# I. Capability Description:

The Hardware Asset Management (HWAM) Capability provides organizations visibility into the hardware devices operating on their network(s), so they can manage and defend them in an appropriate manner. It also provides a view of device management responsibility such that prioritized defects can be presented to the assigned party for mitigation actions and risk acceptance decisions. It is important to note that how well the devices are managed is measured in other capability areas. HWAM is a critical component in a mature CDM capability because if a device is not known, it cannot be managed by the CDM program.

HWAM identifies devices that are present on the network and compares them with the desired state inventory to determine if they are authorized.  Some devices are network-addressable, and others are removable and connected to one or more network-addressable devices, such as USB drives.  The means the process for identifying the actual devices will vary, depending on the automated capabilities available and which 'type' of device it is.

Devices in Scope

- Computers (Portable, Mobile, Desktop, etc.)
- Networking devices and appliances
- Storage Area Network Appliances
- Communications devices
- Input/Output devices (if addressable or shared)
- Both physical and virtual devices
- USB and other removable devices (with memory/storage)

HWAM makes sure these devices are:

- Identified
- Authorized
- Managed

The CDM process (as adapted for your D/A) will provide insight into what percentage of the actual hardware assets are included in the desired state, and of those, how many of them identify an assigned device manager.

# II. Initialization of Desired State Inventory (DSI):

The initial DSI can be derived from multiple different sources. As an example, the D/A may maintain an offline or an online listing of all known devices in property management databases. Authentication services such as Active Directory, Lightweight Active Directory Protocol (LDAP) listings, and RADIUS Servers can be used to identify active devices. Existing network detection and management tools can also be good sources to help build an initial DSI.

Use the existing databases or property management systems to determine the enterprise unique device identifier for each device, and capture all the existing information about that device that is known and required for the DSI. If no unique identifier had been used before one needs to be established. It will be considered the primary key used to tie the other attributes back to the device.

The following information will need to be captured for each entry in the DSI to compare with the actual state data:

1. Data necessary to accurately and uniquely identify the device
   - To be able to validate that the device on the network is the device authorized
   - Can be tied to a combination of things (example: IP and MAC address)
2. Expected CPE, when available, (vendor, product, version, release level) or equivalent
   - To help determine the type of device
   - To ensure all appropriate defects for a device are defined, run, and reported
3. Device Manager
   - Person or organization (group) who is responsible for managing the hardware asset
   - To identify who will fix specific risk conditions
   - To assess the responsible individuals' risk management performance
4. Data necessary to physically locate hardware assets (such as a physical location attribute)
   - So managers can find the device to fix it
   - To identify mobile devices so that extra controls can be assigned
5. Data necessary to physically identify the asset (such as property number or serial number)
   - To be able to independently validate that the remotely found device is actually this device, and not an imposter
6. Expected status of the device (e.g, authorized, expired, pending approval) to include: Date first authorized, Date of most recent authorization, Date authorization revoked
   - To determine which devices in the authorized hardware inventory are not likely to be found in actual state inventory
   - To help quantify risk and trigger appropriate prioritized response to defects
7. The period of time the asset is authorized
   - To ensure reauthorization occurs as required and applicable
   - This should consider sunset dates or termination dates of service/maintenance agreements

This data will provide what is minimally needed to support the HWAM capability, however the D/A can further define local attributes for each devices as necessary or desired.

A complete and accurate desired state is the cornerstone to the CDM processes and thus the role of the Desired State Manager (DSM) is critically important. The desired state managers ensure that data specifying the desired state of the relevant capability (in this case HWAM) is entered into CDM correctly. The DSM for the CDM Target Network has a special role to resolve any ambiguity about which information system (if any) has unauthorized or unmanaged devices in its boundary.

The D/A should identify a candidate or group prior to implementation of the CMaaS Solution. They may need to augment this role with additional personnel upon implementation, or during major system changes which will require large scale changes to the DSI. The role should be in the information assurance function or enterprise security group of the organization, and will require working closely with the change management process, property management, and the device mangers to ensure that the processes outlined below are executed. They are ultimately responsible for ensuring that each authorized device is entered into the DSI and assigned a manager. They are also responsible for validating and ensuring the integrity of what is in the DSI.

## a. Enter legacy data into the Desired State Inventory (DSI)

When using legacy information, it is important to be able to automate its import into the DSI instead of manually entering it. This will save time and lower the likelihood of inaccurate or incomplete information. There may be some additional information that needs to be added to this legacy data after it is ingested from a source. For example, a D/A could start with their current configuration management database or hardware inventory to list the devices that are authorized and/or being managed on the network by some agent. They could then use the property management database to add the additional information about physical location and serial number to the record for that device.

## b. Enter data from automated tools into the Desired State Inventory (DSI)

With large networks or at sites that may not have mature inventory capabilities, it may be easier to start with the output of sensors to create an inventory of deployed, connected, or communicating devices. The D/A can use the same sensors designed to collect actual state data for HWAM or they can use sensors they already have deployed to create an initial DSI prior to CDM implementation. The hardest part with using automated tools to create the initial DSI is that sensors are not able to collect all the ancillary information that is required. They may also miss remotely deployed devices with variable connection frequencies. The tools must be able to create an identifier or set of identifiers for a device to enable reconciliation with the identifier in the legacy databases.

When using automated methods to support the discovery of assets when building out the desired state inventory, a number of methods exist:

### Active Scanners

Active scanners are agentless and probe preconfigured network ranges for devices. Once devices are identified, the scanners will attempt to determine the type, and login with preconfigured credentials. This is useful for detection of devices that are powered on and connected to the network at the time of the scan. These scanners also perform analysis of configuration and patch compliance to support some of the other capability areas.

There are several key considerations when using an existing active scanner to help populate the DSI. It is important to note that existing sensors are already serving a specific purpose within the organization, and reconfiguration of them to support HWAM initialization in accordance with these considerations may not be possible.

1. Configure active scanner to be able to reach all of the devices
    - This should include all network ranges and subnets that can service a device.
    - In D/As with multiple sites or a distributed network architecture, scan nodes can be deployed that report back to a master scan interface. This is an important consideration in reducing the network load over links between sites.
    - Management network scans will need separate CDM infrastructure from production networks to ensure the networks are not bridged by the active scanner.
2. Configure credentials in the active scanner

- While the scanner will do its best to guess what the device is without credentials, with credentials it can authenticate and pull down a wealth of information about the device for entry into the DSI.
- With proper credentials the active scanner can identify every USB device that has been connected to the host (more on this below). When capturing USB devices using this method, the desired state manager should review each discovered instance to determine whether or not the device is in fact authorized.
- Credentials should be run under service accounts and not individual users. Management of credentials is part of other CDM capability areas.

3. Trouble shoot issues
   - If a known subnet cannot be reached changes may need to be made to firewall rules or other network based configurations.

Once the active scanner has returned host information, those hosts should be added to the DSI if authorized and should have a device manager assigned. New devices need to have new DSI information associated with them that is not available from the scanner results themselves.

## Passive Scanners

Passive scanners build profiles for each of the hosts that are communicating over the network traffic that they are monitoring. Placement and proper configuration of the network interface are the most important considerations of deploying a passive sensor. It will scan all traffic that it is capable of seeing and keep record of the hosts, ports, and protocols being used on that network traffic. This passive approach is an advantage to active scanners in that active scans only scan what they are configured to target. A passive scanner will detect a device that is not targeted by an active scanner if it is configured on the appropriate network segment. This is especially beneficial when scanning the segments of the network assigned to remote devices, as they may not always be connected during the active scans.

SPAN ports are ideal in most cases as they can be configured to see all network traffic without interfering or bridging VLANs. Passive listeners could be deployed to D/A network choke points such as the main switch for each location.

Once the passive scanner has created host profiles, those hosts should be added to the DSI if not already present. New devices need to have the remaining DSI information associated with them including the authorization status and device manager.

## Endpoint Suites

There are two ways that agent based endpoint solutions can be used to support the initialization of a DSI. First, most agents have a certificate or some other mechanism that allows them to uniquely identify the device on which they are deployed. This identifier can be used by other processes (e.g., active scanners can collect the agent ID) to uniquely identify the device.

Second, agent based endpoint solutions often leverage Active Directory and Lightweight Active Directory Protocol (LDAP) listings to identify devices. If new hosts are discovered and they are candidates to receive the agent, the tool can often be configured to automatically deploy it. The management interfaces for these endpoint solutions can report on these new devices and the organization can update the initial DSI. New devices need to have the remaining DSI information associated with them.

### Special Considerations for USB Devices

USB devices can present some challenges in that they are not always connected and they are not directly scan-able from the network. While all should indicate a Vendor ID and Product ID for driver purposes, not all will present a serial number to uniquely identify them. This information is stored in the system registry and is retrievable by credentialed active scans, even if the device has been disconnected. Endpoints suites can also capture USB devices that are connected to the monitored hosts. The D/A should do their best to only allow certain brands of USB devices that do present serial numbers so that they can uniquely be tracked. If an approved USB device does not have an associated serial number, the D/A will need to do their best to try to uniquely identify them via other means. This can be done by correlating the Vendor and Product IDs of each USB device with other known information, such as host that the device was connected to and/or the user who connected it.

## III. Management of Desired State Inventory:

Once the DSI is initialized and the HWAM capability is operational, management of the DSI must be timely, accurate, and cover all in-scope devices, otherwise defects will continue to be identified in CDM. The following sections detail potential ways to minimize the existence of systemic defects related to these issues.

### a. Timeliness

If devices are deployed on the network before they are entered into the DSI there will be systemic defects for unauthorized devices. If the manual processes that update authorization decisions, list device managers, or enter other relevant information in the DSI are inefficient, then there will be systemic defects for expired authorizations and unmanaged devices. There are steps that can be taken to avoid these potential issues:

- **DSI inventory update process (*adding a new device)*:** New devices that are added to the network should be captured in the DSI via the organization's change management process before they are added to the network. If the change management documentation process is too slow, the D/A could update the HWAM DSI when a new device is being considered for authorization with all the relevant information and a status of "pending". Then once the change management process approves the authorization all that needs to be done is to change the status and enter the date. The D/A could make it part of the approval process to ensure that all the required information is already in the DSI.
- **DSI inventory update process (*removing a device)*:** The D/A may need to augment the decommissioning/sunsetting process to remove devices from the DSI as they are removed from the D/A's operational environment.
- **Major system changes:** A major system change such as a reconfiguration of the network or the addition of an enclave may warrant significant changes to the DSI that could have a ripple effect on the HWAM capability. The change management processes need to be followed regardless of the number of devices, and the necessary information needs to be captured before new devices are deployed. Ideally a lab or staging environment can be used to collect and validate information provided via the change management processes before going operational. This would minimize the potential number of defects introduced by the major change. In instances

where large volumes of devices are added or removed from the DSI, the D/A should consider using custom scripts/batch jobs to update device status in the DSI versus manual update of status in order to reduce overall time to update device status in the overall D/A change management process.

### b. Completeness/Coverage

As an essential foundation of the CDM program, an organization needs to identify and actively maintain a complete HWAM DSI. Often a single organization is made up of multiple different sub-organizations, and each sub-organization may follow their own process to enter devices into their desired state inventory. The overall organization must be able to maintain or access a complete DSI view that includes timely information for all the sub-organizations. In order to ensure the maintenance of a complete DSI view, the D/A should consider the following processes and tips:

- **Sub-organization DSI inclusion in CDM:** In a federated model each sub-organization may employ different change management processes and may maintain their own DSI. All required desired state data elements will need to be updated in CDM in real-time. In those federated environment instances, it will be necessary for DSI information to be replicated or made accessible to CDM. While individual organization can maintain their own local instances of their DSI, all changes in their DSI (which is considered the authoritative source) must be replicated or accessible to CDM in order to ensure an accurate comparison to actual state. This may require distributed desired state managers to properly manage the federated processes and ensure the updated information is reflected in the CDM desired state.

### c. Accuracy

Recognizing the transient nature of many hardware devices and determining how to handle those circumstances proves to be one of the harder integration issues for the HWAM capability. This is because the number of transient devices, and how often they are expected to be connected to the network is mostly influenced by the local environment and policies. For example, D/A employee laptops will constantly be added and removed from the actual state environment, and this will happen at different frequencies for different D/A environments. As such, the D/A needs to develop a process to handle their typical circumstances for non-static devices like laptops to prevent the incorrect identification of “Authorized device not present” defects. For example, the D/A should consider adding a local attribute for transience in the DSI such that a non-reporting defect for the device (device is in the desired state but not actual state) does not get scored for some organized defined, reasonable period of time. The D/A could also create a process for changing the status of an authorization to “suspended” when people are detailed or traveling and they are not expected to log in with their laptop for an extended period of time.

## IV. Question and Answer:

1. Why does HWAM require a desired state inventory? Why does it need to be automated?
    a. The desired state provides the baseline to analyze the actual state against to discover defects. A real time assessment will capture the actual state of the hardware devices on

the network however the results need to be compared to a desired state in order to identify new devices, or devices that are not authorized and managed. Automating this process is important because manual reconciliation could take weeks or longer with a high probability of errors.

2. How does the desired state inventory relate to what devices are authorized?
    a. The DSI is the authoritative listing from the internal D/A processes of devices that have been authorized to connect to the network.
3. What is the Desired State Manger
    a. The desired state manager ensures that data specifying the desired state of the relevant capability (in this case HWAM) is entered into the CDM system's desired state data, and is available to guide the actual state collection sub-system.
4. Is the Desired State manager better thought of as a person or a group in my organization?
    a. It depends on the size of the organization, but a group is preferred to avoid a single point of failure and enhance timeliness and accuracy of DSI updates.
5. What is a Device Manager?
    a. Device managers are (for HWAM) responsible for adding/removing devices from the network, and for the hardware configuration of each device (adding and removing hardware components).Note that a device manager can actually be a group not just an individual.
6. Is a Device Manger different from a device owner or user?
    a. With proper segregation of duties employed, owners and users rarely have the ability to make changes to devices or install/uninstall them from the network. It is the manager who can do these things and the manager who is held accountable for defects associated with their devices.
7. Why does HWAM require each device to have a manager?
    a. In order to have a point of contact for when defects are detected on the device and to hold someone responsible for defects.
    b. Unmanaged devices tend to be more vulnerable than managed devices. Assigning a manager and holding them accountable for mitigating risk conditions for devices they manage mitigates this risk.
8. Is the device manager better thought of as a person or a group in my organization?
    a. It depends on the size of the organization, but a group is preferred to avoid a single point of failure and enhance response time to defects.
9. What are the advantages of passive listening to initialize my DSI?
    a. Passive listening may discover devices that are not otherwise detected by an active scan for various reasons. This can include that the active scanner is not configured to scan the range of IP addresses the device resides in, or that the device is offline when the active scan is run.
10. Why does passive listening need to be supplemented by active methods?
    a. Active methods log into devices and record more detailed information then possible by passive scanning. This provides a wealth of information to support the HWAM capability that is not otherwise available via passive scanning.
11. Should we wait until we have a perfect desired state inventory to start HWAM?
    a. No, executing HWAM operations will help to refine the desired state. For typical IT environments that are ever changing, an accurate desired state inventory is unlikely without running the HWAM tools to continually validate the DSI.

12. Can we start without a desired state inventory?
    a. No, an initial desired state inventory must be established to have something to compare to the actual state.
13. Is the process of getting an initial desired state inventory much different from the normal process of running HWAM?
    a. The main difference is the number of devices being added and updated in the DSI is much larger during initial definition than routine processing. Once the initial desired state is built, the normal process of running HWAM will help to refine it.
14. What existing sources of information does my organization have to get started?
    a. Legacy lists and databases that contain information about devices, locations, ownership, serial numbers, authorizations, and other information used to manage those assets.
    b. Directory services such as LDAP, AD, RADIUS and others
    c. Network diagrams
    d. Purchase orders
    e. Path and Configuration management services
15. Why are device identifiers critical to HWAM operations?
    a. There needs to be a way to uniquely record and track each device over time. Duplicate devices or devices whose identifiers cannot be reconciled with the DSI cannot be appropriately managed because the actual device may not be unauthorized or it cannot be located to be removed from the system.
16. How will virtual machines be handled in HWAM?
    a. Virtual machines are included in the HWAM inventory just as any other device. Each needs to be uniquely identified, authorized, and manager. It is important that the hypervisor itself is also included in the inventory. The hypervisor manager may be different from the managers of the virtual machines.