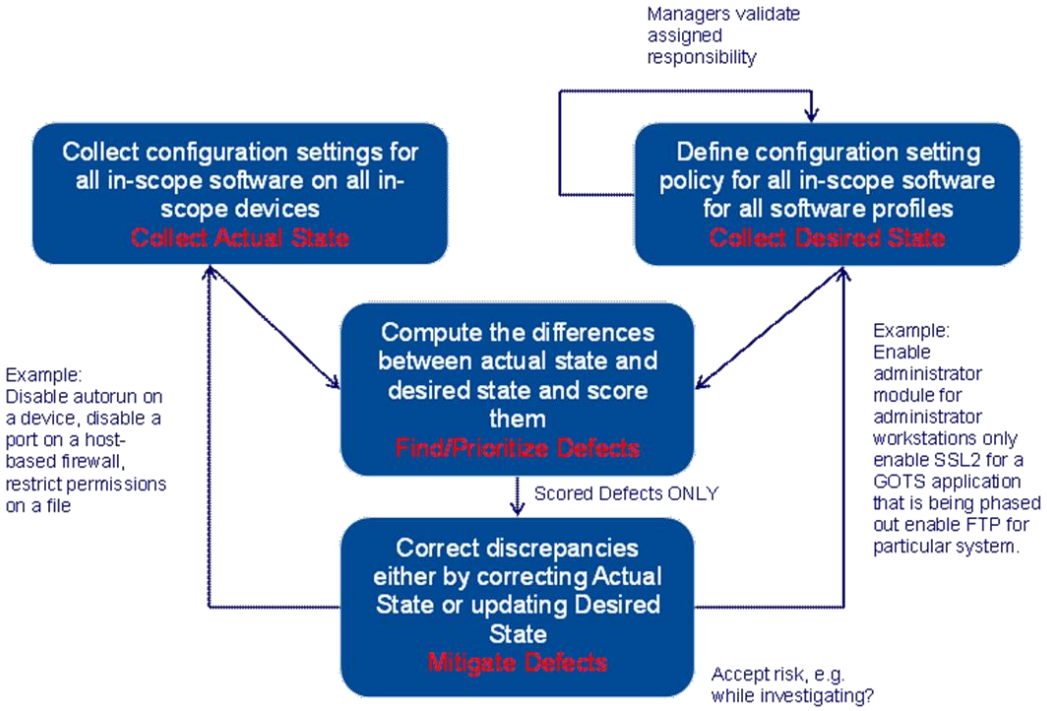
Configuration Settings Management (CSM) Capability Description

Purpose: The Configuration Settings Management (CSM) capability provides a Department or Agency (D/A) visibility into risks associated with improper or non-compliant security-related configuration settings for authorized hardware and software. This capability provides a method to ensure that all in-scope devices are compliant with Common Configuration Enumeration (CCEs) equivalent requirements. This capability is dependent on the existence of both an authorized hardware and authorized software inventory as developed for the Hardware and Software Asset Management Capability.

How does it work? CSM collects information about how authorized hardware and software is configured in the operational environment and compares that with the security-related specifications developed by the D/A. When configuration settings are detected that are less secure than the policy specification, the D/A will either remediate the setting on the device to bring it into complance, remove the software, or properly modify the policy.



How does poor configuration settings management impact the network? Attackers actively target software or hardware with weak or insecure configurations. Once a configuration setting is compromised, it may be used to compromise confidentiality, integrity, and availability of resources or data residing on systems and networks. Because they are exploiting features instead of vulnerabilities, many of these attacks will go undetected because they look like normal activity.

Collect Actual State: Use tools to collect information about the actual configuration setting values for every security-related configuration specification for all in-scope hardware and software for each device on the network. Methods to detect configuration settings (when they were first seen, and when they were last seen) include (but are not limited to)[1]:

- Manual interaction with tools that check hardware configurations
- Active methods (e.g., credentialed scanning software) to collect configuration data from the device remotely
- Active agents on the device to collect and report data on hardware and software configurations

The CDM HWAM and SWAM capabilities will identify the hardware and software assets actually on the network. The CDM CSM process will collect and/or verify the state or values of configuration attributes necessary to determine compliance to configuration policy specifications. Just like the other CDM capabilities, you will need to identify how much of the network and how much of the in-scope software and hardware is being monitored or checked with respect to configuration settings.

Collect Desired State: The primary Desired State specification for CSM is a set of configuration settings for all in scope devices for the D/A[2]. The specification needs to contain the system attributes to check, the required attribute values, and the logic that expresses how to determine if the values constitute a non-compliant state. The other Desired State specification required for CSM is to identify what authorized hardware and software have security-relating settings and to assert whether or not those settings have an existing specification that can be checked. Configuration settings for a particular piece of hardware/software can be the same for every device in the organization, or they can vary by device role or software profile.

CSM will use the HWAM and SWAM Desired State specifications and authorized inventories to ensure that all appropriate in-scope hardware and software are checked for all applicable configuration specifications.

Diagnose (By Finding and Prioritizing Defects): Comparing the values of system attributes on a device with the appropriate configuration specifications will identify non-compliant states that need to be addressed. Verifying that all the appropriate Desired State specifications exist and are updated according to policy will identify any issues with the configuration settings specification processes that can create an additional security risk (e.g., a specification does not exist for a software product that is installed on high value devices across the organization).

---

[1] While non-credentialed scanners or passive listening to traffic from a device can be used in some cases, the information collected is often not specific or accurate enough since most configuration setting checks require access to low-level device/operating system attributes.

[2] The CDM program is only going to define a small set of configuration settings that must be enforced/met by all D/As for a small set of highly targeted or widely used software products. Most of the configuration settings specifications will be specific to the D/A based on their environment and risk tolerance.

See the Defect Type Table for a list of general CSM defects. After these conditions are detected, they will be automatically scored and prioritized (using federal and D/A defined criteria)[3].

Mitigate Defects: The CDM dashboard will generally be organized to show worst problems first. Worst problems should be mitigated first. The following table shows the most important defect types and mitigation options. The full set of Defects and mitigations are documented in the *Configuration Settings Management Datasheet*.

Defect Type	Detection Rule	Mitigation Options
Misconfiguration	Actual State Less Secure than Desired State	• Remediate device configuration OR • Accept Risk OR • Change Desired State Specification (Rare)
Non-reporting	Actual State data unavailable	• Deploy collection capability OR • Restore collection OR • Remove device

[3] Many defects will have a "grace period" built into the scoring function. For CDM, these grace periods are calculated from the time the defect is first identified, not when the desired state specification or actual state changed.

Appendix A - Definitions

Term	Definition
Authorized Hardware Inventory	List of authorized hardware assets for an organization or subnet.
Authorized Software Inventory	Managed whitelisted and blacklisted software for the organization and each device role.
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.[4]
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.[5]
Configuration Setting	A parameter in software that can be modified to change the behavior of the software asset.
Configuration Settings Management (CSM) Capability	The CDM capability that ensures inappropriate configuration settings are identified and reset to an appropriate value to minimize exploitation.
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.
Device Role	An enterprise-wide label for a business or mission function that is associated with D/A-defined information technology assets. The device role is intended allow the refinement of authorization policies related to hardware and software in a manner that ensures that they are appropriately addressing mission needs/risks.
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.

[4] http://cce.mitre.org/

[5] http://nvd.nist.gov/cpe.cfm

Term	**Definition**
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.
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.[6]

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