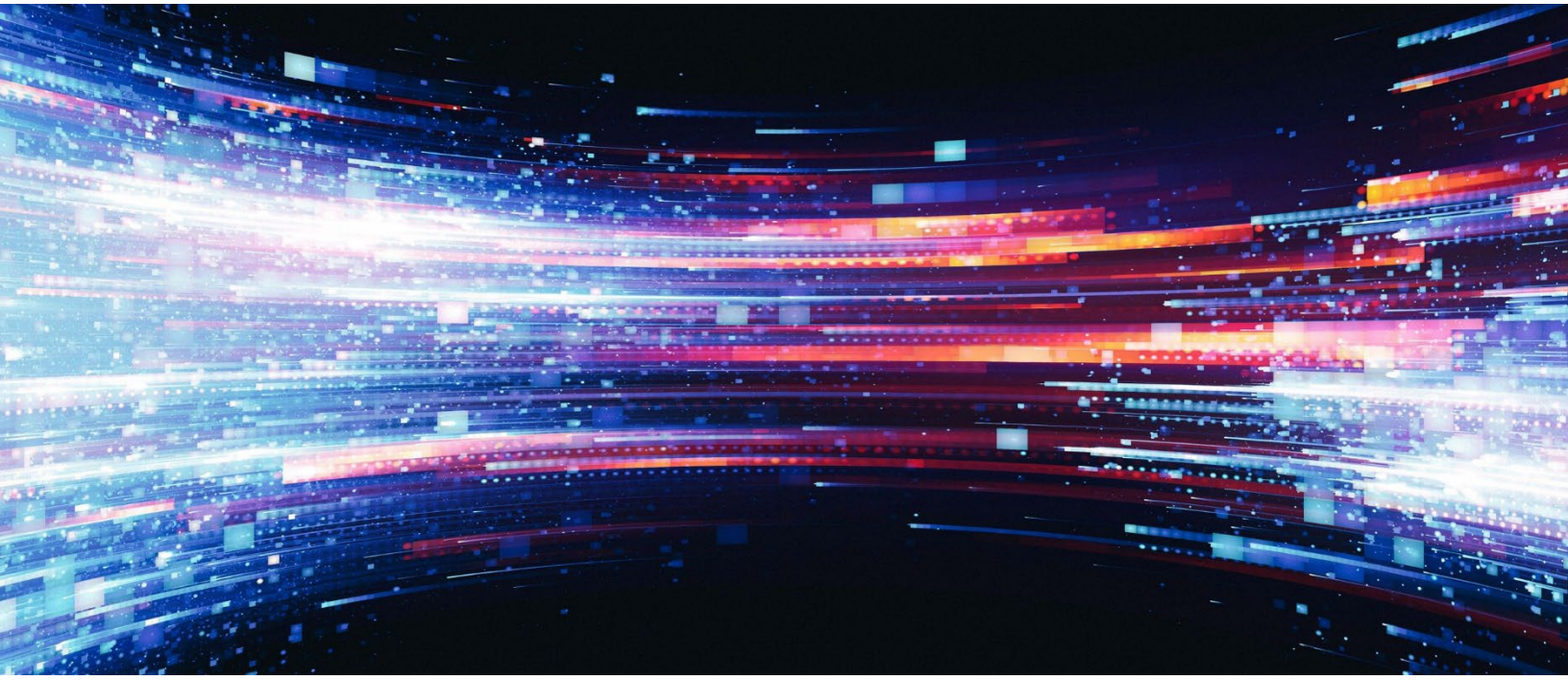
TLP:CLEAR



Continuous Diagnostics and Mitigation (CDM) Program Architecture

CDM Data Model Document

Version 5.0.1

Publication: October 2024
Cybersecurity and Infrastructure Security Agency

TLP:CLEAR

Revision Summary

Below is a table of changes that describes specific changes to this document since the last version, including references to the changed sections/paragraphs. For more details on the changes included in the most recent revision, please refer to Appendix C.

Version	Document Date	Revised by	Description of Change
0.1	August 2016	APL	Initial Draft – Released to DHS for additional content.
0.6	August 2016	CDM PMO	Added additional guidance and content for PMO review.
0.7	August 2016	CDM PMO	Made changes after JHU and PMO discussions/comments.
0.8	September 2016	CDM PMO	Made additional changes after JHU and PMO discussions on 9/8.
1.0	September 2016	CDM PMO	Prepared for Release, updated interrogation specs and Conceptual Model included.
1.1	November 2016	CDM PMO	Incorporated feedback and edits from stakeholders, released.
2.0	April 2017	CDM PMO/APL	Added Phase 2 entities, attributes. Error corrections. Updated key sections to account for CDM Phase 2. Revised Phase 1 items.
2.1	June 2017	CDM PMO/APL	Feedback solicited from CDM stakeholders, incorporated into model. Clarified Interrogation Specifications for Phase 2 to be more consistent with FISMA metrics. Added additional content to key terms and guidance sections.
3.0	February 2018	CDM PMO/APL	Added new entities to support Incident Response Reporting, POAMs, Physical Locations (Facilities). Edited some existing entities to normalize data (e.g., Device Responsibility for device managers, providers, operators). Added Tool/Sensor metadata. Added AWARE data elements.
3.1	May 2018	CDM PMO/APL	Feedback solicited from CDM stakeholders, incorporated into model. Updated/added interrogation specifications for Phase 3 while updating previous Phase 1/2 to be in alignment with LDM edits.
3.5	July 2018	CDM PMO/APL	Derived data entities and attributes to in order to ensure alignment of the program's data requirements to the mission needs regarding Ongoing Assessment for Phase 1 (OAS). Updated/Added additional key definitions for Phase 2 terms. AWARE derived sub-scoring and aggregate scoring attributes. Added requested Data Attributes: Device Make/Model.

Version	Document Date	Revised by	Description of Change
			Changed ConfigurationSettingsOnNetwork to MisconfigurationOnNetwork. Added additional entity/attributes: DeviceScan, OASControlMeasurement, SecurityControl, ManagedAppOnNetwork.
3.7	August 2019	CDM PMO/APL	Identified changes associated with NAC, mobile, and CyHy updates. Updated design of ports, protocols, and services entity. Introduced threat intelligence entity. Added specialization/generalization to LDM design. Added more detailed "release notes" section (Appendix D).
3.8	January 2020	APL	Added and modified entities/attributes for: BOUND-E Certificate. Management capabilities, FISMA metric changes based on FISMA FY19, Policy Decision Point (PDP) architectural changes.
3.8.1	March 2020	CDM PMO	Finalized Draft (3.8.1) based upon feedback/comments. Published.
4.0	March 2022	APL	Added attributes and interrogation specifications supporting Data Quality Assessments and Data Effectiveness Assessments. Clarified Required data, Conditionally Required data, and Recommended data. Updated to FY2021 FISMA metrics.
4.1	August 2022	CDM PMO/APL	Updates and changes to System/System Boundary around authorization decisions, system names, HVA flags and subsystems. Updates to Vulnerabilities to capture more details that are available through tools and sensors.
4.1.1	October 2023	CDM PMO	Establishes a public-release version, which omits sensitive content that is specific to individual agency deployments and includes editorial refinements throughout.
5.0	October 2024	CDM PMO/APL	Updates to align with latest FY23 FISMA Metrics, which included major changes to metrics and query considerations.
5.0.1	October 2024	CDM PMO	Establishes a public-release version, which omits sensitive content that is specific to individual agency deployments and includes editorial refinements throughout.

Contents

1 INTRODUCTION

1.1 Purpose

The Cybersecurity and Infrastructure Security Agency (CISA) Continuous Diagnostics and Mitigation (CDM) program operates on the premise of a common architecture that relies on capabilities provided by commercial-off-the-shelf (COTS) tools and sensors. In keeping with that approach, the CDM program has identified a need to overlay similar data requirements on the solution to ensure that common program objectives are met and to provide proper clarity to integration needs. This document outlines fundamental data elements that the program expects each CDM solution deployed at agencies to incorporate.

It identifies the minimum set of data requirements needed to leverage the CDM solution to accomplish the program's objectives: to reduce agency threat surface, increase visibility into the federal cybersecurity posture, improve federal cybersecurity response capabilities, and streamline Federal Information Security Modernization Act (FISMA) reporting.

Additionally, this document delivers guidance regarding the data that CDM solutions at agencies must collect, with an explicit understanding that the system will be required to produce datasets from specific interrogations of the CDM data. It is expected that agencies and CDM integrators will enrich these datasets with other relevant Information Security Continuous Monitoring (ISCM) data that fulfill their agency-specific needs.

CDM integrators should use this document to drive development and refinement of the implementation of the holistic solution, incorporating these data requirements into the operational rhythm of security tools and sensors. This will provide data to facilitate the execution of the CDM program's mission objectives.

1.2 Scope

The data requirements discussed in this document represent the minimum required dataset to accomplish the critical objectives of CDM, as foreseen by the CDM Program Management Office (PMO), across different solutions, while achieving consistent results. Currently, the scope is focused on data requirements related to the technical capabilities found under "Asset Management" (formerly Phase 1), "Identity & Access Management" (formerly Phase 2), and "Network Security Management" (formerly Phase 3). Detailed operational capabilities are found under the following decomposed tool functionalities:

- Asset Management (inclusive of mobile devices) (formerly known as Phase 1)
    - Hardware Asset Management (HWAM)
    - Software Asset Management (SWAM)
        - Application Execution Control (AEC)
    - Configuration Settings Management (CSM)
    - Vulnerability Management (VUL)
        - Enterprise Mobility Management (EMM) Mobile Threat Defense
- Identity & Access Management [formerly known as Phase 2]
    - Manage Trust in People Granted Access (TRUST)
    - Manage Security Related Behavior (BEHAVE)
    - Manage Credentials and Authentication (CRED)
    - Manage Account Access (PRIV)

- Network Security Management [formerly known as Phase 3]
    - Manage Events (MNGEVT)
        - Incident Response
        - Ongoing Assessment (supporting Asset Management data only)
    - Operate, Manage, and Improve (OMI)
        - System and Information Integrity (supporting incident response)
    - BOUND-E
        - Certificate Management (non-person entities only)
    - BOUND-F to Manage Network Filters and Boundary Controls
        - Network Access Protection

It is anticipated that additional content will be incorporated in subsequent iterations of this artifact as new technical capabilities are added to the CDM program operational baseline.

CDM's conceptual architecture and associated security frameworks, which convey program needs through CDM Technical Capabilities, Volume 1 and Volume 2, are also used to derive necessary data requirements that are reflected in this model. Specifically in scope are the definitions of the logical groupings of key cybersecurity information in the following constructs:

- Master Device Records (MDRs)
- Master User Records (MURs)
- Master Incident Records (MIRs)
- FISMA and Organizational Unit (OU) Containers

The CDM datasets included are decomposed into entities and attributes within the interrogation specifications section. They provide strong traceability for data requirements laid out for agencies (i.e., "must have" data). Another core principle of the program that influences the common schema is the system's capability of "standardized scoring" through an algorithm that produces a quantitative measurement to facilitate prioritization and enumeration of risk-relevant states across the .gov enterprise. To support this effort, the CDM Data Model includes data requirements for a standardized federal risk score, the Agency-Wide Adaptive Risk Enumeration (AWARE) methodology.[1] AWARE requires that specific data be collected or calculated to successfully implement the algorithm, and the data model acquiesces to these data requirements.

Finally, it is important to note that physical schemas and as-built designs are largely out of scope of this document. It is the CDM dashboard developer's responsibility to develop and align the physical data schema (i.e., CDM "data target") to the intent of this logical model through the requirements and solution engineering activities within the program.[2]

[1] For more information of the AWARE algorithm, refer to Appendix A.
[2] For more information on how to use and interpret this document, refer to the guidance within Section 2.

1.3 Audience

This document's intended audience is assumed to have a working knowledge of the CDM program. The audience primarily includes CISA Cybersecurity Division staff,[3] CDM participating agencies' staff, CDM Dynamic and Evolving Federal Network Defense (DEFEND) integrators, and the CDM dashboard provider.

1.4 Context for the Model Derivation Process

CDM is:

- **A process** within an agency's ISCM strategy, as originally mandated in the Office of Management and Budget (OMB) Memorandum (M) 14-03[4] (now superseded by OMB M-19-02[5]), to strengthen the security posture of the federal civilian networks by enabling operators to continuously search for flaws, collect results, triage and analyze results, fix the worst flaws first, and report progress.
- **A program** that provides continuous monitoring, diagnosis, and mitigation capabilities by centrally coordinating the procurement, installation, operation, and maintenance of diagnostic sensors (tools) and dashboards deployed to participating agencies and a federal-level cyber diagnostic dashboard maintained at the Department of Homeland Security (DHS).
- **A system** consisting of multiple instantiations of tools and dashboards that work together to enable the CDM process.

The CDM Data Model is a **common schema** of data elements and attributes based on recommendations and requirements conveyed in the CDM architecture. This common schema is authoritative in developing the data requirements for the CDM program and represents the to-be state of the data both within (as ingested and stored) and outside of (as queried and reported) Layer C of the CDM architecture (see Figure 1-1). With regard to data queried or reported, a core set of **data interrogation actions** were captured based on input from various sources that were solicited in developing this artifact, including the CDM Technical Capabilities,[6] Volume 1 and Volume 2 and the Chief Information Officer (CIO) Federal Information Security Modernization Act (FISMA) Metrics. In the case of the FISMA metrics, this document focused on information that could be specifically tied to CDM asset, identity and access, network security, and data management capabilities (formerly Phase 1, 2, 3, and 4 security capabilities, respectively). Each data interrogation action represents key fundamental mechanisms of the CDM solution, satisfying mission requirements for summary reporting, scoring, and/or defect prioritization.

The cohesive philosophy of normalizing metrics and key machine information is required to facilitate a standard CDM dashboard platform across all agencies (representing the aforementioned "Layer C "of the architecture as shown below). As one of the central aspects of CDM, the dashboard serves as the primary means by which the CDM Logical Data Model (LDM) can be physically implemented. Through the development and deployment of the CDM agency dashboard, a physical schema ("as-built" by the dashboard developer), which is aligned to the intent and requirements of the LDM, provides the realized vision of a normalized CDM dataset (i.e., common schema).

---

[3] Specifically, this includes CISA Cybersecurity Division staff who support operationalization or oversight of the CDM program.

[4] "Enhancing the Security of Federal Information and Information Systems," M-14-03, November 18, 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.

[5] "Management Requirements," M-19-02, October 25, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/10/M-19-02.pdf.

[6] These documents describe the requirements for the CDM program that are consistent with the overarching goal of enabling U.S. government entities to assess and improve the security posture of an agency's information systems. These requirements will be used for the CDM solicitations called Dynamically Evolving Federal Enterprise Network Defense (DEFEND) program as well as the Schedule 70 CDM-SIN Approved Product List (APL).

Leveraging this architecture, the federal dashboard collates the summary information and risk scores produced by the multiple agency dashboards to enable standardized, comprehensive cyber visibility into the entire civilian government enterprise. This CDM dashboard hierarchy represents the operationalization of the data architecture within this artifact. It allows for the common schema to be enumerated and queried at each agency, with the results providing stronger cybersecurity measurements across the agencies.

The CDM Data Model entities and attributes[7] described in this document were iteratively derived using the following process:

1. Enumerate all relevant data interrogation actions that have traceability to one or more of the key reference materials (see Appendix A).
2. Generate specifications for each data interrogation action identified in a fully defined, common standard format (e.g., SQL[8]).
3. Derive data entities and attributes to meet the interrogation specifications (i.e., a common schema for CDM technical capabilities).
4. Develop a data dictionary that clearly describes the required entities and attributes to provide a consistent understanding for the audience.

[7] Refer to Section 2 for more information regarding Unified Modeling Language (UML) entity relationship (ER) diagraming, entities, and attributes.

[8] Structured Query Language (SQL) is a special purpose language for accessing data in databases. In this case, it is a well-known formal language that can be used to specify the interaction of the data interrogation action with the object data within the CDM system.

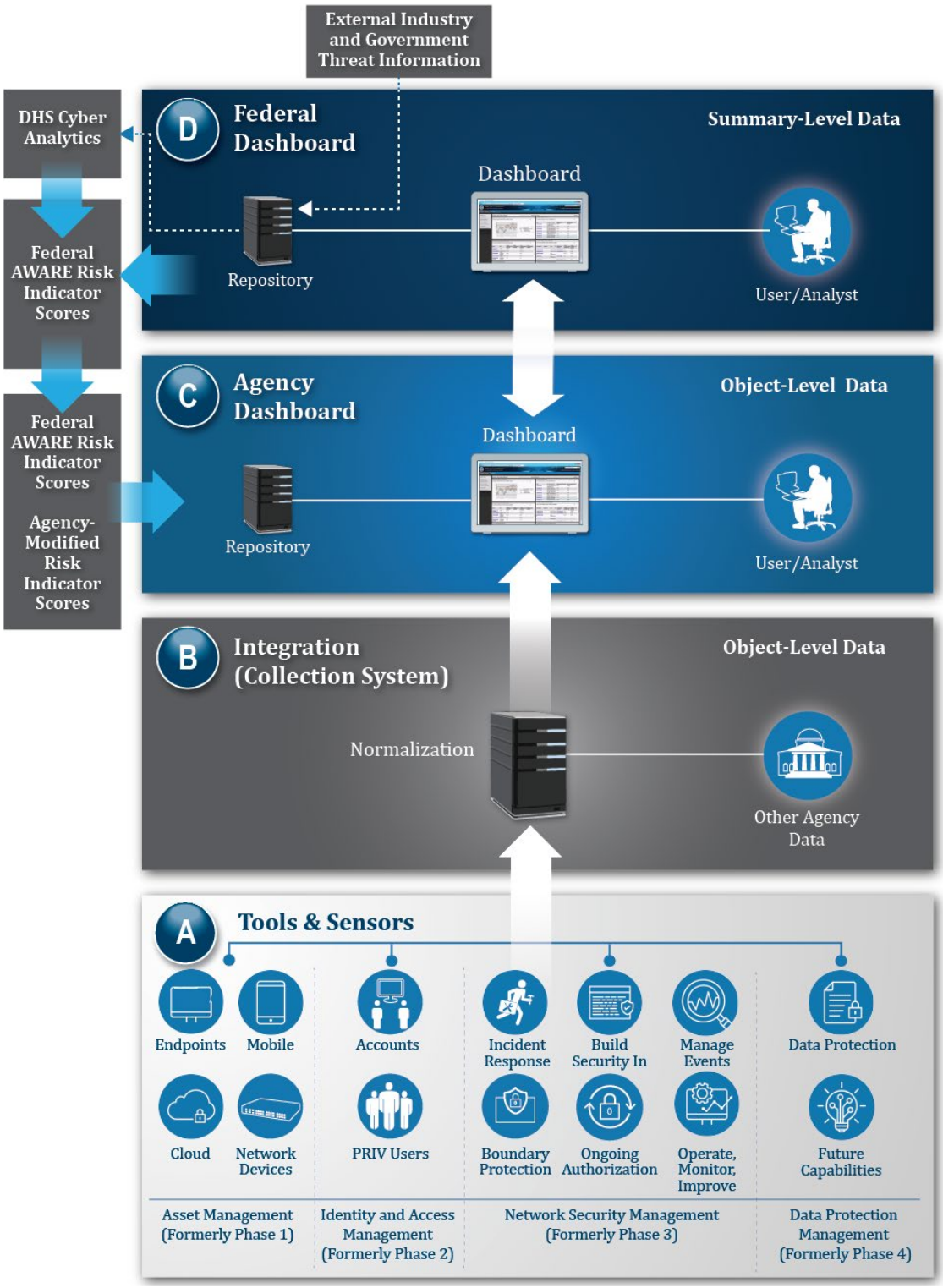


Figure 1-1: CDM "ABCD" diagram showing the distinct layers of the architecture. The CDM Data Model focuses on the interface between layers B and C, clarifying the common datasets to be provided by B aligned to expected inputs in C.

2 CDM GUIDANCE IN INTERPRETING THE DATA MODEL

This section provides guidance on practices and principles that are necessary to support the consistent adoption and use of the CDM Data Model and its related artifacts (e.g., the LDM itself). The guidance relevant to the CDM program will change over time as the scope of the program expands to provide more capability and coverage.

The LDM is compatible with previous conventions that outline the data modeling process (e.g., DoDAF DIV-2). Some of the fundamental underpinnings of a logical model are that it "allows analysis of an architecture's data definition aspect, without consideration of implementation-specific or product-specific issues," and that it is intended "to provide a common dictionary of data definitions to consistently express models wherever logical-level data elements are included in the descriptions."[9]

Appropriately, the program expects these documents (CDM LDM and Data Model Document) to be leveraged within two primary use cases:

1. As an authoritative data architecture document that clarifies what the data requirements are for the common schema, implemented to the intent of the government by the dashboard developer through a physical schema (i.e., dashboard data target) and subsequently by the DEFEND integrators.
2. As a general guidance document to clarify the authoritative operational definitions of key terms, attributes, concepts, required correlation between datasets for implementation, etc.

Note: This CDM Data Model Document is part of a collective set of artifacts that are intended to be used together to achieve the goals outlined in Section 1 of this document. Specifically, this document should be reviewed in conjunction with **CDM_LDM_[VerNO].png**, which provides the LDM itself in a visually based Unified Modeling Language (UML)-entity relationship (ER) structure.

2.1 CDM Datasets

CDM datasets may be categorized as follows:

- CDM Effectiveness Measures: Datasets that are designed to assist analysts in assessing the operating effectiveness or overall health of the CDM subsystems at agencies. Examples include CSM and VUL scan timeliness or configurations during scan execution.
- Inventory Metadata: Datasets that characterize CDM container inventories. Examples include inventories of installed software, devices, and privileged users per system boundary and per organizational unit.
- CDM-Defined Defect Checks: Datasets that periodically compare an object's actual state (as derived from sensors) with the desired security state (as established by policy). Examples include unauthorized device, unauthorized software, and vulnerable devices.
- Ongoing Assessment and Monitoring: Datasets that are directly traceable to information security frameworks, such as the Risk Management Framework (RMF), the Cybersecurity Framework (CSF), and/or the MITRE ATT&CK® framework.
- FISMA CIO Reporting Data: Datasets that support the FISMA metrics survey [FY2023 CIO FISMA Metrics], which specifies required reporting for all federal agencies in order to demonstrate

[9] "DoDAF Viewpoints and Models, Data and Information Viewpoint, DIV-2: Logical Data Model," U.S. Department of Defense, accessed August 17, 2023, https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_div2/.

effectiveness in strengthening federal cybersecurity through policy and practices.

Some datasets are intended for future integration into the CDM system but are still theoretical (i.e., non-operational) and have not been baselined into the program's requirements.

2.2 Relational Structure and Implications

The LDM referenced in this document represents a UML-based entity relationship diagram (ERD) of the key data elements that the CDM PMO has determined as applicable to a minimally effective implementation of the CDM solution. Consistent with ERD design, the principal parts of the LDM are *entities* and *attributes*:

- Entities are principal objects (subjects) between which relationships are established; typically, they facilitate the capture of important datasets. Entities are commonly thought of as "tables" or "classes" in data design, although this document exclusively uses the term "entity."
- Attributes represent the detailed properties of each entity, which facilitate describing, through data, the unique characteristics of an instance of that entity. Each entity is normalized to feature the same type of attributes and each instance of an entity may have different values for those attributes. For example, if **DeviceOnNetwork** represents an entity with attributes of **DeviceCategory**, **DeviceFQDN**, and **DeviceType,** the unique properties of each device are inventoried in a "device collection" for the CDM solution. It is important to note that relationships between entities may feature attributes that describe the characteristics of that relationship, and not all attributes are equal (e.g., some can be used as unique identifiers and some can be multivalued). The data dictionary in this document provides additional guidance regarding differences between entities and attributes, including the type and use of attributes.

Along with the LDM, this document represents and describes the CDM mission needs, including required business processes, relationships, and sufficient level of detail for collected data. This document does not include or describe a physical data model representation and therefore is agnostic to specific technical implementation details. However, while the storage and execution of queries or searches within the actual CDM solutions might not follow the standard relational database construct, the overall solution must produce result sets subject to the proper expression of the relationships as described in this document.

The visualization of the data elements and their associated relationships creates a coupling of CDM data that the PMO will leverage to produce specific information for agency stakeholders and oversight bodies such as the OMB.

Finally, as mentioned previously, this document provides supporting information for an LDM and, as such, does not completely decompose all relationships between all entities as a physical data model utilized by a relational database management system might do. Specifically, most many-to-many relationships between entities—in which instances of elements from both sides of the relationship can be associated with multiple instances from the peer entity—have *implied* associative tables (also known as cross-reference tables) for which primary keys from each entity can be combined to create a logical primary key by bringing together two foreign keys from each of the related entities. Tables such as these have been utilized in interrogation specifications and have been noted as appropriate for the audience to consider.

In cases when supplemental attributes exist within an implied associative table and need to be clarified and defined, these are formally modeled in the LDM. For example, Figure 2-1 (from the CDM LDM) shows a many-to-many relationship between the **DeviceOnNetwork** and the **UniqueSoftware** entities, with a formally modeled associative table (i.e., no longer implied). The additional attributes needed to be captured within the CDM LDM and data model document for clarity and completeness.

Figure 2-1: Many-to-many relationship between DeviceOnNetwork and UniqueSoftware with a "realized" implied table [SoftwareInstalledOnDevice]

2.3 Specialization/Generalization

Specialization is the process of describing a set of *subclasses* of an entity. The set of subclasses that form a specialization describe a distinguishing set of characteristics of the entity, which is the *superclass.* Examples of specializations in the CDM LDM include **ToolSensorDeviceOnNetwork** and **MobileDeviceOnNetwork**, which are specializations of the superclass **DeviceOnNetwork**:

- A **MobileDeviceOnNetwork** describes a type of **DeviceOnNetwork** (i.e., a mobile device is a category of device that is captured as part of a system). The distinguishing characteristic of the device entity that describes this specialization is a device category of mobile device. Similarly, **ToolSensorDeviceOnNetwork** describes a specialization of a **DeviceOnNetwork** serving in a particular CDM security capability-based role (i.e., a device that serves in the role of sensing devices, vulnerabilities, or misconfigurations on the network).
- A specialization is typically used in data modeling to capture a special set of attributes that are specific to a subclass but share all other attributes with the superclass. In the **ToolSensorDeviceOnNetwork** example specialization, a tool/sensor device has many of the attributes a generic device has, but it also has tool/sensor-specific attributes (e.g., **ToolSensorType**, **ToolSensorVersion, ToolSensorProduct, ToolSensorVendor, ToolSensorUpdate,** and **NVDLastUpdateDate**).
- A specialization may also capture a special relationship the subclass entity has with another entity that the superclass entity does not. In the **MobileDeviceOnNetwork** example, a mobile device relates to a user in a way that a generic device does not; it captures the user that a mobile device is assigned to. Therefore, there is a unique relationship between **MobileDeviceOnNetwork** and **User** that does not exist between **DeviceOnNetwork** and **User**.

Generalization is the reverse of specialization, where the differences among a set of entities are suppressed and their common features are captured in a generalized entity. For example, the **DeviceOnNetwork** entity can be viewed as a generalization of **ToolSensorDeviceOnNetwork** and **MobileDeviceOnNetwork**. While specializations and generalizations can be transformed into relations in different ways in database implementations (physical model), this document assumes, for ease of query construction, that specializations in relational implementations are being transformed into separate tables along with a table for the superclass within a relational database implementation. For example, refer to the interrogation specification ***Mobile Devices Without Full Device Encryption:*** *Use CDM to find the number of mobile devices without full device/disk encryption enabled.* This interrogation specification envisions a table **DeviceOnNetwork** and a table **MobileDeviceOnNetwork** to create the query that would satisfy the interrogation specification (see Table 2-1). An example of these modeling constructs can be seen below in Figure 2-2 for **DeviceOnNetwork**, **MobileDeviceOnNetwork,** and **ToolSensorDeviceOnNetwork**.

Table 2-1: CDM interrogation specification that defines the use of specialization MobileDeviceOnNetwork

Mobile Devices Without Full Device Encryption: Use CDM to find the number of mobile devices without full device/disk encryption enabled. **(CDM PMO)**	SELECT DeviceOnNetwork.SystemBoundaryID, COUNT(MobileDeviceOnNetwork.DeviceOnNetworkID) FROM DeviceOnNetwork INNER JOIN MobileDeviceOnNetwork ON DeviceOnNetwork.DeviceOnNetworkID = MobileDeviceOnNetwork.DeviceOnNetworkID WHERE DeviceOnNetwork.DeviceEncrypted = "FALSE" -OR- SELECT DeviceOnNetwork.SystemBoundaryID, COUNT(DeviceOnNetwork.DeviceOnNetworkID) FROM DeviceOnNetwork WHERE DeviceOnNetwork.DeviceCategory = "MOBILE DEVICE" AND DeviceOnNetwork.DeviceEncrypted = "FALSE"

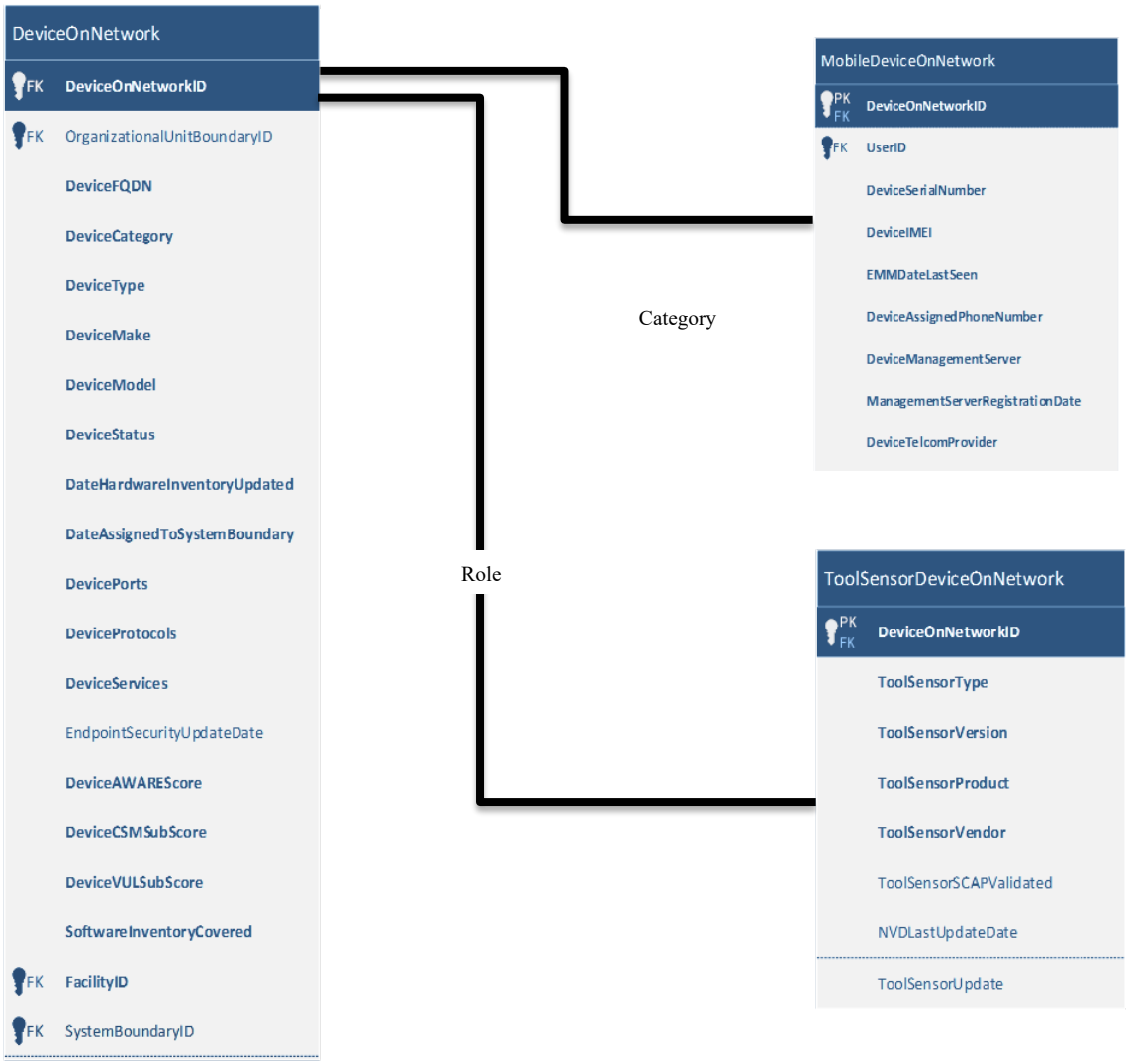


Figure 2-2: DeviceOnNetwork with specializations MobileDeviceOnNetwork and ToolSensorDeviceOnNetwork

2.4 Multivalued Attributes

Within each CDM Data Model entity, attributes represent a discrete, singular value or characteristic of an entity. In some cases, *multivalued* attributes represent relevant characteristics that can have multiple values instead of just one. An example of a multivalued attribute in the CDM Data Model is the **DeviceAssignedPhoneNumbers** attribute in the **MobileDeviceOnNetwork** entity. The mobile device phone number may not typically be a singular value but rather 1 - n values representing one or more phone numbers assigned to the mobile device; therefore, it is modeled as a multivalued attribute. Multivalued attributes are typically transformed into relationships within relational physical data models. This typical transformation is reflected in the interrogation specifications involving multivalued attributes from the CDM LDM. See Figure 2-3.

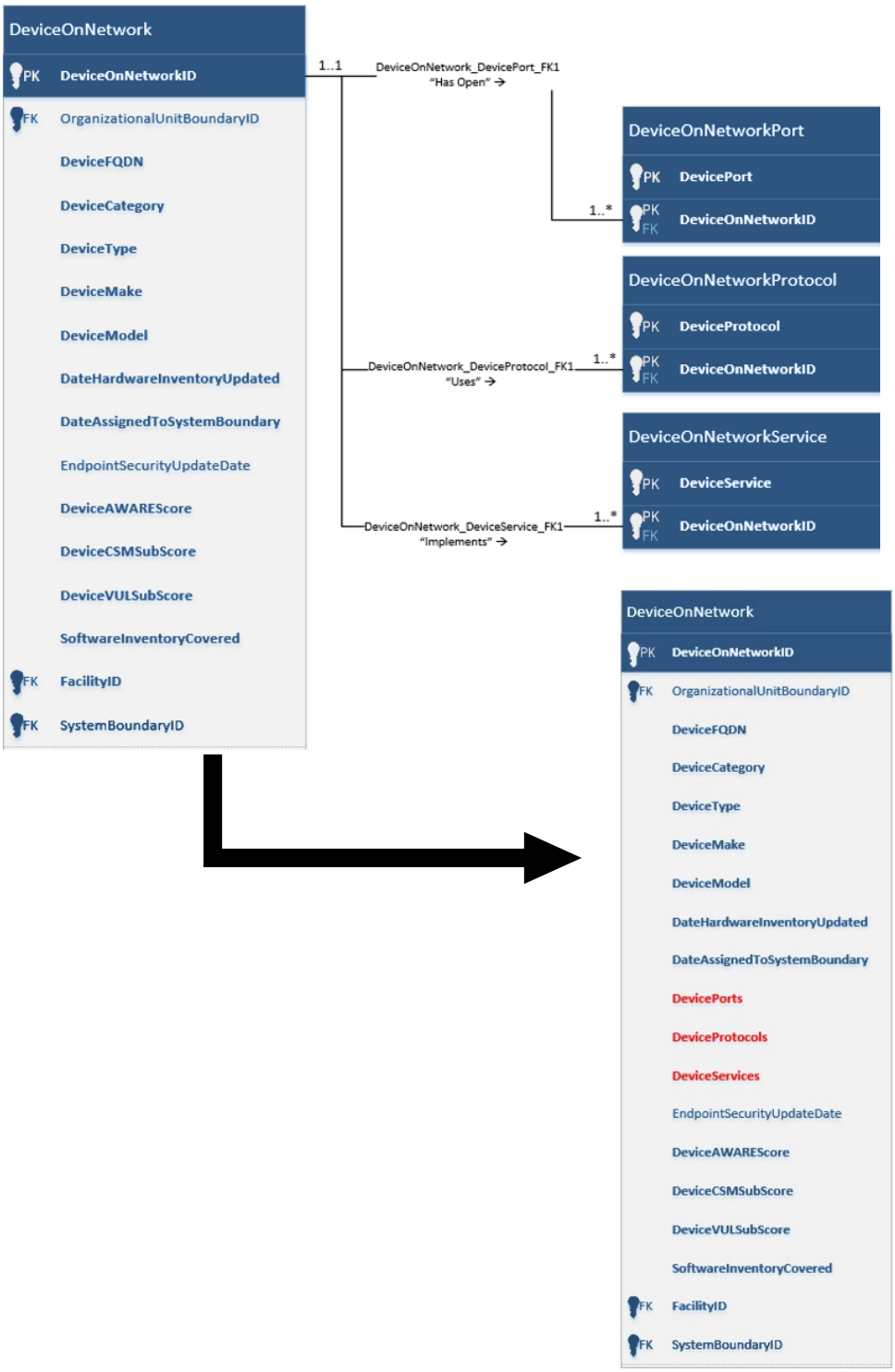


Figure 2-3: Multivalued attributes DevicePort, DeviceProtocol, and DeviceService illustrate typical one-to-many relationships that would be created in a database management system and used in queries.

2.5 Master Device Record: Unique Identification of Hardware Devices

The first phase of CDM is grounded in developing a comprehensive inventory of what is on the agency's network through the identification and discovery of IT assets. This allows for enumeration of fundamental CDM containers (i.e., organizational unit [OU] and FISMA containers) such that security policies and assessments can be conducted. To support this end state, the logical construct described as the master device record (MDR) was developed, enabling the CDM solution to group vital characteristics on each inventoried device in a way that can be uniquely referenced for determining desirable states for that device.

Elements of the MDR include attributes specified in the **DeviceOnNetwork** entity in addition to the CDM Asset Management capability attributes that have security relevance, which include discovered vulnerabilities (VUL), discovered misconfigurations (CSM), and installed software (SWAM). See Figure 2-4 for more information.

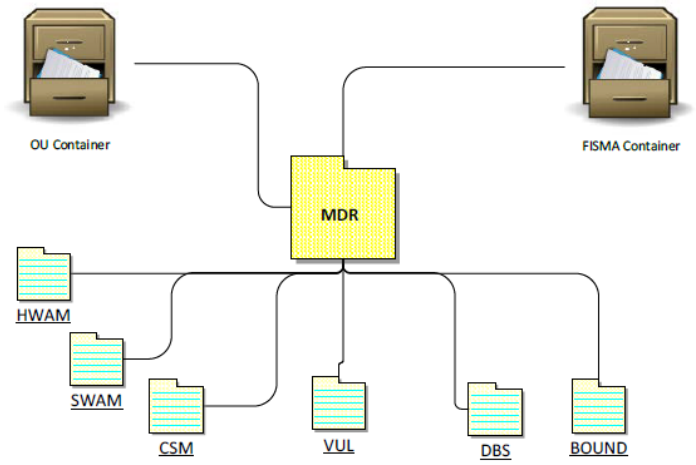


Figure 2-4: MDR illustrated: CDM Technical Capabilities Volume 1, Defining Actual and Desired States, version 1.1

To implement the MDR, the CDM program requires a CDM solution to be able to uniquely identify hardware devices within a department or agency (hardware unique identifier [UID]). The **DeviceOnNetworkID** field is stipulated in the CDM Data Model as a facilitator of this capability, allowing the association with a unique identifier (i.e., primary key) with a hardware asset once it has been identified within the CDM data that resides within the agency's CDM solution. The CDM Data Model does not prescribe the methodology for achieving this identification; the agencies and their CDM integrators must leverage the data on hand to achieve this. Some relevant characteristics of IT assets that could be used in this derivation of a UID include the following:

- Fully Qualified Domain Name (FQDN)
- Globally unique ID as assigned by OSs or hypervisors (e.g., vCenter)
- Custom registry keys or data tokens that reside within the OS
- MAC addresses
- IP addresses (e.g., static management IPs or Dynamic Host Configuration Protocol-Bounded IPs)
- Hardware profile (e.g., presence of certain physical hardware)

Through the ability to uniquely identify hardware assets and the combination of required, reportable hardware attributes as prescribed in the CDM Data Model under the **DeviceOnNetwork** entity, the concept of the MDR can be realized.

2.6 Creating a Software Inventory: Unique Identification of Software

Another key requirement for an effective, secure CDM solution is its ability to discover software within an agency. Similar to the idea of the MDR, the CDM solution needs to filter through various software installations,

including lower-level software components, such as binaries, executables, and other data points within the agency environment, in order to positively identify particular software products. This requirement, represented in the LDM as the **UniqueSoftwareID** attribute, also necessitates the ability to determine variations between major and minor revisions while deduplicating the same software (rev/version) that may have slightly different common naming conventions in the system on which it operates (e.g., in the Windows registry).

The CDM solution is heavily dependent on unique identification of software products—also referred to as software configuration items (SWCI) in the CDM program's requirements—to determine vulnerabilities, configuration settings, and authorization of use. For the purposes of this data model and the expectations of the CDM program, the scope of software inventories focuses on distinguishing and classifying SWCIs (i.e., software products) and not software components, which represent much larger sets of files that are packaged or related together to comprise an SWCI that operates on an endpoint.

The CDM program expects CDM integrators to inventory all relevant software components using CDM tools and to normalize this raw data into relevant software product inventory data for the purposes of data ingestion into other layers of the CDM solution. In this manner, each CDM solution shall have the capability to allow end users to understand what software products are composed of what software components; however, tracking these relationships for upward reporting into the CDM agency dashboard is not expected.

The CDM Data Model does not directly dictate the methodology for achieving unique identification of software products; however, some relevant characteristics that can be leveraged include the following:

- Hash values (either of executable code or a combination of associated binaries and other library files employed)
- Industry naming values:
    - Imprinted on install (e.g., Windows Registry)
    - Queried from management tool (e.g., IBM BigFix, Microsoft System Center)
    - Pulled from any associated configuration files
    - Queried from a package manager (e.g., RPM)
    - Retrieved from other interrogation methods

2.7 Managed Applications: Risk Accountability Based on HWAM and SWAM Datasets

Agencies manage IT assets at various levels of granularity as appropriate for the situation. This includes taking into account many factors, such as mission impact and accountability. In practice, it is common to have "split responsibilities" on devices and their associated software when agencies determine that certain applications have distinct business functions or operational requirements (e.g., FISMA System A has authority over the secure configuration of web software that resides on Device B, whose authority regarding secure configuration of the OS resides under the logical boundary of FISMA System B).

As part of implementing functionality that aligns with common agency practices, the CDM architecture allows for the risk management process of separating groupings of installed software into artificial management constructs. This construct is referred to as a "managed application" (**ManagedAppOnNetwork** in the LDM) and is instantiated using vital information from both HWAM (i.e., devices on the network) and SWAM (i.e., software on the network) inventories. Once codified, a managed application can then be associated with other security-relevant information produced from CDM tools/sensors, including CSM (misconfigurations) and VUL (vulnerabilities) datasets. This ensures that security risk accountability is assigned appropriately and is

consistent with agency policy, personnel roles, and the NIST RMFt's.

Table 2-2: Examples of Interrogation Specifications for the Managed Application Concept

Data Interrogation Action	Interrogation Specification
Total "Managed Application" Count: Use CDM to find the number of actively managed applications within the organization's unclassified network(s). (Analogous to the **Total Hardware Assets** interrogation action)	SELECT ManagedAppOnNetwork.OrganizationalUnitBoundaryID, COUNT(ManagedAppOnNetwork.ManagedAppOnNetworkID) AS TotalManagedApplications FROM ManagedAppOnNetwork GROUP BY ManagedAppOnNetwork.OrganizationalUnitBoundaryID
Vulnerable "Managed Applications": Use CDM to find networks hosting vulnerable managed applications for which a patch or workaround may be needed. (Analogous to the **Vulnerable Devices** interrogation action)	SELECT ManagedAppOnNetwork.SystemBoundaryID, ManagedAppOnNetwork.ManagedAppOnNetworkID FROM ManagedAppOnNetwork INNER JOIN VulnerabilityOnNetwork ON ManagedAppOnNetwork.ManagedAppOnNetworkID = VulnerabilityOnNetwork.ManagedAppOnNetworkID GROUP BY ManagedAppOnNetwork.SystemBoundaryID

Agencies can instantiate managed applications by including discrete, inventoried software into an artificial entity that will share a common set of attributes (e.g., Namespace, Organizational/System Boundary Membership). This process logically segments applications with higher-level business functions from the supporting host OS or infrastructure on which it resides. This has a multifaceted benefit in that (1) there is an organic instantiation of risk inheritance to other supporting IT assets, which can be explicitly traced, and (2) managed applications can now serve as a potential anchor point for an itemized assignment of risk (e.g., vulnerabilities/misconfigurations) that is distinct from their host OSs or infrastructure. The result is traceability for security practitioners who have the responsibility, authority, and, ultimately, motivation to take appropriate action.

Agencies, as part of their internal governance processes, can develop any number of these managed applications to accurately reflect the desired state of their IT asset inventory for assessment and authorization purposes. Due to the many similarities to devices from a data interrogation perspective, the CDM Data Model Document does not explicitly include managed applications in its queries. Where appropriate, the data interrogation specifications annotate which queries can be executed on the **ManagedAppOnNetwork** entity, making it transparent how the CDM datasets can be extended to support this concept. See Table 2-2 for examples of interrogation specifications that have been adapted to the managed application concept.

2.8 Master User Record: Unique Identification of People

In the second phase of CDM, the program will model various attributes and entities that focus on the awareness of who is on an agency's network and, given their status on the network, what the implications are for the security of systems within the agency's boundary. This is principally accomplished by development of CDM's master user record (MUR) construct, which is defined as follows: "The MUR represents an entity (person or non-person) that requests access to information, information systems, and facilities and deals with 'Who is on the network?' The MUR includes information about credentials (i.e., elements of who) for identification, authorization (i.e., elements of trust) for access rights and permissions for granted access, accounts associated with information systems, and appropriate training for specific roles and responsibilities."

Within the context of the CDM Data Model, the MUR is employed when an agency user is *uniquely* (see below) transcribed into an instance of the *User* entity (as defined in the data model with the required information) with proper associations made with that user's CDM Identity and Access Management attributes. These attributes, referred to as PRIV, CRED, BEHAVE, and TRUST, are tailored and assigned to each agency user based upon their roles and responsibilities at the agency. See Figure 2-5.

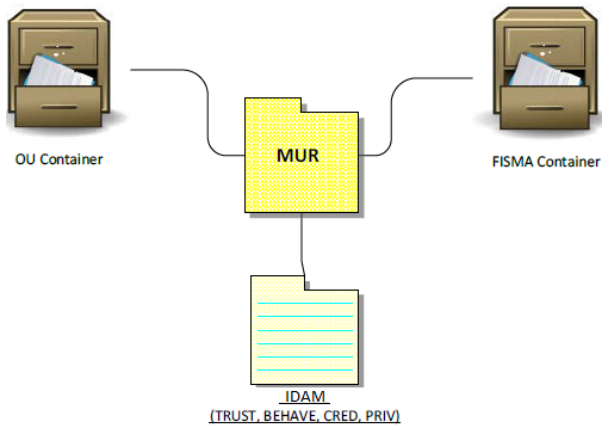


Figure 2-5: MUR illustrated: CDM Technical Capabilities Volume 1, Defining Actual and Desired States, version 1.1

The MUR requires that a user be codified in a manner that has absolute fidelity, is non-duplicative, and can be uniquely traced to CDM instantiated containers (i.e., FISMA containers/systems, OU containers/hierarchy). This requirement for unique identification of users within a network can be implemented using a variety of technical methods and information within the enterprise, such as:

- Combination of full name (first name, middle name, family name)
- Electronic Data Interchange Personal Identifier
- Agency unique employee ID number
- IT systems-derived UIDs – Active Directory GUID, User Principal Name (UPN), etc.
- Other agency-specified identification attributes[10]

In the CDM Data Model, the *UserID* attribute will accommodate the data output of any integrator's approach to implementing the unique identification requirement. It is the primary key for the MUR. Using the unique identification properly along with the capture attributes (i.e., PRIV, CRED, BEHAVE, TRUST) within the MUR, CDM users will be able to identify deficiencies against an agency's desired state (as documented by policies) for agency personnel and to produce actionable data.

[10] Agencies and integrators should be cognizant of any sensitive PII issues that may arise when determining what attributes may be implemented to fulfill this requirement, including any additional technical controls that may be necessary to protect any PII resident in the CDM system.

2.9 Creating the Master Incident Record: Tying Incidents, Related Events, Actors, and Activities Together

The master incident record (MIR) was conceptually architected to support the mission need of determining what, from a security incident relevant perspective, is happening on the network.[11] This capability is implemented by logically tying events, CDM-produced machine data, and containers together with activities and attributes that describe a suspected or confirmed security incident and the agency's response. This process allows for traditional, previously isolated reporting processes to be enriched by virtue of harmonizing incident information with other conceptual elements under CDM—such as OU and FISMA containers, MDRs, and MURs. The combination of these constructs can be fully leveraged to support existing reporting requirements within the .gov space as required by federal initiatives (i.e., CISA Federal Incident Notification Guidelines).

In the CDM LDM, the MIR is visually represented by relating entities such as incident (**IncidentOnNetwork**), events produced by agency tools **(EventOnNetwork)**, actions that have potentially detrimental impacts (**IncidentAction**), and the actors that contributed to the incident **(IncidentActor).** These information types are then contextually tied together with information under CDM device and user data to portray a holistic picture of potentially impactful occurrences that could reduce the security of a system or its assets. Additionally, the CDM Data Model tracks activities that are conducted in response to the incident through **ResponseActivity** entity, which models what critical steps may be taken by an agency to initiate containment, eradication, and/or recovery after confirmation of an incident. Finally, as part of collecting the salient attributes necessary to report the incident, any indicators (**IndicatorOfCompromise**) are documented and associated with the MIR.

It is critical to note that within the CDM architecture, the MIR and all associated entities and attributes will support incident response reporting at an elevated view that is not overly burdened by unprocessed, raw data—data that has not been refined, analyzed, and correlated to a suspected or confirmed incident (see **Event** in Data Model Key Terms section for additional context). To achieve this, lower levels of the CDM architecture (i.e., tool/sensor layers[12]) will be leveraged to implement CDM and agency-related policies that produce and correlate the information needed to establish sufficient evidence that anomalous or undesired activity is occurring within the network—activity that requires incident response and management.

This "processing" of raw event data to security actionable information is then recorded as an **EventOnNetwork** and provides the targeted, detailed information that is critical in the identification process of an incident on an agency's network. As an incident is codified and recorded, it is further investigated and analyzed to parse out the other related attributes and entities, including the actions that may have caused or been involved in the incident (**IncidentThreatAction**) and the actor who might have initiated the actions **(IncidentActor).**

[11] NIST defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." CDM uses the same common understanding in the definition of "incident" within this document.

[12] Tools and sensors provided under the capabilities within "Network Security Management" phase, such as "Manage Events (MNGEVT)," "Operate, Monitor, and Improve (OMI)," which includes products classified as SIEM tools, endpoint detection and response tools, IDS/IPS, etc., are anticipated to support the CDM architecture under this requirement.

2.10 Organizational Unit Containers (Organizational Unit Boundaries)

Standardizing the definition of the agency organizational structure is key to (1) providing organizational unit (OU) context in support of risk posture scoring and (2) providing finer-grained identification of the OU policy parameters referred to within NIST SP 800-53 definitions. The CDM solution requires that object-level data (e.g., IT assets/devices) be grouped into OU containers for reporting, policy mapping, and risk posture scoring. The CDM PMO requires that an agency minimally decompose its OU hierarchy and organize associated CDM objects to at least one level. Agencies may go beyond one level if desired, but the data will always be aggregated for reporting purposes to the federal dashboard to one level of depth. See Figure 2-6 for the DHS OU hierarchy decomposed to one level of organizational depth.

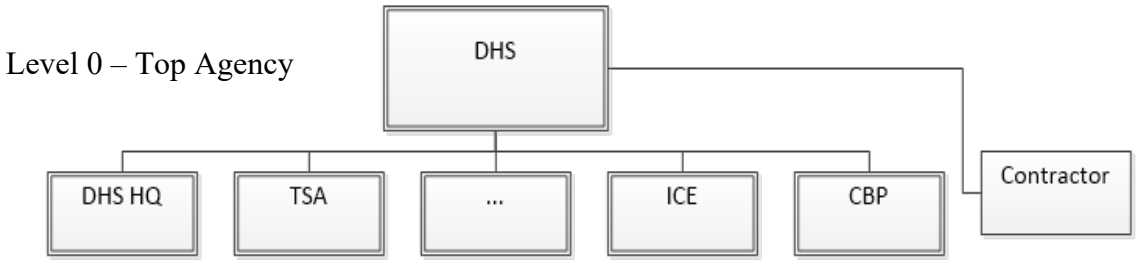


Figure 2-6: OU Hierarchy for the Department of Homeland Security

2.11 FISMA System Containers (System Boundaries)

FISMA system containers, also known as FISMA containers, information system, and/or system boundaries, represent a core organizational construction for the implementation of the CDM solution. This construction is informed by security artifacts, such as a system security plan, and represents a logical boundary for which common security controls and policies are applied to a grouping of related assets (e.g., networks, devices, and people) to accomplish some mission or business objective, per the NIST RMF.[13] The FISMA container should also be thought of as the authorization boundary for an information system for which security controls and FIPS impact ratings apply.

[13] Identifying well-conceived information system boundaries is challenging but necessary for achieving the fundamental objectives of the CDM program. Agencies and integrators should refer to NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems" for additional guidance.

2.12 CVE and CCE Dictionaries

The CDM Data Model stipulates that the solution be capable of referencing a dictionary of well-documented standards for identifying software vulnerabilities and configurations. The anticipated process is that CDM-provided scanners or configuration managers will produce raw results that identify "defects" (e.g., vulnerabilities or configurations outside the baseline) that natively might not be standardized across industry using a common identifier. To normalize this data and provide relevant support information that is consistent with the CDM objectives of helping agencies find, prioritize, and address the "worst things first," the CDM program has engineered an information exchange mechanism between the CDM federal and agency dashboards. This "flow down" of information shall provide the following standardized information:

- A content dictionary of all common vulnerabilities and exposures (CVEs) and their related scoring parameters for the CDM program, represented as the **CVEDictionary** entity in the data model.
- A partial content dictionary of common configuration enumerations (CCE) that detail critical security configurations reported to the CDM program, represented as the **CCEDictionary** entity in the data model.
- A partial, referential list of all common platform enumeration (CPE) records for the CDM program as available from external sources to facilitate the normalizing and reporting quality of software assets in agency CDM solutions.

The CDM program expects that updates to these sets of information (CVE, CCE, and CPE) will be disseminated on a recurring schedule to ensure all agencies have the latest, consistent dictionary of these standards. The CDM federal dashboard will continue to derive updates based upon a combination of external sources, such as:

- NVD feeds – CVEs, CCEs, CPEs: https://nvd.nist.gov/vuln/data-feeds#
- Industry available data (e.g., threat feeds, vulnerability reports)
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs): https://www.disa.mil/~/media/files/disa/news/conference/cif/briefing/ia_stig_scap_and_data_metrics.pdf
- CDM-specific derivation (e.g., creation of new CPEs/CCEs for CDM purposes)[14]

The CDM program requires that every agency's CDM solution maintain a comprehensive referential copy of all the CCEs, CPEs, and CVEs through this prescribed dashboard-to-dashboard information flow, to ensure that all discovered items within an agency have the proper baseline for indexing inventories and risk.

In some cases, such as CCEs and CPEs, agencies will have an operational need to develop their own dictionary entries to properly identify, normalize, and report items in the CDM solution. This is acceptable and expected, with provisions made in the CDM agency dashboard for the creation of local variants of dictionary items that remain at agencies. When agency and federal dictionary items conflict, the federal dashboard-provided information is authoritative.

[14] The CDM program recognizes that certain standards (such as CPEs, CCEs) are not maintained synchronously with industry trends; therefore, there is a need to quickly codify CDM-specific entries of these indicators to maintain a relevant standard. To this end, the program may develop proprietary material (new CPEs, CCEs) that will be used operationally to achieve mission objectives.

2.13 CyHy "Findings" Datasets

The Attack Surface Evaluation (ASE) team within DHS offers the Cyber Hygiene (CyHy): Vulnerability Scanning service to help federal agencies secure their internet/externally facing systems from "weak configuration and known vulnerabilities."[15] Agencies subscribe to this service by coordinating and registering an agency's known public IP space with the ASE team, after which automated scanning occurs on a recurring basis. The results are collated for analysis, and any confirmed findings are shared with agencies.

In coordination with the ASE team, the CDM program is developing an updated data dissemination approach that will allow the CDM system to pull and distribute these findings to facilitate automated, rapid sharing of cyber-relevant information to CDM practitioners. The information will be parsed, allocated, and stored in the CDM solution, where it can be visualized in context of other germane information provided by the CDM tools/sensors, which actively scan the interior of each agency's IT architecture. This cohesive approach will enrich the cyber awareness of agency stakeholders, allowing them to view risk as a measure of both internal and external defects.

The CyHy dataset is awaiting further revision. This will be addressed in the near future.

2.14 Threat Intelligence Within CDM

One of the CDM's core objectives is to provide stakeholders with information that helps them identify and prioritize the worst issues on their network. In full support of this vision and to evolve the CDM system to be a consummate platform for risk management practitioners, the CDM Data Model has incorporated threat intelligence products and correlated them to defects that can greatly benefit from this external information. Similar to other referential contracts that are containers for CDM-disseminated information (e.g., CCE/CVE dictionaries), the LDM implemented an entity, **ThreatIntelligence**, that can accommodate vendor/organization-agnostic threat intelligence to elevate the understanding of risk of any particular defect that the CDM system may discover within an agency's network.

2.15 CDM-Required Data

This document specifies the data elements that are *required*, *conditionally required*, and *recommended*.

Required data elements are identified as "required" because they fulfill certain CDM mission-essential data needs.[16] Specifically, they represent data that feeds CDM data requirements (e.g. interrogation actions indicating CDM PMO-prescribed data needs) and/or AWARE risk posture scoring requirements. Interrogation actions are a set of mechanisms that enable users to interrogate the information collected by CDM in a meaningful way.

Conditionally required data elements are identified as "conditionally required" because they are required if a certain condition exists. They carry the same related guidance as "required" (i.e., CDM mission-essential datasets) but do not unilaterally apply without some additional context. This additional context includes the following:

- CDM capability required for production: Some agencies may not have access to the security capabilities necessary to produce this data. Therefore, the data may be required only for CDM solutions that employ that capability (e.g., NAC, EMM).

[15] For more information, see the Cyber Hygiene Services website: https://www.cisa.gov/cyber-hygiene-services.
[16] Note that when required data is discussed in this document, it does not include that dimension of physical implementation where additional data fields may be required to ensure dashboard functionality as designed.

- Context of CDM object: Some attribute-level data requirements apply only when a device or user type is captured in the solution or when other related attributes and/or entities must exist.

For all data elements tagged as "conditionally required," the CDM PMO will state the condition that applies.

Recommended data elements are identified as important but do not necessarily directly satisfy essential data needs. These may be data attributes that support the required (or conditionally required) data by providing operational context or other information to assist agency decision makers. These are recommended data elements that are included in the LDM or come from other sources (e.g., industry) and can enhance an agency dashboard use case; however, elements are not necessarily needed to construct an AWARE risk posture score or provide essential datasets to DHS.[17] The CDM PMO considers these optional but strongly recommended when achievable. *All data elements that are not required or conditionally required are recommended*.

[17] Datasets that are "recommended" shall be considered required if agency policy or other agency-directed input deems them necessary for an operationally effective CDM solution. Absent this direction, it is expected that the recommended data is acquired and ingested if/when available by tools (best effort).

3 DATA MODEL KEY TERMS

CDM Data Model key terms provide additional context for reference when interpreting the logical and conceptual data models and their associated entities and attributes.

Account – In the CDM Data Model, an account represents the intersection of a CRED associated with a user (as defined in this document) and a token (i.e., data needed to verify account ownership such as a secret assertion, digital certificate, PIN, password). Accounts have privileges and entitlements assigned, which can be leveraged upon successful user authentication. (See **Account** in the Data Dictionary for the Logical Data Model section.) [CDM PMO]

Actual State – The discoverable/observable state of relevant objects (e.g., devices, software, people, credentials, accounts) based on security-related, sensor-collected information. The actual state includes the states and/or behaviors that may indicate the presence of a security defect. [CDM Technical Capabilities, Vol. 1] [CDM PMO]

Approved Software – Software products collated from an agency-defined approved software list that has been developed and validated, subject to policy. Software does not have to be installed or present on an agency's network to be on the approved software list. Approved software lists may be documented through a combination of system security plans (SSPs), proper enterprise architectural governance policies by an agency or organizational unit (e.g., an approved enterprise architecture and relevant technical insertions at an agency may be automatically authorized to all subordinate OUs and their FISMA systems, and thus would be part of an approved software list that pertains to these structures), and/or by virtue of individual device-based dispensations. Approved software lists are considered part of "desired state" policies that are used by the CDM system to determine if/when authorized/unauthorized software exists.

Authentication – An event that occurs when a user is bound to an account through leveraging a specific CRED and the proper token, which are verified digitally. The result of a successful authentication event is that a user properly validates account ownership by leveraging the appropriate CRED assigned to them, which then permits the user to exercise privileges and access rights authorized for that account. [CDM PMO]

"Authorized" Device – A device is considered authorized—by CDM and as it relates to this data model—if it belongs to a FISMA system boundary (i.e., information system, FISMA containers; see **SystemBoundary** for more information) that has a current, valid ATO. FISMA system boundaries are authorized by an authorizing official who provides an authorization decision and formally assumes responsibility for operating an information system at an acceptable level of risk. Devices not associated to authorized system boundaries are considered "unauthorized." Agency policies determine when/if associations to any SystemBoundary are made and may be implemented in CDM tools/sensors directly. [CDM PMO]

"Authorized" Software – Installed software is considered authorized if it is on the agency's approved software list that is associated with the device. (See **SoftwareAuthorizationStatus** in the Data Dictionary for the Logical Data Model section.) [CDM PMO]

Authorization Decision – An action related to authorizing a system for a prescribed level of operation by an authorizing official. (See **AuthorizationDecision** in the Data Dictionary for the Logical Data Model section.) [CDM PMO]

Authorizing Official – A senior federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the nation. [NIST SP 800-53 r5, 800-53A r5, and 800-37 r2] (See

AuthorizingOfficial in the Data Dictionary for the Logical Data Model section.) [CDM PMO]

AWARE [risk posture scoring Igorithm] – AWARE (Agency-Wide Adaptive Risk Enumeration) is the CDM Program's attack surface risk posture scoring methodology that provides participating agencies with situational awareness of cyber risk related to cyber posture and encourages prioritized remediation of vulnerabilities with a special emphasis on real-world threats. [AWARE Technical Design]

BEHAVE – Departments and agencies have an increased risk when any user is granted access to facilities, systems, and information without the appropriate security training, demonstrated skill, specialty knowledge, or suitable certification. These users may have been granted access to resources or sensitive data through a) incomplete security-related documentation or training, b) ineffective training, or c) failure to have been assigned the proper training for access. The overall purpose of the Manage Security-Related Behavior (BEHAVE) capability is to document that authorized users exhibit appropriate security-related behavior. For CDM, appropriate security-related behavior is defined as actions that have been understood and agreed to by the user via user agreements, training, job requirements, or similar methods. Exhibiting appropriate security-related behavior is limited to verifying the existence of artifacts that demonstrate the user's compliance to security-related behavior policy associated with systems access or job performance. Collecting data associated with completed training, testing, and security-related BEHAVE documentation will provide measurable data elements for the creation of automated security checks. These security checks provide the basis for automating the monitoring, reporting, and prioritizing of security-related behavior deficiencies in an agency's cyber environment. (See **BEHAVE** in the Data Dictionary for the Logical Data Model section.) [CDM Technical Capabilities, Vol. 2]

Benchmark – A set of federal security configuration settings that may be used in developing a standardized set of configuration requirements for agency IT systems. Available standard industry benchmarks include:

- United States Government Configuration Baseline (USGCB)
- DISA Secure Technical Implementation Guides (STIGs)
- Center for Internet Security Benchmarks (CIS Benchmarks)

For the CDM program, the common (minimum) baseline across the .gov domain will incorporate key high-priority configurations that should be implemented across all agencies. Initially, these have been scoped to the STIG category 1 (most severe) configurations and have been incorporated into the CCE Dictionary for all agencies to measure against. Although there will be many similarities between the scope of the common federal baseline and any local agency baseline, it is expected that both sets shall be measured by the CDM solution. (See related item **MisConfigurationOnNetwork** in the Data Dictionary for the Logical Data Model section.) [CDM PMO]

CCE Dictionary – A logical configuration item used by the CDM solution to ingest and provide a baseline of configuration settings that the CDM program will leverage for identification of security risk. For CCEs in this dictionary, this activity includes looking at key configurations whose settings have significant IT security ramifications; violation of expected values for these settings should be carefully examined and remediated by organizations. The entries in the CCE Dictionary (provided by the federal dashboard as government-furnished information [GFI] to agency dashboards) represent a minimum defined standard for scoring and reporting, and are not intended to be a comprehensive list of all potential configuration items across all operating environments. Agencies are expected to extend this approach and implement their own unique, local CCEs that are consistent with their configuration baseline and go beyond the CDM-provided benchmark. (See **CCEDictionary and CCEInfo** in the Data Dictionary for the Logical Data Model section) [CDM PMO]

Certificates – A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its validity period. [NIST SP 800-57 pt1, r5]

Common Configuration Enumeration (CCE)[18] – A dictionary of unique identifiers for common system configuration issues. CCE assigns a unique common identifier to a particular security-related configuration issue. When dealing with information from multiple sources, use of consistent identifiers can improve data correlation; enable interoperability; foster automation; and ease the gathering of metrics for use in situation awareness, IT security audits, and regulatory compliance. (See **CCEID and CCEInfo** in the Data Dictionary for the Logical Data Model section.) [NIST.gov] [CDM PMO]

Common Vulnerabilities and Exposures (CVEs) – An individual record from a dictionary of publicly known information security vulnerabilities and exposures. It includes a standard for information security vulnerability names. The standard allows data exchange between security products. CVEs are used to populate CDM vulnerable software data. (See **CVEID, CVEType, CVEDescription, CVEReferences,** et al. in the Data Dictionary for the Logical Data Model section.) [CVE.MITRE.gov]

CRED – The CDM Data Model digital manifestation of a user that determines how a user can successfully authenticate (bind) to an account and its associated privileges and entitlements. Many agencies employ an established process for issuing different credential types and defining authentication requirement policies to access various systems and information. In the CDM Data Model, CRED documents this process by collecting the key information on the binding of credentials to users and allows for modeling of what accounts users are authorized to access. When properly implemented in the CDM solution, the documentation of CRED will help ensure every user can be determined to have proper authentication for access to facilities, systems, and information. CRED will also provide insight into whether or not authentication, reissuance, and revocation policies are incurring more risk than deemed acceptable by the agency. (See **CRED** in the Data Dictionary for the Logical Data Model section.) [CDM Technical Capabilities, Vol. 2]

Credential – Evidence attesting to one's right to credit or authority. In the NIST Standard, it is the PIV card or derived PIV credential associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. [NIST FIPS 201-3]

Critical Software – Any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: is designed to run with elevated privilege or manage privileges; has direct or privileged access to networking or computing resources; is designed to control access to data or OT; performs a function critical to trust; or operates outside of normal trust boundaries with privileged access.[19] This definition applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes.

CVE Dictionary – Provided as GFI to CDM solutions and used to baseline key standardizations that the CDM program will leverage to identify security risk. For CVEs, this includes looking at a comprehensive list of vulnerabilities as codified by the NVD. This element will serve as a referential data item, for which

[18] Not all CCEs, as codified by NVD, will be leveraged. The CDM program will prescriptively tailor out which CCEs are of importance (in scope) for discovery or risk posture scoring purposes through the interoperability within the dashboard hierarchy or supplemental guidance. In addition, the CDM program may rely on other sources for configuration settings management checks beyond the NVD's current repository.

[19] "Critical Software – Definition & Explanatory Material," Executive Order 14028, Improving the Nation's Cybersecurity, last modified July 9, 2021. https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory.

supplementation information about a CVE will be present. (See **CVEDictionary** in the Data Dictionary for the Logical Data Model section.)

CyHy Finding – A cybersecurity-relevant weakness or vulnerability that has been discovered by the external scanning activities executed by the ASE team. CyHy findings span different types of "defects" as defined by the CDM program and, on a case-by-case basis, may be indicative of a misconfiguration or vulnerability on network, the latter of which will have a normalized CVE ID assigned to it. Each CyHy finding has calculated values (in days) associated with its age to facilitate BOD compliance. [CyHy]

Data Interrogation Action – Data interrogation actions are a set of mechanisms that enable users to interrogate the information collected by CDM. The desired behavior of data interrogation actions is that they can be specified such that CDM can execute them directly on CDM data without having to modify the CDM implementation. They shall be specified such that an inconsistent result due to an action being interpreted differently by each instance of CDM does not occur. [CDM PMO]

Denied Software – Denied software are software products that may be collated from an agency-defined denied software list that has been developed and validated, subject to policy. Denied software lists may be documented through a combination of SSPs, proper enterprise architectural governance policies by each agency or organizational unit (e.g., an approved EA and relevant technical insertions at an agency may be automatically authorized to all subordinate OUs and their FISMA systems), or by virtue of device-based dispensations. Enforcement of and compliance with denied software lists are considered part of desired state policies that are used by the CDM system to determine if/when authorized/unauthorized software exists.

Derived PIV Credential – A credential issued based on proof of possession and control of a PIV card. Derived PIV credentials are typically used in situations that do not easily accommodate a PIV card, such as in conjunction with mobile devices. [NIST FIPS 201-3]

Desired State – A defined value, list, or rule (specification) that details or enables the derivation of the state desired by an organization to reduce its information security risk. Desired state specifications are generally derived from policy and provided within interrogation specifications. [CDM PMO]

Device On Network – A physical and/or virtual hardware asset managed, inventoried, or otherwise detected by the CDM solution. For CDM Asset Management capability, in-scope IT assets are "IP addressable" over an agency's network. To be included in the CDM implementation, these assets are also positively adjudicated as "in scope" within appropriate agency enclaves by the CDM PMO.

The **DeviceOnNetwork** entity is modeled as a generalization (superclass) with specialization (subclass) entities of **ToolSensorDeviceOnNetwork** and **MobileDeviceOnNetwork**. (See **DeviceOnNetwork** in the Data Dictionary for the Logical Data Model section.) [CDM Technical Capabilities, Vol. 2] [CDM PMO]

(***Note:*** *This model is based on the policy that each device discovered belongs to a single documented FISMA system/boundary, as stipulated by NIST special publications.)*

Digital Worker – An automated, software-based tool, application, or agent that performs a business task or process similar to a human user and uses artificial intelligence (AI) or other autonomous decision-making capabilities. [Digital Worker Identity Playbook (idmanagement.gov)]

Event [On Network] – Any observable occurrence in a system or network [NIST 800-61]. A discovered event can be informational, such as documenting a successful authentication event on a web server (e.g., "User John logged into WebAcme.Org"), and logging data captured such as in Microsoft Sysmon logging, or adverse in nature (e.g., "System SQL.corp.net unreachable for 60 seconds"), depending on the context of the tools and what they are configured to detect and report on. What distinguishes the deluge of events that are triggered

and captured directly by tools/sensors from the events that are correlated and curated for use in the CDM system (i.e., inventoried in this data model as **EventOnNetwork**) is the actual analysis/synthesis of the original event from raw data to "relevant" information—information indicating activity in the network that presents risk to information systems and requires attention. The transformation of raw data into relevant information is largely encapsulated into two sources: (1) CDM processes and (2) agency policies. CDM processes are indicative of pre-established capabilities and the established reporting structure conveyed in this model—e.g., the requirement to report negatively adjudicated NAC events in the solution). Agency policies generically describe mature processes and technologies that facilitate, in a manual or automated fashion, the transformation of any set of events into risk information—e.g., determination of malicious activities by correlation of firewall events to malware indicators). Agency technologies and supporting processes, which may be provided by capabilities baselined within CDM, will generally improve the proactive identification of risk-relevant events and may include investments in areas such as the following:

- Intrusion detection/prevention systems
- Threat intelligence/automated indicator sharing systems
- Machine-learning (ML)/AI-based applications (within or external to tools)
- Security information and event management solutions (SIEM)[20]

Technologies should be customized to reflect tools and sensors that are most closely aligned to agencies' policies and procedures for incident detection and management based upon their own thresholds (e.g., clipping levels, "accuracy" of an alert, and source(s) of alerts).

Events are inventoried within the CDM architecture only in relation to facilitating the identification and reporting of confirmed or suspected IT-based security incidents.

In the LDM, events are captured in the **EventOnNetwork** entity and modeled as a generalization (superclass) with specialization (subclass) entities that relate to the various types of CDM-recognized events and the distinctiveness of their data. For example, **NACEventOnNetwork, UnauthorizedSWEventOnNetwork,** and **MaliciousEventOnNetwork** are type-casted for NAC, SWAM, and incident response-related CDM capabilities, respectively. [CDM Technical Capabilities, Vol. 2]

Entitlement – Entitlements are specific rights that are traceable to a higher-level privilege. Entitlements are used to help illustrate the scope of access that a privileged account may have within the bounds of the privilege category. The agency has complete discretion on how best to implement this entity and its related attributes. Some illustrative examples:

- An account that is deemed to have elevated privileges of the *NETADMIN* [*Network Administrator*] type may also inherit associated *FIREWALL* and/or *ROUTER* entitlements on a particular FISMA system.
- An agency has identified a unique **PRIVType** that accounts for its PRIV for its cloud infrastructure. Associated with this *AGENCYDEFINED* PRIV, the agency creates an entitlement of type *IaaS* to indicate that the account with this PRIV has elevated rights to infrastructure-as-a-service (IaaS) resources in the public cloud. (See **Entitlement** in the Data Dictionary for the Logical Data Model section.) [CDM PMO]
- An agency has implemented Microsoft Active Directory, which authoritatively controls, through security groups, administrative access to clustered hypervisors that support an agency's virtual infrastructure.

[20] For a comprehensive listing, please refer to the program's baseline of requirements for CDM capabilities.

The entitlement may be the enumerated names and description of these security groups—for example, "SecurityGroup-vCenter_DataCenterAlpha," "Grants super administrative privileges to entire VMWare cluster in Data Center Alpha."

Facility – For the purposes of the CDM program, facilities are any physical space (site, campus, building, etc.) that can be documented to facilitate the assignment of geographical information for agency personnel or FISMA system components (e.g., devices, software, etc.) for physical asset accountability. Facilities can be official duty stations, datacenters, or some combination of both. In the CDM Data Model, facilities may also be interrelated, such that a larger facility holds and is related to a more specific locale that is more informational for documenting an asset's physical location (e.g., a server room or datacenter inside an agency's campus location). When the physical location of assets is fluid, as is the case with cloud services, provider-related information (e.g., company name, specific information on hosting agreements) may be provided. Facilities may be agency owned/operated or provided as a service through a hosting agreement. Under CDM, all colocation, contractor owned/operated, and cloud hosting providers* should be documented if they are relevant to people or devices covered by CDM.

**Note:* In many circumstances under shared services (e.g., cloud providers), it might not be realistic to document actual geographical location. In these scenarios, it is critical to capture not the physical location, such as an address, but rather the organizational information of the hosting company and any related geographic information on the location of the hosting center, which may vary by vendor. For example, "AWS GovCloud™," "US-EAST Region" would be an appropriate moniker for virtual servers that are hosted by AWS on behalf of an agency.

Federal Vulnerability Action (FVA) – The FVA factor is a key part of the AWARE risk posture scoring algorithm. It encourages agency action on open vulnerabilities by employing a weight factor on a CVE due to a heightened threat level for that CVE, per federal guidance. DHS will provide the user actor for such FVA determinations, which will occur at the federal dashboard, as well as influence scores for agency dashboards. [AWARE Technical Design]

FIPS 199 Impact Components: The generalized format for expressing the security category (SC) of an information system (IS): SC information system = [(confidentiality, impact), (integrity, impact), (availability, impact)]. (See **ImpactLevel** in the Data Dictionary for the Logical Data Model section.) [FIPS Pub 199, 44 U.S.C., SEC. 3542] [CDM PMO]

- **Availability** – The applicable FIPS 199 impact level used to indicate timeliness, reliability of access, and use of information within a FISMA system.
- **Confidentiality** – The applicable FIPS 199 impact level used to indicate the appropriate level of rigor to preserve authorized restrictions on information access and disclosure, including the means for protecting personal privacy and propriety information.
- **Integrity** – The applicable FIPS 199 impact level used to indicate protection necessary to guard against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

IAL/AAL – Identity Assurance Level (IAL) is a category that conveys the degree of confidence that a person's claimed identity is their real identity, as defined in NIST SP 800-63. IAL has three levels: IAL1 (Some confidence); IAL2 (High confidence); IAL 3 (Very high confidence). Authenticator Assurance Level (AAL) is a measure of the strength of an authentication mechanism and, therefore, the confidence in it, as defined in NIST SP 800-63. AAL has three levels: AAL1 (Some confidence); AAL2 (High confidence); AAL3 (Very high

confidence). When combined, IAL3/AAL3 represents the assurance levels associated with a PIV card. In the future, the CDM solution will be capable of ingesting, analyzing, and documenting different IAL/AAL levels independently, as applicable, to identify and access management data. [NIST SP 800-63-3]

Incident [On Network] – Incidents are formally defined by NIST as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices… ," [NIST 800-61]. The CDM architecture follows this guidance and requires agencies to codify any "cyber"[21] incident that is suspected or confirmed within the boundary of an agency's network. The enumeration of the context of each incident is driven by associated attributes derived from federal guidance (i.e., CISA Federal Incident Notification Guidelines, NIST 800-61r2) and further enriched with strategic information sourced from other industry standards, such as Veris, Malware Attribute Enumeration and Characterization (MAEC)™, Common Attack Pattern Enumerations and Classifications (CAPEC)™, and others. Incidents are typically populated from data that is sourced from correlated events (**EventOnNetwork**). This data can indicate network activity that may be unauthorized, malicious, or otherwise in violation of explicit IT policy. Correlated events may be facilitated by automation or manual attribution to incidents, but when possible, should be associated and reported as part of the detailed contextual information of each incident. The CDM architecture is primarily focused on documenting incidents from a strategic perspective, including leveraging the necessary entities and attributes to satisfy all federal requirements relating to reporting to DHS and other federal oversight bodies. [CDM Technical Capabilities, Vol. 2]

Industrial Control Systems (ICSs) – A general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other control system configurations, such as programmable logic controllers (PLCs) often found in industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). ICS is associated with OT.

Internet of Things (IoT) – User or industrial devices that are connected to the internet. IoT devices include sensors, controllers, and household appliances. IoT devices have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. The IoT devices and related definitions have evolved over time, originally including non-industrial devices, but now seemingly including industrial OT devices that are connected to the internet (IoT) as well.

Interrogation Specification – A specification that can be automated in some way and is in a formal language that describes how a data interrogation action should interact with the CDM data. It produces datasets that fulfill a fundamental data request with a consistent result for the CDM program (e.g., discover unauthorized assets). Interrogation specifications are derived from various cybersecurity-relevant artifacts including, but not limited to, CDM program requirements, common federal yearly reported metrics (i.e., FISMA metrics), NIST publications, and other federal requirements (e.g., FIPS). See Appendix A for more information. [CDM PMO]

Known Exploited Vulnerabilities (KEVs) – For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the Known Exploited Vulnerability (KEV) catalog, the authoritative source for vulnerabilities that have been exploited in the wild. CISA strongly recommends all organizations review and monitor the KEV

[21] The CDM program currently as scoped includes reportable incidents that are only "cybersecurity related." This includes incidents that are germane to computer systems and networks as generally attributable to human-caused threats (e.g., malicious actors, human errors) and not natural disasters, power failures, etc.

catalog and prioritize remediation of listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

Local Account [**Local System Account**, **Local Users**]: An account that is predefined locally on a device, commonly to execute or run a defined service (e.g., service account) with some set of privileges on that device. Local accounts are typically not centrally managed, granting access to individual devices exclusively with authentication and authorization decisions adjudicated by the device itself.

"Managed" Application: A managed application is a construct within the CDM solution that allows for the separation of accountability between specific installed software (e.g., actively managed applications) and other aspects of the supporting device or infrastructure in order to provide more granular risk tracking and reporting. Analogous to a type of information system "component" as defined by the NIST RMF, managed applications support the need to implement "split responsibilities" between software and their devices (or supporting infrastructure) when deemed appropriate by an agency. In the CDM LDM, this functionality is achieved by creating a logical entity (**ManagedAppOnNetwork**) that captures discrete instances of installed software detected on devices under a common namespace to facilitate unique identification and subsequent risk assignment. The specifications for each managed application are constructed and inventoried based on agency governance and policy. The **ManagedAppOnNetwork** entity has the same organizational and system boundary traceability requirements as a traditional device in the CDM LDM. [CDM PMO]

"Managed" Device – A device is considered managed within the CDM solution if it satisfies both of the following conditions:

- Has an identified information system owner for the associated system boundary of the device
- Has an assigned OU tag (i.e., assigned to an OU container, facilitating GFE status)

Agency policy dictates how devices are associated with information system boundaries, and this association will indirectly allow information system owner assignments, presumed to be one-to-many, to devices to occur. Assigning responsible and accountable parties to devices is one of the fundamental needs for addressing security deficiencies and helps ensure proper oversight and governance. The information "system owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system."[22] Any device that does not have this key party assigned (including lack of an OU boundary assignment) is considered "unmanaged." (See **OrganizationalUnitBoundary** and **SystemBoundary** in the Data Dictionary for the Logical Data Model section for further clarification.) [CDM PMO]

Misconfiguration – A configuration that is discovered, through interrogation of a device, to be in violation of the expected value(s) as specified by parameters for that configuration in the CCEDictionary. [CDM PMO]

Multifactor Authentication (MFA) – An authentication process that requires multiple response inputs drawing on a variety of personal factors, namely:

- Something you know (e.g., personal identification number [PIN] or password)
- Something you have (e.g., PIV card or token)
- Something you are (e.g., biometrics)

For CDM Data Model context, MFA is critical in providing levels of assurance for account authentication (and associated privileges) and is germane for credential management, as proper IAL/AAL credentials are

[22] NIST, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Risk for Security and Privacy," NIST SP 800-37r2, December 2018, https://csrc.nist.gov/pubs/sp/800/37/r2/final.

commonly used to meet MFA requirements. [CDM PMO]

Network Access Protection [Network Access Control (NAC)] – Network access protection is the formal name of the technical capability that falls within the BOUND-F suite of network-based controls. In the context of this document, the terms network access control (NAC) and network access protection are equivalent. They relate to a capability that ensures a device is allowed/permitted to connect and access resources on an enterprise network only if that device is "compliant" or satisfies some set of agency policies that are implemented in a CDM tool/sensor (i.e., NAC tool) that is actively performing validation against those policies. Examples of these policies include updated software patches being installed, antivirus signatures being up to date, nonexistence of certain vulnerabilities, etc. The NAC tool may take proactive measures (BLOCK or QUARANTINE) predicated on a device's compliance. [CDM Technical Capabilities, Vol. 2]

Network Account – An account that provides access to an agency's network and information system(s). A network account is characterized by an enterprise centralized account management system that mediates authentication and authorization activities. Examples are Kerberos for Microsoft's Active Directory-centric networks or RADIUS protocol on other centrally authenticated networks. [CDM PMO]

(***Note:*** *"Network Account" is not necessarily inclusive of the large variety of accounts that operate within the boundaries of a given network and might be under control of a single sign-on solution*.)

NIST Security Control [Security control] – The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. [NIST 800-53 r5]

Non-Person Entity (NPE) – An autonomous service, application, or device that may be granted a CRED in order to accomplish a necessary function within an agency. An NPE can facilitate documentation of an account that is intended for use by a system/application (i.e., service account) to either accomplish some necessary function or provide a group service that does not require a person to actively manage or log in to use, such as a group mailbox. (See **UserType** in the Data Dictionary for the Logical Data Model section.) [FISMA FY20 CIO, CDM PMO]

Organizational Unit (OU) – An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or any of its operational subcomponents, such as an operational division or bureau). (See **OrganizationalUnitBoundary** in the Data Dictionary for the Logical Data Model section.) [NIST SP 800-53; SP 800-53A; SP 800-37] [CDM PMO]

Personal Identity Verification (PIV) – Physical artifact (e.g., identity card, smart card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable). The federal standard for this is specified as FIPS 201. (See **CREDType** in the Data Dictionary for the Logical Data Model section.) [FY 2021 CIO FISMA Metrics]

PRIV – PRIV in the CDM Data Model represents *elevated* privileges (i.e., above the baseline set for users) for physical or logical *infrastructure* resources that employ access restrictions. PRIV elements collectively describe what levels of elevated privileges are employed by an account on a system. PRIV types in the CDM Data Model are "network/infrastructure or enterprise" in scope and have been specified in the model. Agencies may specify a more specific/distinct variation of an infrastructure PRIV that is not present in the model. (See **PRIVType** in the Data Dictionary for the Logical Data Model section.) [CDM PMO]

Privileged Network Account – A network account with elevated privileges; typically allocated to system administrators, network administrators, and others who are responsible for system/application control, monitoring, or administration functions. (See **AccountType** in the Data Dictionary for the Logical Data Model section.) [FY 2021 CIO FISMA Metrics]

Relying Party (RP) (aka Service Provider [SP]) – An entity that relies upon the subscriber's authenticator(s) and credentials, or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system. (NIST SP 800-63-3)

Response Activity – Various stages and activities are included in the incident response lifecycle, including the following:

- Detection and analysis
- Containment
- Eradication
- Post-incident activities (e.g., lessons learned)

To facilitate holistic reporting under CDM, agencies are asked to detail, to the fullest extent possible, these activities using the related data attributes under the **ResponseActivity** entity. The model also requires associating agency resources who would serve as lead personnel in either an execution, oversight, and/or accountability role in relation to these activities. Ideally, a collection of well-documented response activities can be used to construct a cradle-to-grave timeline of agency actions in response to a specific incident on an agency's network. [NIST 800-61r2]

Robotic Process Automation (RPA) – A low- to no-code COTS technology that can be used to automate repetitive, rules-based tasks. [RPA Program Playbook v1.1 (digital.gov)]

Shared Account – An account that is utilized by a group rather than an individual person. Shared accounts are not associated with a particular person. In the CDM Data Model, shared accounts are discovered through the documentation of associating CRED, which allows authentication to a specific account to more than one user record (MUR). [FISMA FY20 CIO, CDM PMO]

Shared Secret – A secret used in authentication that is known to the subscriber and the verifier. (NIST SP 800-63-3)

Summary Data – The product used by DHS to facilitate assessment of cybersecurity risk across the federal enterprise. Derived from data in the CDM agency dashboard, this is intended to be "aggregated summary" information that precludes the need to send object-level data to DHS. Summary data is a summarization of the gathered datasets from CDM architectural layers A through C; datasets should generally avoid attribution to an individual device or user. [CDM PMO]

System [FISMA System, FISMA Container] – A boundary including all components of an information system to be authorized for operation by an authorizing official, excluding separately authorized systems, to which the information system is connected. A system may include one or multiple **subsystems**, where there is a need to divide complex systems into a set of manageable system elements or identify those elements that support a similar mission but are sufficiently distinct to be identified separately.[23] A system is also commonly referred to

[23] NIST, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Risk for Security and Privacy," NIST SP 800-37r2, December 2018, https://csrc.nist.gov/pubs/sp/800/37/r2/final.

as a FISMA System. (See **SystemBoundary** and **SystemBoundaryID** in the Data Dictionary for the Logical Data Model section.) [CNSSI-4009; NIST SP 800-53; SP 800-53A; SP 800-37] [CDM PMO]

TRUST – In the CDM Data Model, TRUST reflects collected data attributes that document agency processes attempting to reduce the probability of loss in availability, integrity, and confidentiality of data by capturing that only properly identity-proofed and vetted users are given access to systems through accounts and their associated privileges. TRUST is directly tied to users through the User element (i.e., MUR) and allows CDM users to clearly document the relevant TRUST processes executed, including background investigations, non-disclosure agreements, suitability processes, and contractor vetting processes. TRUST should be clearly assigned to users after identity-proofing and ideally is positively adjudicated before subsequent credentialing and account provisioning occurs. TRUST elements provide the agency visibility into the risk associated with the vetting of users for privileged access. (See **TRUST** in the Data Dictionary for the Logical Data Model section.) [CDM PMO]

Unique Identifiers (UIDs) [*EntityName*ID] – Identifiers (also interpreted as primary keys and index values) that enable a record, entity, or other inventoried item to be singled out by referencing the UID value in a query or search. In the CDM Data Model, various entities leverage the UID concept and the implied requirement to be uniquely identifiable by a referential attribute (e.g., The **SystemBoundaryID** attribute shall uniquely identify a FISMA system). [CDM PMO]

Unique Software – An inventory item that represents a formally named software product, which is an abstract encapsulation of a unique application or codebase found on an agency's network that can actively run (i.e., access/utilize memory space, create central processing unit [CPU] tasks/threads) on an IT hardware asset. A software product may be composed of multiple ancillary items, such as software component files (e.g., code libraries, dynamic-link libraries [DLLs], scripts, multiple .exe, .rar, .rpms). Unique software records can be discovered either from automated sensors (e.g., CDM-provided SWAM tools) or from other authoritative software inventory sources providing relevant information about software that exists within an agency's boundary (e.g., logistics database, configuration management databases, license management software systems). (See **UniqueSoftware** in the Data Dictionary for the Logical Data Model section.) [CDM Technical Capabilities, Vol. 2] [CDM PMO]

User – An entity that is used in the CDM Data Model as an authoritative record of information for any particular person (or non-person) entity within the agency's purview. The User entity serves as an anchor for the MUR, which aggregates critical CDM attributes, such as provisioned credentials (**CRED**), adjudicated vetting processes (**TRUST**), and agency stipulated user training (**BEHAVE**). (See **User** in the Data Dictionary for the Logical Data Model section.) [CDM PMO]

4 DATA DICTIONARY FOR THE LOGICAL DATA MODEL

This section contains the attributes and entities within the CDM LDM provided as GFI to CDM stakeholders. It is intended to clarify the information requirements of each attribute, as called out by the model. Note that all data is implicitly expected to be provided by the CDM solution unless otherwise specified. If data is optional or not available, the CDM solution can produce a default representation of a NULL or EMPTY value as appropriate. However, in cases where the data attribute is required, a NULL value may constitute a defect (i.e., unassigned values for required attributes that are necessary for evaluating an expression will be considered a potential defect). Principal source materials used in derivation of these entities and attributes are noted in brackets (e.g., [CDM PMO] indicates that mission requirements and/or derived needs are principally used in producing this data element). **Recall from Section 2.15 that all data elements that are not required or conditionally required are recommended.**

Account – An entity that represents the means by which a user (a person or non-person entity) can access a system. (See **Account** in Data Model Key Terms for additional context). [CDM PMO] [REQUIRED]

AccountCreationDate – An attribute that captures the date an account was created. [CDM PMO]

AccountExpirationDate – An attribute that captures the date an account is due to expire. [CDM PMO] [REQUIRED] (***Note***: *This attribute should be updated when accounts are "renewed" or "reauthorized" as part of a recurring review process.*)

AccountID – An attribute that captures a universally unique identifier referencing a specific account on a physical or logical system. [CDM PMO] [REQUIRED]

AccountName – An attribute that captures an agency-specified common name for each created account instance captured by the CDM system (e.g., "John Doe-Account on GSS123"). [CDM PMO]

AccountReviewDate – An attribute that captures the last date an account review was known to be conducted. [CDM PMO] [CONDITIONALLY REQUIRED]

AccountReviewGracePeriod – An attribute that captures a period of time, in days, indicating the agency-defined periodicity for account reviews, such that when it is exceeded by **AccountReviewDate**, some agency-defined action is required, as dictated by policy (e.g., immediate review triggered or required, notification to security office). [CDM PMO]

AccountStatus – An attribute that captures the last reported status of an account. Values for this attribute shall only be one of the following:

- ENABLED
- DISABLED
- EXPIRED
- LOCKED

[CDM PMO] [REQUIRED]

AccountStatusGracePeriod – Captures the agency-determined length of time, in days, the **AccountStatus** attribute is allowed to remain in any status, beyond which some action is recommended where applicable, as determined by agency policy (e.g., amount of time agency allows an account to remain in EXPIRED status before the account is DISABLED). [CDM PMO]

AccountType – An attribute that captures the privilege scope and applicability of an account within an agency. Values for this attribute shall be only one of the following:

- PRIVILEGED NETWORK
- PRIVILEGED LOCAL
- UNPRIVILEGED NETWORK
- UNPRIVILEGED LOCAL

[CDM PMO] [REQUIRED]

DateAccountStatusInitiated – An attribute that captures the date when an **Account** entity's (specific account instance) status last underwent any of the following events:

- Any change of state (e.g., from ENABLED to LOCKED, LOCKED to DISABLED) including:
  - Date when **Account** is first provisioned or discovered

[CDM PMO] [REQUIRED]

BEHAVE – An entity that represents the means by which CDM stores and represents information on appropriate security-related behavior, such as fulfilling training, certification, or knowledge-based requirements. (See **BEHAVE** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

BEHAVECreationDate – An attribute that captures the date BEHAVE was originally created/tracked. [CDM PMO]

BEHAVEDescription – An attribute that captures the description of the salient characteristics of a specific security-related **BEHAVE** element (e.g., "Yearly mandated information security training for administrators"). [CDM PMO]

BEHAVEExpirationDate – An attribute that captures the date upon which a security-related **BEHAVE** entity (e.g., Record of Completed Training) becomes invalid. [CDM PMO] [REQUIRED] (***Note:*** *This attribute should be updated when* ***BEHAVE*** *is "renewed" or "recompleted" as part of a recurring process.*)

BEHAVEID – An attribute that captures a universally unique identifier that references an appropriate security-related **BEHAVE** element. (See **BEHAVE** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

BEHAVEName – An attribute that captures an agency-specified common name for each **BEHAVE** instance captured by the CDM system (e.g., "Annual Windows Server System Administration Refresher"). [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because some agencies may not maintain a common name.)*

BEHAVEReviewDate – An attribute that captures the last known date a **BEHAVE** review was conducted. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because review date has not yet happened at some agencies.)*

BEHAVEReviewGracePeriod – An attribute that captures a period of time, in days, indicating the agency-defined periodicity for **BEHAVE** reviews, such that when it is exceeded by **BEHAVEReviewDate**, some agency-defined action is required, as dictated by policy (e.g., immediate review triggered or required, notification to security office). [CDM PMO]

BEHAVEStatus[24] – An attribute that describes the current status of the security-related **BEHAVE** element. Valid values must be one of the following:

- COMPLETED – **BEHAVE** is current, completed.
- PENDING (a temporary status) – **BEHAVE** has been assigned, is within grace period, or is otherwise in the process of being completed.
- INCOMPLETE – **BEHAVE** has not been fully completed.
- EXPIRED – **BEHAVE** has expired.

[CDM PMO] [REQUIRED]

BEHAVEStatusGracePeriod – An attribute that captures the agency-determined length of time, in days, the **BEHAVEStatus** attribute is allowed to remain in any status, beyond which some action is recommended where applicable, as determined by agency policy (e.g., amount of time agency allows a user to renew or complete **BEHAVE** requirement per agency policy for a privileged user, amount of time agency allows **BEHAVE** to be EXPIRED before account is LOCKED).[25] [CDM PMO]

BEHAVEType – An attribute that captures the class of a security-related **BEHAVE** element, which shall have only one of the following values:

- CSAT (Cybersecurity Awareness Training) – As stipulated by FISMA metrics
- PHISHING – Agency-conducted phishing exercises, as stipulated by FISMA metrics
- ROLE TRAINING – Role-based security training as defined by agency policy to fulfill FISMA requirements
- KNOWLEDGE – Training or other event that increases skill set, knowledge building
- CERTIFICATION
- AGENCY OTHER – Training not otherwise explicitly listed above, including specialized purpose training requirements as determined by agency policy or routine general user training, such as entry on duty (EOD) security awareness training, rules of behavior training, etc.

[CDM PMO] [REQUIRED]

DateBEHAVEStatusInitiated – An attribute that captures the date when a **BEHAVE** entity's status (specific instance of a user's training) last underwent any of the following events:

- **Any** change of state (e.g., from COMPLETED to EXPIRED, PENDING to INCOMPLETE), including:
  - Date when **BEHAVE** is first COMPLETED or first classified as PENDING.
  - "Re-COMPLETED" (i.e., **BEHAVE** requirement(s) have been re-satisfied whereby the state remains "COMPLETED" but new date data is acquired through updating the **DateBEHAVEStatusInitated** attribute with a new date).

[CDM PMO] [REQUIRED]

[24] Initially, the BEHAVE capability identifies users that have not successfully completed the appropriate security training. This can easily be adapted to identify unsuccessful demonstration (via testing) of learned knowledge objectives.

[25] It is common to have a grace period in which a person is authorized for access, given an account, and given a number of months to complete the required training. In these instances, it is important to monitor whether the requirement has been met by the end of the grace period.

CCEDictionary – An entity that represents a specific device configuration that has relevant IT security implications for agencies. [CDM PMO] [REQUIRED]. (***Note***: *The CDM PMO configurations that will be required for scoring and summary reporting to the federal dashboard will be disseminated as a set of* **CCEDictionary** *entities along with each entity's respective attributes through the dashboard-to-dashboard communication flow. For additional information, refer to the* *CVE and CCE Dictionaries section*.)

BenchmarkSettingsCount – An attribute that captures the number of discrete DISA STIG CAT 1 benchmark checks exclusively associated with AWARE CSM scoring in a given benchmark, which would be compared with **CSMSettingsCount** to help identify potential data quality problems. [CDM PMO] [REQUIRED]

BenchmarkName – An attribute that captures the DISA STIG CAT 1 benchmark name. [CDM PMO] [REQUIRED]

BenchmarkRelease – An attribute that captures the DISA STIG CAT 1 benchmark release. [CDM PMO] [REQUIRED]

BenchmarkVersion – An attribute that captures the DISA STIG CAT 1 benchmark version. [CDM PMO] [REQUIRED]

CCEAlternateID – An attribute that captures an alternate identifier for identification of the security-relevant configuration item (e.g., manufacturer, agency-defined UID). [CDM PMO]

CCEDictionaryUpdateDate – An attribute that captures the date that the **CCEDictionary** data entry was last modified. [CDM PMO] [REQUIRED]

CCEID – An attribute that captures a universally unique identifier assigned to a specific configuration setting, which may be associated with a discovered configuration deficiency that is present on a device within the inventory of an agency. (See **CCE** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

CCEProvidedDescription – An attribute that captures the general description of the configuration that is being audited as specified by an external source, such as the National Checklist Program (NCP) repository, DISA, or similar. [CDM PMO] [REQUIRED]

> ***Sample Value:*** *"Allowing anonymous logon users (null session connections) to list all account names and enumerate all shared resources can provide a map of potential points to attack the system."*

CCEProvidedFix – An attribute that captures the recommended hardened configuration as specified by an external source, such as the NCP repository, DISA, or similar (e.g., Fix Text). [CDM PMO] [REQUIRED]

> ***Sample Value:*** *"Set the following Group Policy setting to Enabled. Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network Access: Do not allow anonymous enumeration of SAM accounts and shares."*

CCEProvidedParameters – An attribute that captures the machine-level configuration parameters that are checked as part of successful verification of the configuration setting (e.g., registry keys, permission settings). [CDM PMO] [REQUIRED]

> ***Sample Value:***
> *"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous"*

CCEPublishedDate – An attribute that captures the original date the **CCE Dictionary** entry was codified or published. [CDM PMO] [REQUIRED]

CCEScore – An attribute that captures a "Standardized Configuration Score" as assigned by the CCE Dictionary. [AWARE Technical Design] [REQUIRED]

CCESource – An attribute that captures the source of the **CCEDictionary** entry (configuration settings) as being established by either FEDERAL or AGENCY. (See **Benchmark** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

Certificate – An entity that captures the associated information of a digital certificate, which minimally includes (1) identifying the certification authority issuing it, (2) naming or identifying its subscriber, (3) including the subscriber's public key, (4) identifying its operational period, and (5) including whether it is digitally signed by the certification authority issuing it. [NIST SP 800-32] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because some agencies may not have access to the **Certificate Management** security capabilities **[BOUND-E]** necessary to produce this data; therefore, the data is required only for certain CDM solutions that employ **Certificate Management**.)*

CertificateCA – An attribute that captures the name of the certificate authority (CA). The CA confirms the identities of parties sending or receiving the electronic communications. [NIST SP 800-32] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

CertificateCreatedDate – An attribute that captures the date of certificate creation. [CDM PMO]

CertificateDescription – An attribute that captures mission/operational usage information (e.g., "supports TLS for ABOE.gov," "supports mission system XYZ"). [CDM PMO]

CertificateDistinguishedName – An attribute that captures a sequence of relative distinguished names (RDNs) of the entry, which represents the object and those of all of its superior entries (in descending order). Each RDN is a set of one or more attribute type and value pairs expressed as a type/value pair. [CDM PMO and ITU-T Rec-X.501-2016]

CertificateExtendedKeyUsage – An attribute that captures the information relating to one or more purposes for which the certified public key may be used, in addition to, or in place of, the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates (e.g., "Server Authentication" OID 1.3.6.1.5.5.7.3.1). [RFC 5280]

CertificateFQDN – An attribute that captures the fully qualified domain name of a certificate, if applicable. A FQDN is a domain name that includes the labels of all superior nodes in the internet Domain Name System (DNS). [CDM PMO]

CertificateID – An attribute that captures a unique identifier for a certificate. For instance, this could be based on the serial number and issuer name fields. [CDM PMO] [CONDITIONALLY REQUIRED] (*Note: See above for explanation of "conditionally required.")*

CertificateIssuer – An attribute that captures the name of the certificate issuer or "SELF-SIGNED" value. The issuer is the distinguished name of the trusted third party that generated the certificate. [CDM PMO, NIST SP 800-32]

CertificateKeyUsage – An attribute that captures the set of generic uses for the key. For users or systems, the key may be used for digital signatures on documents, authentication, key management, or data encipherment. For CAs, the key may be used for verifying signatures on certificates or certificate revocation lists (CRLs). This field can be extracted from the X.509 Key Usage certificate

extension field. This attribute may have one or more of the following values:

- DIGITALSIGNATURE
- NONREPUDIATION
- KEYENCIPHERMENT
- DATAENCIPHERMENT
- KEYAGREEMENT
- KEYCERTSIGN
- CRLSIGN
- ENCIPHERONLY
- DECIPHERONLY

[NIST SP 800-32]

CertificateLastReportingDate – An attribute that captures the date of the last (most recent) certificate check. [CDM PMO]

CertificatePublicKeySize – An attribute that captures the size (in bits) of the certificate public key. [CDM PMO]

CertificateRiskStatus – An attribute that captures a Boolean value that indicates whether one or more certificate defects have been detected for the inventoried certificate that may put an agency's infrastructure at risk. [CDM PMO]

CertificateSignatureAlgorithm – An attribute that captures the algorithm used to sign the content using the private key. [CDM PMO]

CertificateSignatureHashAlgorithm – An attribute that captures the algorithm used to hash the certificate content before signing; this is used in certificate path construction. [CDM PMO]

CertificateSubject – An attribute that captures the "subject" field of the certificate, which details the entity named in the certificate. [CDM PMO, NIST SP 800-32]

CertificateSubjectAlternateName – An attribute that captures the subject alternative name for a certificate. The subject alternative name extension is used to provide other name forms for the owner of the private key, such as DNS names or email addresses. [NIST SP 800-32]

CertificateSubjectCommonName – An attribute that captures a certificate's subject common name; this is typically composed of host plus domain name (e.g., www.dhs.gov). [CDM PMO]

CertificateValidFromDate – An attribute that captures the "Valid from" date of a certificate. [CDM PMO]

CertificateValidToDate – An attribute that captures the "Valid to" date of a certificate. [CDM PMO]

CertificateDefectCondition – An entity that represents a single discovered certificate-related defect that can be analyzed by the agency for risk determination. Certificate defects are based on certificate parameters not aligned with industry best practices and/or agency certificate polices (as found and reported by the certificate management tool/sensor) that need to be addressed. [CDM PMO]

CertificateDefectConditionID – An attribute that captures a unique identifier for a certificate defect condition, represented by the **CertificateDefectCondition** entity. [CDM PMO]

CertificateDefectDetail – An attribute that captures the certificate risk(s) (indicated by **CertificateRiskStatus**) into well-formed categories, including one or more of the following types of certificate risks:

- EXPIRING CERTIFICATES
- INVALID PERIOD
- EXPIRED PERIOD
- FAILED VALIDATION
- INVALID DOMAIN NAME
- UNAPPROVED ISSUER
- SELF-SIGNED CERTIFICATE
- UNAPPROVED SIGNING ALGORITHM
- UNAPPROVED HASHING ALGORITHM
- UNIQUE NAME VIOLATION
- WEAK PUBLIC KEY SIZE
- WEAK SIGNING ALGORITHM
- OTHER (as specified)

[CDM PMO]

CertificateDefectDiscoveryDate – An attribute that captures the date when the certificate defect was first discovered. [CDM PMO]

CertificateDefectException – A Boolean attribute that captures the existence of a defect exception, if applicable, to a related certificate defect. [CDM PMO]

CertificateDefectExceptionDescription – An attribute that captures the justification or rationale associated with an agency's exception(s) to detected certificate defect. [CDM PMO]

CRED – An entity that represents an object that authoritatively binds an identity to a token possessed and controlled by a user for purposes of providing a level of assurance to grant logical or physical access. (See **CRED** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

CREDCreationDate – An attribute that captures the date **CRED** was originally issued/tracked. [CDM PMO]

CREDDescription – An attribute that captures a description of the salient characteristics of a specific security-related **CRED** element (e.g., "Standard agency PIV card issued to employees"). [CDM PMO]

CREDExpirationDate – An attribute that captures the date upon which an issued **CRED** entity becomes invalid. [CDM PMO] (***Note:*** *This attribute should be updated when* ***CRED*** *are "renewed," "reissued," or "reauthorized" as part of a recurring review process.*)

CREDID – An attribute that captures a universally unique identifier that references a specific **CRED**

element. [CDM PMO] [REQUIRED]

CREDName – An attribute that captures an agency-specified common name for each **CRED** instance captured by the CDM system (e.g., "DOD CAC – USCG," "OTP Token Generator v3.1"). [CDM PMO]

CREDReviewDate – An attribute that captures the last known date a **CRED** review was conducted. [CDM PMO] [CONDITIONALLY REQUIRED]

CREDReviewGracePeriod – An attribute that captures a period of time, in days, indicating the agency-defined periodicity for **CRED** reviews, such that when it is exceeded by **CREDReviewDate**, some agency-defined action is required, as dictated by policy (e.g., immediate review triggered or required; notification to security office). [CDM PMO]

CREDStatus – An attribute that captures the last reported status of a **CRED** element, which shall be only one of the following values:

- PENDING
- ISSUED
- SUSPENDED
- EXPIRED
- REVOKED

[CDM PMO] [REQUIRED]

CREDStatusGracePeriod – An attribute that captures the agency-determined length of time, in days, the **CREDStatus** attribute is allowed to remain in any status, beyond which some action is recommended where applicable, as determined by agency policy (e.g., amount of time allowable for a **CRED** to remain in SUSPENDED status before it is formally REVOKED; amount of time **CRED** is allowed to be in an EXPIRED state before accounts are DISABLED). [CDM PMO]

CREDType – An attribute that captures the class of a **CRED** element inventoried by the CDM system. Values for this attribute shall be only one of the following:

- USERID PASSWORD
- PIV CARD (IAL/AAL 3)
- DERIVED PIV (AAL2)
- DERIVED PIV (AAL3)
- BIOMETRIC
- CAC CARD
- AAL3CREDENTIAL
- AGENCY OTHER

[CDM PMO] [REQUIRED]

DateCREDStatusInitiated – An attribute that captures the date when a **CRED** entity's status (specific instance of a **CRED**) last underwent any of the following events:

- **Any** change of state (e.g., from ISSUED to EXPIRED, EXPIRED to ISSUED), including:

- Date when **CRED** is first ISSUED or first classified as PENDING.
- RE-ISSUED (i.e., renewed whereby the state remains ISSUED but new date data is acquired through updating the **DateCREDStatusInitated** attribute with a new date).

[CDM PMO] [REQUIRED]

CVEDictionary – An entity that represents authoritative information for the CDM solution for a specific, referenced CVE. [CDM PMO] [REQUIRED] (***Note***: *The vulnerabilities that will be required to be discovered, inventoried, and summarily reported to the federal dashboard will be disseminated as a set of* **CVEDictionary** *entities, along with each entity's respective attributes, through the dashboard-to-dashboard communication flow. For additional information, refer to the CVE and CCE Dictionaries section.*)

CVEDescription – An attribute that captures the general description of the vulnerability as specified by an external source, such as the NVD. [CDM PMO] [CDM PMO] [REQUIRED]

> ***Sample Value:*** *"/usr/ucb/ps in Sun Microsystems Solaris 8 and 9, and certain earlier releases, allows local users to view the environment variables and values of arbitrary processes via the -e option."*

CVEDictionaryUpdateDate – An attribute that captures the date that the **CVEDictionary** data entry was last updated. [CDM PMO] [REQUIRED]

CVEID – An attribute that captures a universally unique identifier assigned to a specific vulnerability, as defined by its relevant CVE (i.e., Assigned CVE Identification), which is associated with a discovered vulnerability in software that is present within the inventory of an agency. (See **CVE** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

CVEPublishedDate – An attribute that captures the original date the CVE dictionary entry was codified or published. [CDM PMO] [REQUIRED]

CVEReferences – An attribute that captures any external uniform resource locators (URLs)/uniform resource identifiers (URIs) that add more contextual information around the CVE, such as reference links to a software manufacturer's website or a security bulletin. [CDM PMO]

CVEScore – An attribute that captures the scoring parameter as determined by the CDM program and provided by the CVE dictionary (i.e., CVSS Score v2 and/or v3). [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because NVD may maintain some CVEs with no scores; otherwise required.)*

CVEType – An attribute that captures the type of vulnerability, currently defined as the Common Weakness Enumeration Identifier(s) (CWE IDs), under which the CVE is categorized. [CDM PMO]

FVAStatus – A Boolean attribute that captures whether a CVE is classified as an FVA. (See **Federal Vulnerability Action** in Data Model Key Terms for additional context.) [AWARE Technical Design] [REQUIRED]

FVAWeight – An attribute that captures, when a CVE is designated as an FVA, the additional weight factor that is applied to an open FVA vulnerability on an agency's network. This is a parameter that is implemented in the AWARE risk posture scoring methodology. (See **Federal Vulnerability Action** in Data Model Key Terms Data Model Key Terms for additional context.) [AWARE Technical Design] [REQUIRED]

KEVDateAdded – An attribute that captures the date the KEV was added to the catalog. [CDM PMO]

[CONDITIONALLY REQUIRED]

KEVDescription – An attribute that captures a brief description of the KEV. [CDM PMO] [CONDITIONALLY REQUIRED]

KEVDueDate – An attribute that captures the date the required action is due. [CDM PMO] [CONDITIONALLY REQUIRED]

KEVInCatalogue – An attribute that captures whether the KEV is present in the catalog. [CDM PMO] [CONDITIONALLY REQUIRED]

KEVRequiredAction – An attribute that captures the action required for mitigation. [CDM PMO] [CONDITIONALLY REQUIRED]

KEVNotes – An attribute that captures a link to notes provided for the KEV. [CDM PMO]

CyHyFinding – An entity that captures a specific CyHy reported vulnerability or finding detail. [CDM PMO] [REQUIRED]

CyHyClosedDate – An attribute that captures the date of finding (ticket) closure. [CyHy]

CyHyConfirmedAge – An attribute that captures the calculated age, in days, of a finding based upon the difference between the original discovery date of the finding and the last time the finding was scanned/detected. [CyHy]

CyHyCurrentAge – An attribute that captures the calculated age, in days, of a finding based upon the difference between the original discovery date of the finding and the current date. [BOD 19-02]

CyHyCVSSBaseScore – An attribute that captures the CyHy-provided CVSS base score (may be estimated for non-CVE findings based on CyHy-specific tool calculations). [CyHy]

CyHyDescription – An attribute that captures the informational description or explanation of a specific finding. [CyHy]

CyHyFindingID – An attribute that captures a unique identifier for a CyHy finding. [CDM PMO] [REQUIRED]

CyHyInitialDetection – An attribute that captures the time stamp (date/time) when the finding was first detected. [CyHy] [REQUIRED]

CyHyIPAddress – An attribute that captures the IP address (e.g., host) of the scanned device. [CyHy]

CyHyLatestDetection – An attribute that captures the time the CyHy scanner last detected a specific finding. [CyHy]

CyHyName – An attribute that captures the name of the specific finding (e.g., “Cross Side”) [CyHy]

CyHyOwner – An attribute that captures the organization that owns an IP address of a device associated with a finding. [CyHy]

CyHyPort – An attribute that captures the number of the vulnerable port. [CyHy]

CyHySeverity – An attribute that captures the (modified) CVSS v2.0 severity rating (includes critical). [CyHy] [REQUIRED]

CyHySolution – An attribute that captures the mitigation/fix to resolve a finding. [CyHy]

CyHySource – An attribute that captures the (tool) source of a finding (e.g., “Nessus”). [CyHy]

CyHySourceID – An attribute that captures the source-specific identifier of a finding (e.g., the scanner plugin identifier that detected the vulnerability). [CyHy]

DeviceInterface – An entity that captures an active device interface (or interfaces) using IP to communicate across an agency's network. [CDM PMO] [REQUIRED]

DeviceOnNetwork – An entity that captures information about hardware assets that are in scope for CDM. This entity is considered the fundamental record of the MDR construct. (See **DeviceOnNetwork** in Data Model Key Terms and the Master Device Records (MDR): Unique Identification of Hardware Devices section for additional context*). [Attach N 1.4.1]* [CDM PMO] [REQUIRED]

DateAssignedToSystemBoundary – An attribute that captures the date that a managed asset (i.e., device or managed application) was last assigned to a **SystemBoundary** (i.e., FISMA/Information System). [CDM PMO] [REQUIRED]

DateHardwareInventoryUpdated – An attribute that captures the date a hardware device's inventory information record was last updated with data from any source/tool/sensor that is relevant for discovery, scanning, or otherwise detecting hardware device data. (***Note***: *This attribute should reflect the last time that a hardware device was "seen" or updated through a discovery or scanning process, even if no values have changed since the last discovery*.) [CDM PMO] [REQUIRED]

DeviceAuthorizationStatus – An attribute that captures an agency's policy assessment of whether a device is authorized to be on a network. [CDM PMO] [REQUIRED]

DeviceAWARECSMSubScore – A **derived** attribute that captures the calculated secure configuration management AWARE risk posture sub-score (e.g., open misconfigurations/CCEs) associated with an agency device. [CDM PMO] [REQUIRED]

DeviceAWAREScore – A **derived** attribute that captures the calculated AWARE risk posture score associated with an agency device. [CDM PMO]

DeviceAWAREUAHSubScore – A **derived** attribute that captures the calculated unauthorized device AWARE risk posture sub-score (i.e., **unauthorized** as described above in Data Model Key Terms section) associated with an agency device. [CDM PMO] [REQUIRED]

DeviceAWAREVULSubScore – A **derived** attribute that captures the calculated vulnerability AWARE risk posture sub-score (e.g., open CVEs) associated with an agency device. [CDM PMO] [REQUIRED]

DeviceCategory – An attribute that captures the FISMA-defined device role of a discovered device within the CDM inventory. The values of this attribute are fixed and are defined by the CDM PMO. The valid values for **DeviceCategory** shall be **one**[26] and only one of the following values:

- ENDPOINT – Both physical and virtual endpoints
- NETWORKING DEVICE – Both physical and virtual
- OTHER INPUT/OUTPUT (I/O) DEVICE – Other I/O devices not explicitly called out
- IoT
- OT

[FY24 CIO FISMA Metrics] [REQUIRED]

[26] Devices that fall under multiple categories should be assigned only to the **one** category that best describes the asset.

DeviceEncrypted – An attribute that captures the status indicating whether all the device's relevant datastores are encrypted.[27] [CDM PMO] [REQUIRED]

DeviceFQDN – An attribute that captures the FQDN of a device. [CDM PMO] [REQUIRED]

DeviceIPvEnabled – An attribute that captures the device IP version status as .gov transitions to IPv6-only deployments. The values are one of the following:

- IPv4
- IPv6
- DUAL-STACK – Refers to deployments where IPv4 **and** IPv6 are enabled.

[CDM PMO]

DeviceManagedStatus – An attribute that captures the status indicating whether a device is managed or unmanaged. [CDM PMO] [REQUIRED]

DeviceModelVersion – An attribute that captures the specific model and version of a device (e.g., "Latitude E7250," "MacBook Air 13 2018"). [CDM PMO] [REQUIRED]

DeviceOnNetworkID – An attribute that captures a universally unique identifier that references a device discovered within the CDM inventory. The agency's CDM solution shall be able to search, locate, or otherwise identify an IT asset operating within an agency solely by querying by this attribute. The CDM PMO has no specific requirements on how to derive this attribute other than stipulating its uniqueness. This is the primary index value of the MDR construct. [CDM PMO] [REQUIRED]

Additional Context: See Master Device Records (MDR): Unique identification of Hardware Devices (Hardware UIDs) section.

DeviceOS – An attribute that captures the full name (i.e., name of OS, major version of OS, and release where applicable) of the primary OS of the device (e.g., Windows 10 64-bit, MacOS 11 [Big Sur], Windows Server 2019). [CDM PMO] [REQUIRED]

DeviceSpecialTypeWindowsActiveDirectoryServiceRunning – An attribute that captures a Boolean value for a device that has Windows Active Directory service running. [CDM PMO] [REQUIRED]

DeviceSpecialTypeWindowsExchangeServiceRunning – An attribute that captures a Boolean value for a device that has Windows Exchange service running. [CDM PMO] [REQUIRED]

DeviceSpecialTypeWindowsDomainNameServiceRunning – An attribute that captures a Boolean value for a device that has Windows Domain Name Service running. [CDM PMO] [REQUIRED]

DeviceStatus – An attribute that captures the relevant, current disposition of a device in the CDM inventory, as informed by CDM tools/sensors:

- ACTIVE – Device is in an active state on the agency's network as recently detected by a CDM tool/sensor.
- ACTIVE-VETTED – For agencies employing CDM's network access protection capability: Device has been vetted against agency policies by the CDM system upon establishing a connection

[27] For CDM, datastores that should be encrypted include any persistently (i.e., non-volatile) attached (i.e., fixed or embedded) storage that is likely to contain sensitive data whose unauthorized disclosure would likely result in a formal security incident (i.e., sensitive PII, agency mission/business data, etc.).

to the network, was allowed access, AND was recently inventoried and/or detected by any CDM tool/sensor.

- INACTIVE – Device has last seen timestamp of greater than > 14 calendar days and less than < 30 calendar days.
- QUARANTINED – For agencies employing CDM's network access protection capability: Device has been put into an isolated state by the CDM system and is pending some automated or manual intervention to remediate agency policy violations such as AV updates, vulnerability remediation/patching requirements, etc.; any device restricted by CDM's network access protection capability to anything less than full access to approved network resources is considered to be in a "QUARANTINED" state.
- BLOCKED – For agencies employing CDM's network access protection capability: Device was in violation of some set of agency polices and blocked from joining the network.
- STALE – Device is pending removal and has not been seen by the authoritative HWAM sensor in => 30 calendar days, yet is present in data store.

[CDM PMO] [REQUIRED]

DeviceType – An attribute that captures a sub-type that can be used to typecast devices to traditionally understood groupings, which may be one or more of the following values:

Sub-types of DeviceCategory: ENDPOINT

A. SERVERS – Mainframes, minicomputers, and midrange computers
B. WORKSTATIONS – Desktops, laptops, tablet PCs, and netbooks
C. SMARTPHONES – Other mobile computing devices
D. VIRTUAL MACHINES – Virtual machines or applications that can be addressed

Sub-types of DeviceCategory: NETWORKING DEVICE

A. MODEMS
B. ROUTERS
C. SWITCHES
D. BRIDGING DEVICES
E. GATEWAY DEVICES – to/from internet or other external networks
F. WIRELESS ACCESS POINTS
G. INTRUSION DETECTION SYSTEMS
H. INTRUSION PREVENTION SYSTEMS
I. FIREWALLS
J. NETWORK ADDRESS TRANSLATORS – NAT devices
K. HYBRID NETWORK ADDRESS TRANSLATORS (e.g., NAT routers)
L. LOAD BALANCERS

M. VPNs

N. ENCRYPTORS/DECRYPTORS

O. PUBLIC KEY INFRASTRUCTURE (PKI)

Sub-types of DeviceCategory: OTHERIODEVICE

A. PRINTERS – Plotters, copiers, multifunction devices

B. SCANNERS (including cameras)

C. FAX PORTALS

D. ACCESSIBLE STORAGE DEVICES

E. VOICE OVER INTERNET PROTOCOL PHONES

F. OTHER INFORMATION SECURITY MONITORING DEVICES

G. OTHER DEVICES ADDRESSABLE ON THE NETWORK

*(**Note:** DeviceType sub-types are not expected to yield new device data for a specified subtype.)*

[CDM PMO] [REQUIRED]

DeviceVendor – An attribute that captures the vendor (manufacturer) of a device (e.g., Dell Inc., HP Inc.). [CDM PMO] [REQUIRED]

EndpointSecurityUpdateDate – An attribute that captures the date a device's endpoint security product (e.g., endpoint protection platforms, audio-visual solutions) last received a security-relevant update (e.g., signature updates, DAT/definition file updates, threat indicator/pattern updates). [CDM PMO] [REQUIRED]

HighValueAssetFlag – An attribute that captures the flag indicating whether a device is a high-value asset or not. [CDM PMO] [REQUIRED]

SoftwareInventoryCovered – An attribute that captures "enterprise software management coverage" on an individual endpoint (indicating a device is covered by enterprise software asset inventory management system, such as Microsoft Configuration Manager, IBM BigFix, etc.). This value indicates coverages as required for FISMA CIO annual reporting. [FY2020 CIO FISMA Metrics] [REQUIRED]

DeviceSubComponent – An entity that captures a hardware subcomponent of a device (e.g., CPU, hard disk drive). [CDM PMO]

DeviceSubComponentDescription – An attribute that captures a textual description of a device subcomponent. [CDM PMO]

DeviceSubComponentModel – An attribute that captures the model name/identifier of a device subcomponent (e.g., Core-i5 8550U). [CDM PMO]

DeviceSubComponentType – An attribute that captures the type of a device subcomponent as:

- PROCESSOR (central processing unit of system)
- DISK (physical solid state, magnetic disks installed/fixed within a hardware device)
- OTHER (agency-specific subcomponent captured)

[CDM PMO]

DeviceSubComponentVendor – An attribute that captures the name of the vendor that makes the device subcomponent (e.g., Intel, AMD). [CDM PMO]

DeviceSubComponentID – An attribute that captures a partial identifier for each device subcomponent within an agency's network. [CDM PMO]

DeviceScan – An entity that captures information relating to the results of device scans produced by CDM tools/sensors on agency networks. [CDM PMO] [REQUIRED]

Credentialed – A Boolean attribute that captures the type of device scan as either CREDENTIALED (i.e., CDM tool/sensor successfully authenticates to device with a valid credential) or NON-CREDENTIALED (i.e., unauthenticated scan). [CDM PMO] [REQUIRED]

CSMSettingsCount – An attribute that captures number of discrete DISA STIG CAT 1 benchmark checks exclusively associated with AWARE CSM scoring, per device scan evaluation. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because this applies only to CSM scans.)*

DeviceScanAuthOutcome – An attribute that captures the authentication result of a credentialed device scan, which shall be only one of following:

- SUCCESS (i.e., scan was successfully authenticated to produce detailed scan data)
- FAIL (i.e., scan was unsuccessfully authenticated and did not produce detailed scan data)

Any agent-based scan is expected to be successfully credentialed. Where both network- and agent-based scans apply to a given device, the agent-based scan is expected to supersede. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because it applies only if the scan is a credentialed scan—i.e., Credentialed = "TRUE.")*

DeviceScanDate – An attribute that captures the date and time a device scan completed. [CDM PMO] [REQUIRED]

DeviceScanID – An attribute that captures a unique identifier for each device scan recorded/conducted within an agency's network. [CDM PMO] [REQUIRED]

DeviceScanMethod – An attribute that captures what VUL method was used to detect the vulnerability on the device, which shall be one of the following values:

- Agent-based
- Network-based

[CDM PMO]

DeviceScanType – An attribute that captures the type of information produced by the device scan performed on a device. This attribute shall be one or more of the following:

- CSM (producing misconfiguration information/CCEs)
- VUL (producing vulnerability information/CVEs)
- MTD (producing mobile vulnerability information)
- EMM (producing mobile asset inventories)
- SWAM (producing authorized software information through the AEC sub-capability and

software inventory updates)

- HWAM (producing hardware asset management information)
- BOUND-F
- MNGEVT

[CDM PMO] [REQUIRED]

ScanBenchmarkName – An attribute that captures the DISA STIG CAT 1 benchmark name from a misconfiguration scan. [CDM PMO] [CONDITIONALLY REQUIRED]

ScanBenchmarkRelease – An attribute that captures the DISA STIG CAT 1 benchmark release from a misconfiguration scan. [CDM PMO] [CONDITIONALLY REQUIRED]

ScanBenchmarkVersion – An attribute that captures the DISA STIG CAT 1 benchmark version from a misconfiguration scan. [CDM PMO] [CONDITIONALLY REQUIRED]

Entitlement – An entity that captures a more granular recording of access rights, supporting the higher-level privileged access stipulated in the PRIV element. (See **Entitlement** in Data Model Key Terms for additional context). [CDM PMO]

EntitlementDescription – An attribute that captures a descriptive text to illustrate the entitlement type (e.g., this entitlement allows for modification of configurations of zones, subnets, and IP access control lists on *FIREWALLS* within the enterprise.). [CDM PMO]

EntitlementID – An attribute that captures a unique identifier for a specific entitlement. [CDM PMO]

EntitlementName – An attribute that captures an agency's common name for each **entitlement** instance captured by the CDM system (e.g., "Server Admin in Org Enclave 1 – LINUX ONLY," "Security Group-vCENTER_DC"). [CDM PMO]

EntitlementType – An attribute that captures the name (type) of entitlement inherent to the privilege that is associated with a higher-level privilege (e.g., FIREWALL, ROUTER, CORE SWITCH). [CDM PMO]

EventOnNetwork – An entity that captures an "observable occurrence in a system or network" inventoried in the CDM solution due to a correlation to occurring agency network activities. The event is likely part of a suspected or confirmed security incident, as reported by a CDM tool/sensor based upon defined parameters (e.g., agency or CDM policy-based triggers/alerts). (See **Event** in Data Model Key Terms for additional context) [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because some agencies may not have access to the **Event Management** security capabilities necessary to produce this data; therefore, the data is required only for certain CDM solutions that employ **Event Management**.)*

EventName – An attribute that captures a descriptive name/title for an event (e.g., Generic ICMP Event, Unauthorized File Transfer Protocol [FTP] Attempt, Malicious Script Detected). [CDM PMO]

EventOnNetworkID – An attribute that captures a unique identifier for each event that occurs on an agency's network that has been analyzed and attributed to the timeline of an incident or suspicious activity on the agency's network. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

EventRawData – An attribute that captures that raw event message (e.g., entire log entry in its original state, such as Common Event Format, Log Event Extended Format, Syslog message, etc.) as reported from the agency tool. [CDM PMO]

EventSeverity – An attribute that captures the agency-defined, normalized, severity rating (e.g., Generic ICMP Event, Priority: 3, Unauthorized Access detected: Critical Priority, etc.) of the incident-related event as reported by the agency tool. [CDM PMO]

*(**Note:** Required only if the tool provides this data natively and the agency implements a severity schema that enables this data to be useful.)*

EventTimeStamp – An attribute that captures the time stamp (i.e., date, time, and time zone) when the tool triggered and reported the event. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

EventType – An attribute that captures information that identifies the type or category of the **EventOnNetwork** record as predefined by the CDM PMO or tailored by an agency tool or process. The value of this attribute may be one of the following values:

- UNAUTHORIZED SOFTWARE EXECUTION ATTEMPT – Endpoint attempts to run unauthorized software as reported by the CDM tool/sensor supporting AEC, a sub-capability under the SWAM capability
- MALICIOUS EVENT ALERT – Suspicious information discovered on the network that may be suspected or confirmed to be part of malicious activities to compromise the security of the agency's IT infrastructure
- NETWORK ACCESS PROTECTION EVENT – CDM tool/sensor that supports network access protection/NAC reports some policy violation based upon recently connected devices)
- OTHER (AGENCY DEFINED)

[CDM PMO] [CONDITIONALLY REQUIRED] *(Conditionally required; see above.)*

Facility[28] – An entity that captures the relevant characteristics of a physical site, hosting provider (e.g., Amazon Web Services GovCloud), location housing physical IT assets (e.g., endpoints, subcomponents of a FISMA system), and/or agency personnel (See **Facility** in Data Model Key Terms for additional context.)

FacilityID – An attribute that captures a unique identifier for a specific facility. [CDM PMO] [REQUIRED]

FacilityLocation – An attribute that captures the address for a specific facility. [CDM PMO]

FacilityName – An attribute that captures an agency-specified common name for a specific facility (e.g., San Antonio Data Center). [CDM PMO]

FacilityType – An attribute that captures the type of facility that the physical site most closely resembles. If populated, the entity shall be one or more of the following values:

- AGENCY DATA CENTER – Site that holds a high concentration of data processing equipment (e.g., servers, network equipment)
- COLOCATION
- HOSTING PROVIDER – Including cloud service providers
- OFFICE – Any site that houses IT assets and agency personnel performing day-to-day

[28] The term "facility" is to be interpreted as a set of data that indicates or approximates the physical location of IT assets associated with the data entity (i.e., users, devices, etc.). This entity is not to imply, specify, or relate to any physical security requirements or controls traditionally associated with the NIST PE family of controls (physical access).

activities; official duty station(s)

- CAMPUS/HQ
- STORAGE – Any site that holds offline IT assets for disposition or delivery (e.g., warehouse, logistics depot)

[CDM PMO]

IncidentActor – An entity that represents information regarding an actor principally involved in or responsible for the cause of the **IncidentThreatAction**. [VERIS]

IncidentActorActionNote – An attribute that captures any additional agency information providing context to the **IncidentActor** in relation to the incident on the agency's network. [VERIS]

IncidentActorCategory – An attribute that captures, for an actor that is external to the agency, the category group the actor is most representative of. This attribute may be one of the following:

- ACTIVIST (activist group)
- AUDITOR (auditor)
- COMPETITOR (competitor)
- CUSTOMER
- ENVIRONMENTAL
- FORMER EMPLOYEE (former employee; no longer had access)
- NATION-STATE
- CRIMINAL (organized or professional criminal group)
- ACQUAINTANCE (relative or acquaintance of employee)
- STATE AFFILIATED (state-sponsored or -affiliated group)
- TERRORIST (terrorist group)
- UNAFFILIATED (unaffiliated person that is unknown to the organization)
- UNKNOWN
- OTHER

[VERIS]

IncidentActorID – An attribute that captures a unique identifier for each **IncidentActor**. [VERIS]

IncidentActorName – An attribute that captures the name of an individual person, party, and/or any organizational name/designation associated with the **IncidentThreatAction**. [VERIS]

IncidentActorOrigin – An attribute that captures the geographic origin (country) of the **IncidentActor**. [VERIS]

IncidentActorRelationship – An attribute that captures the relationship of each **IncidentActor** to the organization. The attribute shall be one of the following:

- INTERNAL – a party/person internal to the organization (e.g., employee)

- EXTERNAL – any party external to the organization with no predefined relationship, such as nation-states, advanced persistent threats, criminal groups, etc.
- PARTNER – any group/person with a professional relationship to the organization not granted "internal" access, such as vendors, contracted building custodial staff, security, etc.

[VERIS]

IncidentOnNetwork – An entity that represents a suspected or confirmed, reportable information security incident that has occurred within an agency's network and might negatively impact the confidentiality, integrity, and/or availability of an information system or its assets. (See **Incident** in Data Model Key Terms for additional context.) [Federal Incident Notification Guidelines] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because some agencies may not have access to the **Incident Management** security capabilities necessary to produce this data; therefore, the data is required only for certain CDM solutions that employ **Incident Management**.)*

CIAImpacted – An attribute that captures whether the confidentiality, integrity, or availability of an organization's information system(s) (i.e., FISMA system) were potentially compromised. [Federal Incident Notification Guidelines]

IncidentClassification – An attribute that captures whether a reported incident has been classified as a "Major Incident" by the agency.[29] A "Major incident" requires congressional notification within seven days of identification. [Federal Incident Notification Guidelines]

IncidentDescription – An attribute that captures a brief description of a reported incident that occurred on an agency's network. [Federal Incident Notification Guidelines]

IncidentDetectDate – An attribute that captures the date when any activity associated with a reported incident was first detected. [Federal Incident Notification Guidelines] [CONDITIONALLY REQUIRED] *(Conditionally required; see above.)*

IncidentDetectTime – An attribute that captures the time (including time zone) when any activity associated with a reported incident was first detected. [Federal Incident Notification Guidelines]

IncidentDetermination – An attribute that captures the authenticity and status of the incident. The attribute shall be only one of the following values:

- SUSPECTED (proposed for further analysis/follow-up; captured as a tentative record from some preliminary information)
- CONFIRMED (subject to some agency governed process; has been analyzed and determined to be a confirmed incident within the agency)

[CDM PMO]

IncidentDeterminationDate – An attribute that captures the date the **IncidentDetermination** attribute was set to CONFIRMED. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

IncidentDeterminationTime – An attribute that captures the time (including time zone) the **IncidentDetermination** attribute was set to CONFIRMED. [CDM PMO]

[29] Refer to the most recent OMB guidance for assistance with designation of a "Major Incident." Agencies may also consult with CISA to facilitate this determination.

IncidentFunctionalImpact – An attribute that captures whether the incident functionally impacted the organization. A functional impact is a measure of the actual, ongoing impact to the organization. In many cases (e.g., scans and probes, or a successfully defended attack), little or no incident impact may be experienced. This attribute may have **one** of the following categorical values as defined by CISA:

- NO IMPACT – Event has no impact.
- NO IMPACT TO SERVICES – Event has no impact on any business or ICS services or delivery to entity customers.
- MINIMAL IMPACT TO NON-CRITICAL SERVICES – Event has low level of impact on non-critical systems and services.
- MINIMAL IMPACT TO CRITICAL SERVICES – Event has minimal impact, but the area impacted is a critical system or service, such as email or Active Directory.
- SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – Event has a significant impact on a non-critical service or system.
- DENIAL OF NON-CRITICAL SERVICES – Event denies or destroys a non-critical system.
- SIGNIFICANT IMPACT TO CRITICAL SERVICES – Event has significant impact on a critical system, such as a local administrative account.
- DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – Event renders a critical system unavailable.

[Federal Incident Notification Guidelines]

IncidentFunctionalImpactDescription – An attribute that captures the justification for the reported incident's functional impact designation, including any supplemental information describing the downstream impacts (e.g., mission impacts, business impacts, financial or safety considerations). [Federal Incident Notification Guidelines]

IncidentInformationImpact – An attribute that indicates whether the incident had information impact on the organization. Incidents may affect the confidentiality and integrity of the information stored or processed by various systems. The information impact category describes the type of information lost, compromised, or corrupted. This attribute shall be one or more of the following categorical values as defined by CISA:

- NO IMPACT – Event has no known data impact.
- SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists.
- PRIVACY DATA BREACH – The confidentiality of PII or personal health information (PHI) was compromised.
- PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets, was compromised.
- DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record (MBR) overwrite, have been used against a non-critical system.

- CRITICAL SYSTEMS DATA BREACH – Data pertaining to a critical system has been exfiltrated.
- CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
- DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite, have been used against a critical system.

[Federal Incident Notification Guidelines]

IncidentInformationImpactDescription – An attribute that captures the justification for the reported incident's information impact categorization, including any supplemental information that further describes the information impacted—including, but not limited to, specific descriptors of the information or credentials impacted and justification on why data may/may not be critical to the enterprise. [Federal Incident Notification Guidelines]

IncidentNetworkLocation – An attribute that captures observed activity related to the reported incident and that is categorized using the CISA definition. Categorization shall be one or more of the following:

- LEVEL 0 – UNSUCCESSFUL – Existing network defenses repelled all observed activity.
- LEVEL 1 – BUSINESS DEMILITARIZED ZONE – Activity was observed in the business network's demilitarized zone (DMZ). These systems are generally untrusted and are designed to be exposed to the internet. Examples are a company's web server or email server.
- LEVEL 2 – BUSINESS NETWORK – Activity was observed in the business or corporate network of the victim (i.e., corporate user workstations, application servers, and other non-core management systems).
- LEVEL 3 – BUSINESS NETWORK MANAGEMENT – Activity was observed in business network management systems, such as administrative user workstations, Active Directory servers, or other trust stores.
- LEVEL 4 – CRITICAL SYSTEM DMZ – Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services, such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.
- LEVEL 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management, such as human-machine interfaces in ICSs.
- LEVEL 6 – CRITICAL SYSTEMS – Activity was observed in the critical systems that operate critical processes, such as programmable logic controllers in ICS environments.
- LEVEL 7 – SAFETY SYSTEMS – Activity was observed in critical safety systems that ensure the safe operation of an environment. One example of a critical safety system is a fire suppression system.
- UNKNOWN – Activity was observed, but the network segment could not be identified.

[Federal Incident Notification Guidelines]

IncidentOnNetworkID – An attribute that captures an agency's assigned unique identifier for an incident on the agency's network that has been captured and reported (e.g., incident tracking number). [Federal Incident Notification Guidelines] [CONDITIONALLY REQUIRED] *(**Note:** See above for*

explanation of "conditionally required.")

IncidentPrimaryAttackVector – An attribute that captures the attack vector(s) that led to the reported incident, as determined by the agency. To facilitate a common set of terms and relationships between government security teams, CDM will use a common taxonomy provided by CISA as developed from NIST SP 800-61 Rev. 3. The value of this attribute shall be one or more of the following types:

- UNKNOWN – Cause of attack is unidentified. This option is acceptable if cause (vector) is unknown upon initial report. The attack vector may be updated in a follow-up report.
- ATTRITION – An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., denial of service [DoS] attack intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures).
- WEB – An attack executed from a website or web-based application (e.g., a cross-site scripting attack used to steal credentials; a redirect to a site that exploits a browser vulnerability and installs malware).
- EMAIL/PHISHING – An attack executed via an email message or attachment (e.g., exploit code disguised as an attached document; a link to a malicious website in the body of an email message).
- EXTERNAL/REMOVABLE MEDIA – An attack executed from removable media or a peripheral device (e.g., malicious code spreading onto a system from an infected flash drive).
- IMPERSONATION/SPOOFING – An attack involving replacement of legitimate content/services with a malicious substitute (e.g., spoofing, man-in-the-middle attacks, rogue wireless access points, and structured query language [SQL] injection attacks).
- IMPROPER USAGE – Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories (e.g., a user installs file-sharing software, leading to the loss of sensitive data; a user performs illegal activities on a system).
- LOSS OR THEFT OF EQUIPMENT – The loss or theft of a computing device or media used by the organization (e.g., a misplaced laptop or mobile device).
- OTHER – An attack method that does not fit into any other vector.

[Federal Incident Notification Guidelines]

(***Note:*** *In the CDM Data Model, subordinate* IncidentThreatAction*(s) may be associated with individual incidents that may facilitate determination of this value. The attribute* ThreatActionMethod*, if determined by agencies, can facilitate more discrete attack processes that can be used to determine the primary vector(s) for reporting.)*

IncidentRecoverability – An attribute that captures the CISA categorization of the scope of resources needed to recover from a reported incident. The attribute shall be classified as one of the following values:

- REGULAR – Time to recovery is predictable with existing resources.
- SUPPLEMENTED – Time to recovery is predictable with additional resources.

- EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
- NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data is ex-filtrated and posted publicly).

[Federal Incident Notification Guidelines]

IncidentRecoverabilityDescription – An attribute that captures the justification for the reported incident's recoverability classification, including any supplemental information describing the type of outside resources needed. [Federal Incident Notification Guidelines]

IncidentRecoverabilityTime – An attribute that captures an estimate of how much time is required (in days) to recover from the reported incident, if known. [Federal Incident Notification Guidelines]

IncidentReportDate – An attribute that captures the date the incident was reported to CISA. [Federal Incident Notification Guidelines] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

IncidentStartDate – An attribute that captures the start date the reported incident. [Federal Incident Notification Guidelines]

(***Note**: This attribute should reflect the projected/confirmed time that the incident started (i.e., when the incident started impacting the agency), which is distinct from the date the agency confirmed the incident. Incident start date/times might occur through subsequent investigation and analysis of events and other associated activity on the agency's network/assets once a declaration of existence of an incident is made.*)

IncidentStartTime – An attribute that captures the time (including time zone) the reported incident started. [Federal Incident Notification Guidelines]

(***Note:** This attribute should reflect the projected/confirmed time that the incident started (i.e., when the incident started impacting the agency), which is distinct from the date the agency confirmed the incident. Incident start date/times might occur through subsequent investigation and analysis of events and other associated activity on the agency's network/assets once a declaration of existence of an incident is made.*)

CISARiskRating – An attribute that captures the CISA assigned risk rating based on the CISA National Cyber Incident Scoring System (NCISS). [Federal Incident Notification Guidelines]

*(**Note:** This information will be provided by the CDM federal dashboard upon receipt, confirmation, and adjudication of the reported incident by DHS.)*

CISATrackingNumber – An attribute that captures the CISA assigned tracking identifier, as assigned from CISA upon submission of the incident report to DHS. [Federal Incident Notification Guidelines]

*(**Note:** This information will be provided by the CDM federal dashboard upon receipt, confirmation, and adjudication of the reported incident by DHS.)*

IncidentThreatAction – An entity that represents some distinct action or event that occurred, which contributed significantly to the cause of the incident (**IncidentOnNetwork**). [VERIS] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because some agencies may not have access to the **Incident Management** security capabilities necessary to produce this data; therefore, the data is required only for certain CDM solutions that employ **Incident Management**.)*

IncidentThreatActionID – An attribute that captures a unique identifier pertaining to a specific **IncidentThreatAction**. [VERIS] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

ThreatActionAgencyNote – An attribute that captures any additional agency information that is relevant to the **IncidentThreatAction**. [VERIS]

ThreatActionCategory – An attribute that captures a category for the **IncidentThreatAction**. The attribute shall be one of the following values:

- MALWARE (installed malware, which includes viruses, worms, and keyloggers)
- HACKING (attempts to circumvent security mechanisms, which include DoS and SQL injection)
- SOCIAL (social engineering)
- MISUSE (policy violations, use of non-approved software or hardware, admin abuse resulting from granted access/privileges, etc.)
- ERROR (unintentional mistakes, errors, misconfigurations, loss devices, etc. that result in an incident)
- PHYSICAL (theft, snooping, sabotage, etc.)
- ENVIRONMENTAL (natural disasters, power failures, etc.)
- UNKNOWN (This option is acceptable if the root cause or vector used in the ThreatAction is unknown upon initial report of the **IncidentOnNetwork**. It allows the **IncidentThreatAction** to be instantiated such that devices can be tied to the incident. It may be updated in a follow-up report or submission of incident data.)

[VERIS] [Federal Incident Notification Guidelines] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

ThreatActionDate – An attribute that captures the date the **IncidentThreatAction** occurred. [VERIS]

ThreatActionMalwareStrain – For each **IncidentThreatAction** that is categorized as *MALWARE*, this is an attribute that captures a common name or known identifier for the strain of malware as identified by any authoritative source the agency may have (e.g., AV tool, threat management tool, endpoint security tool). [VERIS] [MAEC] *(**Note:** This information might not be relevant to some* **IncidentThreatAction** *entities, or malware might not be easily identifiable.)*

ThreatActionMethod – An attribute that captures the primary method(s) ("vectors" in VERIS) used to execute the **IncidentThreatAction** based on the **ThreatActionCategory**. Appendix C provides **ThreatActionMethod** values for each **ThreatActionCategory** (excluding ENVIRONMENTAL and UNKNOWN). [VERIS] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

ThreatActionPattern – An attribute that captures reference(s) to attack pattern(s), if known, using CAPEC catalog numbers and titles (e.g., CAPEC 242 – Code Injection, CAPEC 163 – Spear Phishing). This attribute provides a method to normalize a threat action to MITRE's CAPEC™ catalog. [CAPEC]

ThreatActionVariety – An attribute that captures the relevant malicious threat activity classifications pertaining to an **IncidentThreatAction** based on the **ThreatActionCategory**. This attribute shall be one or more of the values presented in Appendix C, as filtered based on the **ThreatActionCategory**. [VERIS]

[CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

(***Note:** The exhaustive list of possible values is too extensive to be provided here. Refer to APPENDIX C for the fully enumerated set of possible values.*)

IndicatorOfCompromise – An entity that represents an incident-related IOC. [Federal Incident Notification Guidelines] [CONDITIONALLY REQUIRED] *(**Note:** Conditionally required because some agencies may not have access to the **Incident Management** security capabilities necessary to produce this data; therefore, the data is required only for certain CDM solutions that employ **Incident Management**.)*

IndicatorOfCompromiseID – An attribute that captures a unique identifier that pertains to a specific **IndicatorOfCompromise** associated with an incident on an agency's network. [Federal Incident Notification Guidelines] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

IndicatorOfCompromiseData – An attribute that captures the raw data associated with the IOC (e.g., file hash, domain name, IP address, signature), [Federal Incident Notification Guidelines]

IndicatorOfCompromiseDescription – An attribute that captures any context related to the IOC (e.g., type of IOC, location where IOC is likely to be seen, other descriptive information), [Federal Incident Notification Guidelines]

InterfaceName – An attribute that captures the machine-assigned or configured label for the interface associated with a **DeviceIPAddress**. [CDM PMO] [REQUIRED]

IPAddress – An attribute that captures the last known (discovered) IP address(es) configured on each device (e.g., computer, printer) participating in a computer network using IP for communication.

This attribute has the following allowable formats:

- IPv4 valid range: 0.0.0.0 – 255.255.255.255, excluding any reserved IP addresses (e.g., 0.0.0.0, 240.0.0.0/4, and 255.255.255.255)
- IPv6 valid range: 0:0:0:0:0:0:0:0 – FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

[CDM PMO] [REQUIRED]

(***Note**: This should be the last known/sensed "good" IP addresses assigned to the actual device. Subsequent IP addresses affirmatively discovered to belong to a device should take precedence over obsolete IP address assignments.*)

IPAddressAgencyOwned – A Boolean attribute that captures a value that indicates whether the IP address identified for a device is owned or used by the agency identified for the device (e.g., IP address falls within the known managed IP address space of an agency). [FY20 CIO FISMA Metrics]

IPVersion – An attribute that captures the IP version of the IP address for the device interface. Values for this attribute shall be only one of the following:

- IPv4
- IPv6

[CDM PMO] [REQUIRED]

MACAddress – An attribute that captures a media access control (MAC) address that is associated with each **DeviceInterface**. [CDM PMO] [REQUIRED]

MaliciousEventOnNetwork [*EventOnNetwork Specialization*] – An entity that is a specialization of **EventOnNetwork** representing an event suspected to be caused by malicious actor or activities, as detected by CDM tools/sensors that filter, inspect, or analyze network/device activity for known or suspected threats. [CDM PMO]

MaliciousEventAction – An attribute that captures, if applicable, any manual or automated response/actions taken by agency staff or security tools to mitigate the malicious network activity identified (e.g., ran playbook, took device offline, dropped/blocked connection or session, killed process, quarantined malware). [CDM PMO]

MaliciousEventApplicationProtocol – An attribute that captures the application protocol that was observed as part of the malicious event (e.g., FTP, Secure Shell, Hypertext Transfer Protocol, Secure Sockets Layer [SSL]/Transport Layer Security [TLS], TELNET, RDP). [CDM PMO]

MaliciousEventDstHostName – An attribute that captures, if applicable, the identifying string (e.g., hostname, URL, URI) of the destination host/device/resource within a recorded event (e.g., network session, observed activity) suspected to be malicious, as detected by a tool/sensor. [CDM PMO]

MaliciousEventDstIP – An attribute that captures, if applicable, the destination IP address (IPv4 or IPv6) of a host/device/resource within a recorded event (e.g., network session, observed activity) suspected to be malicious, as detected by a tool/sensor. [CDM PMO]

MaliciousEventDstPort – An attribute that captures, if applicable, the destination port (0 – 65535) of a host/device/resource within a recorded event (e.g., network session, observed activity) suspected to be malicious, as detected by a tool/sensor. [CDM PMO]

MaliciousEventReportingReason – An attribute that captures the basis (e.g., signature match, behavior anomalies triggered, matching threat indicators) for suspecting an event is malicious in nature and warrants further investigation or oversight. [CDM PMO]

MaliciousEventSrcHostName – An attribute that captures, if applicable, the identifying string (e.g., hostname, URL, URI) of the source host/device/resource within a recorded event (e.g., network session, observed activity) suspected to be malicious, as detected by a tool/sensor. [CDM PMO]

MaliciousEventSrcIP – An attribute that captures, if applicable, the source IP address (IPv4 or IPv6) of a host/device within a recorded event (e.g., network session, observed activity) suspected to be malicious, as detected by a tool/sensor. [CDM PMO]

MaliciousEventSrcPort – An attribute that captures, if applicable, the source port (0 – 65535) of a host/device within a recorded event (e.g., network session, observed activity) suspected to be malicious, as detected by a tool/sensor. [CDM PMO]

.ManagedAppOnNetwork – An entity that represents a defined application that is under discrete risk management and accountability. (See **Managed Applications** in Data Model Key Terms for additional context.) [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because it may not apply to a particular agency's FISMA containerization needs and related solution implementation.)*

AssignedAWAREScore – An attribute that captures the sum total of all assigned AWARE risk posture sub-scores that is transferred to the managed application. [CDM PMO]

AssignedCSMSubScore – An attribute that captures the assigned CSM sub-score (i.e., AWARE risk posture score directly attributable to discovered misconfigurations) that is transferred to the managed application. [CDM PMO]

AssignedUAHSubscore – A **derived** attribute that captures the calculated unauthorized (UAH) AWARE risk posture sub-score (i.e., unauthorized as described above in the Data Model Key Terms section) associated with an agency's ManagedApp. [CDM PMO]

AssignedVULSubScore – An attribute that captures the assigned VUL sub-score (i.e., AWARE risk posture score directly attributable to discovered vulnerabilities) that is transferred to the managed application. [CDM PMO]

ManagedAppDescription – An attribute that captures any relevant descriptive information in relation to the managed application. [CDM PMO]

ManagedAppOnNetworkID – An attribute that captures a value that uniquely identifies a managed application within the inventory of an agency. [CDM PMO] [REQUIRED]

ManagedAppNamespace – An attribute that captures a label or name of an application that is supported by one or many detected instances of installed software (e.g., website URL, custom app name). [CDM PMO]

MisconfigurationOnNetwork – An entity that represents a single discovered misconfiguration on an agency device. Misconfigurations are a deviation from the allowable federally or agency-defined configuration baseline for any device and represent a potential IT security risk that should be addressed. Federal configuration baselines are defined through the adoption of benchmarks that are clearly stated and represent industry best practice. (See **Benchmark** and **CCE Dictionary** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

ConfigurationCheckDescription – An attribute that captures the CDM tool-specified description of the configuration setting: synopsis of the security setting, its security implications, and relevant operational impact. For example, the CSM scanner reports: *"Allowing anonymous logon users (null session connections) to list all account names and enumerate all shared resources can provide a map of potential points to attack the system."* [CDM PMO] [REQUIRED]

ConfigurationCheckFix – An attribute that captures the CDM tool-specified description of the needed setting(s) to pass the configuration audit (e.g., fix text or fix value[s]). For example, a CSM scanner reports the available mitigation actions to take: *"Set the following Group Policy setting to Enabled. Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares."* [CDM PMO] [REQUIRED]

ConfigurationCheckProductName – An attribute that captures the common product name of software impacted by the configuration setting inventoried (e.g., Windows 2012R2, Red Hat Enterprise Linux, Internet Information Services, SQL Server). [CDM PMO] [REQUIRED]

ConfigurationCheckParameter – An attribute that captures the machine-level configuration parameters checked as reported by the CDM sensor (e.g., registry keys, permission settings). [CDM PMO]

(**Example:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous)

CSMActualSetting – An attribute that captures the actual configuration setting discovered on the device, as reported by the CDM sensor (e.g., LmCompatibilityLevel in HKLM\SYSTEM\CurrentControlSet\Control\Lsa equals "3"). [CDM PMO] [REQUIRED]

CSMExceptionDescription – An attribute that captures the justification or rationale associated with an agency's exception to a mandated configuration setting. [CDM PMO] *(**Note:** This attribute is subject to*

*the allowance of a CSM EXCEPTION [see **CSMStatus**]. If an exception is permitted, this field is required.)*

CSMOriginalDiscoveryDate – An attribute that captures the date when the **ConfigurationSettingsOnNetwork** (i.e., deviation from expected configuration) was first discovered on a specific device. [AWARE Technical Design] [REQUIRED]

CSMStatus – An attribute that captures the status of a particular **MisconfigurationOnNetwork**. The attribute shall be one of the following:

- OPEN
- CSM EXCEPTION – Captures an agency's desire to allow for an exception to a mandated configuration setting on a particular device
- REMEDIATED – Vulnerability has been remediated and is no longer being detected by tool/sensors

[CDM PMO] [REQUIRED]

DateOfCSMScan – An attribute that captures the date of the last (most recent) configuration audit (scan) that found the misconfiguration on a device within the agency's network. [CDM PMO] [REQUIRED] *(**Note:** This attribute should reflect the last time that a misconfiguration was "seen" or updated through a scanning process. If no new relevant details about a misconfiguration are discovered, but it is still seen, this attribute would be updated with the last date the sensor witnessed the misconfiguration.*

MisconfigurationOnNetworkID – An attribute that captures a value that uniquely identifies a captured security-related software misconfiguration as specified within a benchmark and/or agency-defined configuration baseline, represented by the **MisconfigurationOnNetwork** entity. (See **Benchmark** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

MobileDeviceOnNetwork [DeviceOnNetwork Specialization**]** – An entity that captures information about a mobile device (e.g., a cell phone, smartphone, tablet, pager, or other mobile device). **MobileDeviceOnNetwork** is a specialization (subclass) of **DeviceOnNetwork** that enumerates specific category devices with additional attributes and relationships that are important for the CDM solution to capture. [CDM PMO] [REQUIRED]

DeviceAbilityToRemoveEMM – An attribute that captures whether a mobile device user is able to remove the MDM/EMM profile without administrator approval. [CDM PMO] [REQUIRED]

DeviceAccessDeniableByAgency – An attribute that captures whether a mobile device enables agency capability to deny access to agency enterprise services. [CDM PMO] [REQUIRED]

DeviceAssignedPhoneNumbers – A multivalued attribute that captures the phone number(s) assigned to a mobile device with telephony capabilities (e.g., cellular telephone). [CDM PMO]

DeviceCoveredByMTD – An attribute that captures whether a mobile device is covered by an MTD solution. [CDM PMO] [REQUIRED]

DeviceIMEI – An attribute that captures the international mobile equipment identity (IMEI) or mobile equipment identifier (i.e., GUID) of a mobile device. [CDM PMO]

DeviceManagementServer – An attribute that captures the device name (e.g., FQDN), software-as-a-service name, URI, or other appropriate UID of the MDM/EMM server to which the mobile device is

currently registered (enrolled). The MDM/EMM server is expected to be capable of and configured for authorization and remote wiping criteria when aligned with agency policy. [CDM PMO]

DeviceManagementRemoteWipe – An attribute that captures whether the management server is capable of and configured for authorization and remote wiping criteria when aligned with agency policy. [CDM PMO] [REQUIRED]

DeviceSerialNumber – An attribute that captures the serial number of a mobile device. [CDM PMO]

DeviceTelecomProviders – A multivalued attribute that captures the name of the telecom provider(s) serving a mobile device. [CDM PMO]

EMMLastSeenTimestamp – An attribute that captures the time stamp (date, time) when the mobile device last "checked in" (e.g., synchronized, reported back) with the management server (i.e., MDM/EMM) that the device is currently registered (enrolled) with, as reported by the MDM/EMM server. [CDM PMO] [REQUIRED]

NACEventOnNetwork [*EventOnNetwork Specialization*] – An entity that captures the raw event information reported by a CDM tool/sensor supporting the network access protection capability when that tool puts any device into a BLOCKED or QUARANTINED state (see **DeviceStatus** in Data Model Key Terms for more information).

NACEventOnNetwork is a specialization (subclass) of **EventOnNetwork** (see **Network Access Protection** in Data Model Key Terms for additional context). [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because some agencies may not have access to the **Event Management** security capabilities necessary to produce this data; therefore, the data is required only for certain CDM solutions that employ **Event Management**)*

NACEventAction – An attribute that captures the action taken on an endpoint by NAC system that may be one of the following values:

- BLOCK
- QUARANTINE [CDM PMO]

NACEventActionReason – An attribute that captures the basis (i.e., rule/policy violation) for an NAC tool/sensor blocking or quarantining a connecting/connected device (e.g., missing patch, disabled antimalware application). [CDM PMO]

NACEventDeviceIP – An attribute that captures the IP address of the (connecting) device, which the CDM tool/sensor supporting the NAC capability was able to discover upon device connection to the network. [CDM PMO]

NACEventDeviceMAC – An attribute that captures the MAC address of the (connecting) device, which the CDM tool/sensor supporting the NAC capability was able to discover upon device connection to the network. [CDM PMO]

NACEventDeviceName – An attribute that captures the name (e.g., DNS/hostname) of the (connecting) device, which the CDM tool/sensor supporting the NAC capability was able to discover upon device connection to the network. [CDM PMO]

NACEventDeviceOSClassfication – An attribute that captures the OS (e.g., Windows, Ubuntu, macOS, IOS) of the (connecting) device, which the CDM tool/sensor supporting the NAC capability was able to discover upon the device being connected to the network. [CDM PMO]

NACEventDeviceTypeClassification – An attribute that captures the general type/kind of (connecting) device, which the CDM tool/sensor supporting the NAC capability was able to discover (or predict) upon device connection to the network. [CDM PMO]

OrganizationalUnitBoundary – An entity that captures an organization of any size, complexity, or positioning within a hierarchal structure of a department or agency (see **Organizational Unit** in Data Model Key Terms for additional context). The relationship between a Tier 0 organizational unit and a Tier 1 organizational unit is represented by a recursive relationship in the LDM. Recursive relationships are often used to represent hierarchies or networks, where an entity can be connected to other entities of the same type. [CDM PMO] [REQUIRED]

Additional Context: This is the construct that provides the *OU containers* functionality that will provide a capability to group CDM objects of interest. At a *minimum,* the CDM solution shall be capable of providing OU containers that capture the first level of agency hierarchy organization (1 sub organizational unit within a department or agency). Refer to the *Organizational Unit Containers (OU Containers)* section for more information.

OrganizationalUnitBoundaryID – An attribute that captures a UID that identifies a specific organizational unit boundary. [CDM PMO] [REQUIRED]

Additional Context: Refer to the *Organizational Unit Containers (OU Containers) section*.

OrganizationalUnitName – An attribute that captures an agency-defined name for the organization. [CDM PMO] [REQUIRED]

OrganizationalUnitType – An attribute that captures the type of organizational unit for use in determining the provider of the devices inventoried by CDM. The attribute shall be one of the following:

- GOVERNMENT – Devices assigned to this OU are GFE and are subject to this organization's policies.
- CONTRACTOR – Devices assigned to this OU are contractor-provided devices (non-GFE) and are subject to contractor oversight and associated policies.

[CDM PMO] [REQUIRED]

OUAWARECSMSubScoreAVG – A **derived** attribute that captures the average secure configuration management AWARE risk posture sub-score (e.g., open misconfigurations/CCEs) associated with all agency assets assigned to an OU. [CDM PMO] [REQUIRED]

OUAWARECSMSubScoreSUM – A **derived** attribute that captures the aggregated secure configuration management AWARE risk posture sub-score (e.g., open misconfigurations/CCEs) associated with all agency assets assigned to an OU. [CDM PMO] [REQUIRED]

OUAWAREScore – A **derived** attribute that captures the aggregated AWARE risk posture score associated with all agency assets assigned to an OU. [CDM PMO] [REQUIRED]

OUAWAREUAHSubscore – A **derived** attribute that captures the calculated unauthorized device AWARE risk posture sub-score (i.e., unauthorized as described above in the Data Model Key Terms section) associated with all agency assets assigned to an OU. [CDM PMO] [REQUIRED]

OUAWAREVULSubScoreAVG – A **derived** attribute that captures the average vulnerability AWARE risk posture sub-score (e.g., open CVEs) associated with all agency assets assigned to an OU. [CDM PMO] [REQUIRED]

OUAWAREVULSubScoreSUM – A **derived** attribute that captures the aggregated vulnerability AWARE risk posture sub-score (e.g., open CVEs) associated with all agency assets assigned to an OU. [CDM PMO] [REQUIRED]

PRIV – An entity that captures a permission to perform an action. For CDM, the **PRIV** elements focus exclusively on logical actions and associated access. (See **PRIV** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

DatePRIVStatusInitiated – An attribute that captures the date when a **PRIV** entity's (specific instance of a **PRIV**) status last underwent any of the following events:

- **Any** change of state (e.g., from ISSUED to SUSPENDED, SUSPENDED to REVOKED), including:
  - Date when **PRIV** is first ISSUED or first classified as PENDING.
  - RE-ISSUED (i.e., renewed whereby the state remains ISSUED but new date data is acquired through updating the **DatePRIVStatusInitiated** attribute with a new date).

PRIVCreationDate – An attribute that captures the date **PRIV** was originally provisioned/tracked. [CDM PMO]

PRIVDescription – An attribute that captures descriptive text to add additional context or clarity to an instance of the **PRIV** element (e.g., description of unique agency PRIV types, adding supplemental guidance or context for the provisioning of **PRIV** in a specific instance). [CDM PMO]

PRIVExpirationDate – An attribute that captures the date upon which a **PRIV** entity (e.g., privilege of record) becomes invalid. [CDM PMO] [REQUIRED] (***Note***: *This attribute should be updated when **PRIV** elements are "reissued" or "reauthorized" as part of a recurring review process.*)

PRIVID – An attribute that captures a unique identifier referencing a specific **PRIV** instance. [CDM PMO] [REQUIRED]

PRIVName – An attribute that captures an agency's common name for each **PRIV** instance captured by the CDM system (e.g., "ACME.net Domain Administrator"). [CDM PMO]

PRIVReviewDate – A date attribute that captures the last known time a **PRIV** review was conducted. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because the first review date may not yet have transpired .)*

PRIVReviewGracePeriod – An attribute that captures a period of time, in days, indicating the agency-defined periodicity for **PRIV** reviews, such that when it is exceeded by **PRIVReviewDate**, some agency-defined action is required, as dictated by policy (e.g., immediate review triggered or required; notification to security office). [CDM PMO]

PRIVStatus – An attribute that captures the current state of a **PRIV** element or where it is in the issuance process. The attribute shall be one of the following values:

- PENDING
- ISSUED
- SUSPENDED
- EXPIRED

- REVOKED

[CDM PMO] [REQUIRED]

PRIVStatusGracePeriod – An attribute that captures the agency-determined length of time, in days, the **PRIVStatus** attribute is allowed to remain in any status, beyond which time some action is recommended where applicable and as determined by agency policy (e.g., amount of time allowable for a **PRIV** to remain in SUSPENDED status before it is formally REVOKED and/or accounts are LOCKED; amount of time allowable for a **PRIV** to remain in EXPIRED status before accounts are DISABLED). [CDM PMO]

PRIVType – An attribute that categorizes a **PRIV** instance, as determined by the type and scope of the elevated system(s) privileges bestowed to an account. This attribute shall be one of the following values:

- SYSADMIN – System administrator that has administrative or root-level access on network servers.
- SECADMIN – Security administrator that has administrative or root-level access on any target device on the network.
- WINENTADMIN – Windows enterprise administrator that has authoritative administrative access on all Active Directory domain controllers on the network (e.g., expansive control on federated domain controllers that are members of a forest, schema rights).
- WINDOMAINADMIN – Windows domain administrator that has administrative access on Active Directory domain controllers on the network.
- WINWKSADMIN – Windows workstation administrator that has administrative access on Active Directory-connected workstations on the network.
- MFADMIN – Mainframe administrator that has administrative access on mainframe administrative functions on the network.
- ENTLDAPADMIN – Lightweight Directory Access Protocol (LDAP) server administrator that has administrative access on LDAP servers on the network.
- MDMADMIN – MDM administrator that has administrative access on MDM systems that control mobile devices on the network.
- NETADMIN – Network device administrator that has administrative access to network device administration control consoles (e.g., Cisco Identity Services Engine [ISE], IBM Access Client Solutions [ACS], Terminal Access Controller Access Control System Plus [TACACS+], SolarWinds, Junos Space) on the network.
- AGENCYDEFINED – Synonymous to "Other," this value allows agencies to capture the unique **PRIVType** categories that exist at an agency using the **PRIVDescription** attribute to add supplemental information (e.g., database administrator).
- CLOUDADMIN – Cloud administrator that has administrative access to resources within an agency's cloud tenant (e.g., AWS root account, Azure tenant administrator); these critical accounts, which include users with cloud admin-related roles, need to be identified and managed.

- STORAGEADMIN – Administrator of enterprise "storage" accounts associated with storage area networks or other enterprise-managed storage services.
- DATADMIN – Administrator of enterprise "database" accounts associated with structured data.
- LOCALSYSADMIN – Local accounts administrator (e.g., root) that has administrative or root - level access on servers.
- SERVICEACCT – Non-interactive services account, such as Windows services, micro-services, cloud services, etc.
- APPADMIN – Administrator that administers a **ManagedApplicationOnNetwork** or credentials used by those applications.
- DIGWORKACCT – Automated processes that emulate human interactions by utilizing AI/ML.
- RPACCT – Account that is used to that is used to automate repetitive, rules-based tasks.
- IOTACCT – Similar to a **LOCALSYSACCT** but on a system that has constrained capabilities (i.e., IoT).

[CDM PMO] [REQUIRED]

ResponseActivity – An entity that represents a specific activity in response to a suspected or confirmed incident on an agency's network. (See **Response Activity** in Data Model Key Terms for additional context.) [CDM PMO]

ResponseActivityDescription – An attribute that captures the related work, tasks, and actions associated with the **ResponseActivity** (e.g., isolate infected machines; capture memory/disk image; wipe and rebuild). [CDM PMO]

ResponseActivityID – An attribute that captures a unique identifier for each activity that occurs in response to a suspected or confirmed incident on an agency's network; this attribute helps an agency mitigate, triage, or otherwise remediate the impact of an incident. [CDM PMO]

ResponseActivityStartDate – An attribute that captures the date when the **ResponseActivity** was started. [CDM PMO]

ResponseActivityEndDate – An attribute that captures the date when the **ResponseActivity** was completed (if available). [CDM PMO]

SoftwareInstalledOnDevice – An entity that represents a record of all installed software detected on a specific agency device. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because **software** attribute-level data requirements apply only when a device **hosts scanned software**.)*

SoftwareAuthorizationStatus – An attribute that captures an agency's policy assessment of whether software is authorized to be on a device on the network. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required"; expected through the AEC sub-capability.)*

SoftwareFirstDetected – An attribute that captures the date an instance of unique software was first inventoried (i.e., confirmed installed, "seen") on a specific device on an agency's network. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

SoftwareLastDetected – An attribute that captures the date a unique software was last inventoried

(i.e., confirmed installed) on a specific device on an agency's network. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required." This attribute should reflect the last time that this unique software asset was "seen" or updated through a discovery or scanning process. For example, if no relevant details about a software inventory record change, but it is still seen, this attribute would be updated with the last date the sensor witnessed the software.)*

SystemBoundary – An entity that captures a boundary, including all components of an information (FISMA) system to be authorized for operation by an authorizing official, and that excludes separately authorized systems to which the information system is connected. (See **System** in Data Model Key Terms for additional context.) The relationship between a system and a subsystem is represented by a recursive relationship in the LDM. Recursive relationships are often used to represent hierarchies or networks where an entity can be connected to other entities of the same type. [CDM PMO] [REQUIRED]

AuthorizationDecision – An attribute that captures whether a system boundary is authorized to operate. The **AuthorizationDecision** is a Yes/No value. (See **Authorization Decision** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

AuthorizationDecisionType – An attribute that captures the type of authorization a system boundary has for authorization status indication. Values for this attribute shall be only one of the following:

- ATO
- Common control authorization
- Authorization to use
- Denial of authorization

[CDM PMO] [REQUIRED]

***Additional Context*:** Refer to FY21 CIO Annual FISMA Metrics, metric 1.1.3 / 1.1.4.

AuthorizationDecisionDate – An attribute that captures the date of the most recent authorization decision. [CDM PMO] [REQUIRED]

AuthorizationDecisionExpirationDate – An attribute that captures the date that the latest authorization decision expires. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because depending on the type of authorization decision (AuthorizationDecisionType), the ATO may not have an expiration date. For example, an Ongoing Authorization Decision type would not have an expected expiration date.)*

AuthorizationType: An attribute that captures the type of authorization, which shall be only one of the following:

- Initial authorization
- Ongoing authorization
- Reauthorization

[CDM PMO] [CONDITIONALLY REQUIRED] *(Note: "Conditionally required" because these types may not apply to the given system boundary.)*

AuthorizingOfficial – An attribute that captures the name(s) of a senior federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the

use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the nation. [NIST 800-53]

Availability – An attribute that captures the availability component of the FIPS 199 impact level. (See **FIPS 199 Impact Level Component: Availability** in Data Model Key Terms for additional context.) Values for this attribute shall be only one of the following:

- LOW
- MOD (moderate)
- HIGH

[CDM PMO] [REQUIRED]

Confidentiality – An attribute that captures the confidentiality component of the FIPS 199 impact level. (See **FIPS 199 Impact Level Component: Confidentiality** in Data Model Key Terms for additional context.) Values for this attribute shall be only one of the following:

- LOW
- MOD (moderate)
- HIGH

[CDM PMO] [REQUIRED]

HVAFlag – An attribute that captures whether the agency is identifying the FISMA system as containing high-value assets. [CDM PMO] [REQUIRED]

LastTimeAssessmentReviewed – An attribute that captures the review date of the most recent security assessment for the system boundary. [CDM PMO]

ImpactLevel – An attribute that captures the global FIPS 199 impact level across the confidentiality, integrity, and availability components. This attribute is synonymous with *"FIPS High Water Mark."* (See **FIPS 199 Impact Components** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

Integrity – An attribute that captures the integrity component of the FIPS 199 impact level (see **FIPS 199 Impact Level Component: Integrity** in Data Model Key Terms for additional context). Values for this attribute shall be only one of the following:

- LOW
- MOD (moderate)
- HIGH

[FIPS 199]

Subsystem – An attribute that identifies a major subdivision of an information system. It must be associated with at least one Systemboundary without the subsystem attribute. There may be multiple subsystems associated with one Systemboundary. This attribute is Boolean. [CDM PMO]

SystemAWARECSMSubScoreAVG – A **derived** attribute that captures the average secure configuration management AWARE risk posture sub-score (e.g., open misconfigurations/CCEs) associated with all

agency assets assigned to an information system. [CDM PMO] [REQUIRED]

SystemAWARECSMSubScoreSUM – A **derived** attribute that captures the aggregated secure configuration management AWARE risk posture sub-score (e.g., open misconfigurations/CCEs) associated with all agency assets assigned to an information system. [CDM PMO] [REQUIRED]

SystemAWAREScore – A **derived** attribute that captures the aggregated AWARE risk posture score associated with all agency assets assigned to an information system. [CDM PMO] [REQUIRED]

SystemAWAREUAHSubscore – A **derived** attribute that captures the calculated unauthorized device AWARE risk posture sub-score (i.e., unauthorized as described above in the Data Model Key Terms section) associated with all agency assets assigned to an information system. [CDM PMO] [REQUIRED]

SystemAWAREVULSubScoreAVG – A **derived** attribute that captures the average vulnerability AWARE risk posture sub-score (e.g., open CVEs) associated with all agency assets assigned to an information system. [CDM PMO] [REQUIRED]

SystemAWAREVULSubScoreSUM – A **derived** attribute that captures the aggregated vulnerability AWARE risk posture sub-score (e.g., open CVEs) associated with all agency assets assigned to an information system. [CDM PMO] [REQUIRED]

SystemBoundaryID – An attribute that captures a unique identifier that details a specific system boundary. This will be the unique key, name, or descriptor to identify a [FISMA] system for future reporting and reference. (See **System** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

SystemBoundaryName – An attribute that captures the simple name of the system boundary for ease of practical identification and to enable the potential identification of the system business mission. [CDM PMO] [REQUIRED]

SystemOwner – An attribute that captures the full name of the organization official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements) and for ensuring compliance with security requirements. [NIST 800-37] [CDM PMO]

ThreatIntelligence – An entity that captures relevant information about available threat intelligence that has been correlated to some cyber-relevant information within the CDM system. [CDM PMO] [REQUIRED]

CVEAttackingEase – An attribute that captures the level of ease with which the CVE can be successfully exploited. [CDM PMO]

CVEExploit – An attribute that captures the level and severity of exploitation-related activity occurring "in the wild" for a specific CVE. [CDM PMO]

CVEMitigation – An attribute that captures the mitigation activities available for the CVE (e.g., implement web application firewall, patch). [CDM PMO]

CVERiskRating – An attribute that captures an expert assessment, sourced from threat intelligence sources, of a specific CVE's relative risk. [CDM PMO]

CVEVendorFix – An attribute that captures information (i.e., descriptions, URLs) relating to vendor-issued fix(es) or patches for the specific CVE. [CDM PMO] [REQUIRED]

IntelligenceReportIOC – An attribute that captures specific IOCs included in a threat intelligence feed report/product (e.g., file hashes, domain name, IP addresses, signatures). [CDM PMO]

IntelligenceReportName – An attribute that captures the name and/or title of a **ThreatIntelligence**. [CDM PMO]

IntelligenceReportPublishedDate – An attribute that captures the date threat intelligence was published by the originating source (e.g., vendor/provider, organization). [CDM PMO]

IntelligenceReportSummary – An attribute that captures the executive-level summary and/or findings of the threat intelligence. [CDM PMO]

IntelligenceReportType – An attribute that captures the type of threat intelligence that was correlated to CDM system information. The attribute may be one of the following:

- Vulnerability– Threat intelligence that is focused on specific vulnerabilities/CVEs.
- Threat– Threat intelligence that generically focuses on certain TTPs, actors, or active campaigns. [CDM PMO]

ThreatIntelligenceID – An attribute that captures a unique identifier for each threat intelligence feed report/product. [CDM PMO] [REQUIRED]

ToolSensorDeviceOnNetwork [*DeviceOnNetwork Specialization*] – An entity that captures the relevant information about CDM tools or sensors employed to capture cyber-relevant conditions or information (e.g., vulnerability, misconfiguration, etc.). **ToolSensorDeviceOnNetwork** is a specialization (subclass) of **DeviceOnNetwork** and serves a specific CDM-based role on the network. The information in this entity supports enumeration of cyber technologies that are used to perform CDM capabilities. [CDM PMO] [REQUIRED]

NVDLastUpdateDate – An attribute that captures the date the vulnerability, configuration settings scanner, or relevant components within the scanner (e.g., scanner definition data, plug-in updates) were last updated with the latest NVD-relevant information for scanning purposes (e.g., new definitions for updated or newly discovered CVEs). [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because some tools do not receive updates from NVD. Not all tools or sensors will require an NVD-relevant update activity. This attribute is vital for tools whose efficacy for detecting information (e.g., CVEs, CPEs, CCEs) is determined by how current its configuration files are.*)

ToolSensorProduct – This attribute captures the most common and recognizable title or name of the **ToolSensor** (e.g., Nessus® Professional). [CDM PMO] [REQUIRED]

ToolSensorType – An attribute that captures the CDM capability that the tool/sensor supports. The attribute can be one or more of the following values:

- VUL
- CSM
- MTD
- EMM
- HWAM
- SWAM
- BOUND-F: NETWORK ACCESS PROTECTION

- MNGEVT

[CDM PMO] [REQUIRED]

ToolSensorUpdate – This attribute captures the particular update, service pack, or point release of the **ToolSensor** (e.g., Hotfix 5). [CDM PMO] [REQUIRED]

ToolSensorVersion – This attribute captures the vendor-specified identification of the particular release version of the **ToolSensor** (e.g., version 6.10.5). [CDM PMO] [REQUIRED]

ToolSensorVendor – This attribute captures person or organization (e.g., corporation) that manufactured or created the product (e.g., Tenable Inc.). [CDM PMO] [REQUIRED]

TRUST – An entity that describes a specified degree of trust granted to a user. Examples include background investigations such as a National Agency Check (NAC), NAC with Written Inquiries (NACI), Access NACI or Single Scope Background Investigation (SSBI) resulting in a security clearance determination (e.g., Secret or Top Secret); an FBI National Criminal History Check (NCHC); non-disclosure agreements; and "read-ons" for access to sensitive data. [CDM PMO] [REQUIRED]

DateTRUSTStatusInitiated – An attribute that captures the date when a **TRUST** element's status last underwent any of the following events:

- **Any** change of state (e.g., from AUTHORIZED to REVOKED, PENDING to AUTHORIZED) including:
  - Date when **TRUST** is first AUTHORIZED or first classified as PENDING.
  - RE-AUTHORIZED (i.e., renewed whereby the state remains AUTHORIZED but new date data is acquired through updating the **DateTRUSTStatusInitiated** attribute with a new date).

[CDM PMO]

TRUSTCreationDate – An attribute that captures the date **TRUST** was originally completed/tracked. [CDM PMO]

TRUSTDescription – An attribute that allows for descriptive text to add context or clarity to an instance of the **TRUST** element (e.g., description of unique agency **TRUST** types, adding supplemental guidance or context for the establishment of **TRUST** to a specific user, etc.). [CDM PMO]

TRUSTExpirationDate – An attribute that captures the date when a security-related **TRUST** entity (e.g., record) becomes invalid. [CDM PMO] (***Note:*** *This attribute should be updated when* ***TRUST*** *elements are reauthorized or updated as part of a recurring review/reinvestigation process.*)

TRUSTID – An attribute that captures a universally unique identifier referencing a specific **TRUST** instance. [CDM PMO] [REQUIRED]

TRUSTName – An attribute that captures an agency-specified common name for each **TRUST** instance captured by the CDM system (e.g., SSBI for TS/SCI Clearance). [CDM PMO]

TRUSTReviewDate – A date attribute that captures the last known time a **TRUST** review was conducted. [CDM PMO] [CONDITIONALLY REQUIRED]

TRUSTReviewGracePeriod – An attribute that captures a period of time, in days, indicating the agency-defined periodicity for a TRUST review, such that when it is exceeded by **TRUSTReviewDate**, some

agency-defined action is required, as dictated by policy (e.g., immediate review triggered or required; notification to security office). [CDM PMO]

TRUSTStatus – An attribute that captures the current state of a **TRUST** authorization. The value of this attribute shall be only one of the following values:

- PENDING
- AUTHORIZED
- SUSPENDED
- EXPIRED
- REVOKED

[CDM PMO] [REQUIRED]

TRUSTStatusGracePeriod – An attribute that captures the agency-determined length of time, in days, the **TRUSTStatus** attribute is allowed to remain in any status, beyond which some action is recommended where applicable and as determined by agency policy (e.g., amount of time allowable for a **TRUST** to remain in SUSPENDED status before it is formally REVOKED and/or accounts are DISABLED). [CDM PMO]

TRUSTType – An attribute that categorizes the type of screening/vetting required to establish a given instance of **TRUST**, as defined by agency policy. The value of this attribute shall be only one of the following values for CDM:

- INVESTIGATIVE – A completed and favorably adjudicated Tier 1 investigation.
- SUITABILITY – A process or mechanism to determine the fitness for employment or ability to grant access to resources; the scope of determining suitability may involve a review of personal conduct and/or other agency-determined requirements in addition to other vetting processes (e.g., EOD process).
- ROB – Rules of behavior agreement that is a requirement prior to authorization.
- NDA – Non-disclosure agreement that is a requirement prior to authorization.
- FDA – Financial disclosure agreement (form) that must be completed prior to authorization
- AGENCYOTHER – Any unique agency processes used in the vetting/screening of users before establishing **TRUST** for a user within an agency.

[CDM PMO]

UnauthorizedSWEventOnNetwork [*EventOnNetwork Specialization*] – An entity that captures a specialized event that reports when unauthorized software was attempted or successfully executed on a device as reported by the CDM tool supporting the SWAM capability. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because some agencies may not have access to the **Event Management** or AEC security capabilities necessary to produce this data; therefore, the data is required only for certain CDM solutions that employ **Event Management or AEC**. See **EventOnNetwork** above.)*

DeviceRunOnDeviceIP – An attribute that captures the IP of the device that ran the unauthorized software. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

DeviceRunOnName – An attribute that captures the hostname of the device that ran the unauthorized software. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

SoftwareRunInformation – An attribute that captures the relevant software information from the unauthorized software execution event. This includes information corresponding to the software vendor, software product name/version, and/or software executable name, if available. [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** See above for explanation of "conditionally required.")*

UniqueSoftware – An entity that represents information about a software product inventory item that is discovered in an agency. (See **UniqueSoftware** in Data Model Key Terms for additional context.) [CDM Technical Capabilities, Vol. 2] [CDM PMO] [REQUIRED]

CommonProductName – An attribute that captures an alternate common name used to identify executable software discovered by CDM, such as an alias applied/used by an agency or colloquially used by OEM/industry (e.g., Microsoft Word 2013, Acrobat Pro 10). [CDM PMO] [REQUIRED]

Critical – An attribute that captures whether the software meets the critical software criteria as defined by NIST.[30] [EO 14028]

DateSoftwareInventoryUpdated – An attribute that captures the date a unique software inventory asset's information of record was last updated. [CDM PMO] [REQUIRED]

MobileAppBundleID – An attribute that captures the unique identifier of a mobile app—referred to as a "bundle ID" (iOS) or "package name" (Android)—on a mobile device or within a mobile app marketplace (i.e., Google Play, App Store). [CDM PMO]

MobileAppHash – This attribute captures the cryptographic hash of the app installed on a mobile device. [CDM PMO]

SoftwareEdition – An attribute that captures the vendor-specified identification of the particular release edition of the product.

SoftwareProduct – This attribute captures the most common and recognizable title or name of the unique software product on an agency's network as defined by its CPE WFN or industry. [NIST Interagency Report (IR) 7695] [REQUIRED]

SoftwareType – An attribute that captures the type or general categorization of software being inventoried as reported by CDM tools/sensors (e.g., productivity, games, antivirus, web browser). [CDM PMO] [REQUIRED]

SoftwareUpdate – An attribute that captures the particular update, service pack, or point release of the product (e.g., Microsoft .NET Framework v3.5.1 Update SP1). [NIST IR 7695] [REQUIRED]

SoftwareVersion – An attribute that captures the vendor-specified identification of the particular release version of the product (e.g., McAfee VirusScan version 8.5i). [NIST IR 7695] [REQUIRED]

SoftwareVendor – An attribute that captures a person or organization (e.g., corporation) that manufactured or created the product. [NIST IR 7695] [REQUIRED]

UniqueSoftwareID – An attribute that captures a unique identifier that references a specific inventoried software in the CDM solution. [CDM PMO] [REQUIRED]

[30] Definition of "Critical Software" can be found at Critical Software Definition | NIST.

User – An entity that represents any agent (including both person and non-person agents) that accesses any resource, physical or logical, in an organization. (See **User** in Data Model Key Terms for additional context.) [CDM PMO] [REQUIRED]

DateUserStatusInitiated – An attribute that captures the date when a user's status underwent any of the following events:

- **Any** state change to status (e.g., from ACTIVE to INACTIVE, ACTIVE to SEPARATED).
- User is initially inventoried in the CDM system as ACTIVE, SERVICE, or PENDING.

[CDM PMO]

UserEmailAddress – An attribute that captures an email address for the identified user. [CDM PMO]

UserFirstName – An attribute that allows for the entry of the first name (given name) of a person at an agency. [CDM PMO]

UserID – A unique ID/key that references a specific MUR that can be associated with a user in an agency. [CDM PMO] [REQUIRED]

UserJobTitle – An attribute that captures the specification of a job or role title (e.g., job series, functional responsibilities) of a person as determined by an agency. [CDM PMO]

UserLastName – An attribute that allows for the entry of the last name (family name) of a person at an agency with a generational qualifier (e.g., Sr., Jr., III), if this is required by agency policy. [CDM PMO]

UserMiddleName – An attribute that captures the entry of a middle name (if available) of a person at an agency. [CDM PMO]

UserPhoneNumber – An attribute that captures a phone number that can be used to contact the identified user. [CDM PMO]

UserReviewDate – An attribute that captures the last known date a user review was conducted. [CDM PMO]

UserReviewGracePeriod – An attribute that captures a period of time, in days, indicating the agency-defined periodicity for user reviews, such that when it is exceeded by **UserReviewDate**, some agency-defined action is required as dictated by policy (e.g., immediate review triggered or required; notification to security office). [CDM PMO]

UserStatus – An attribute that captures the last reported status of a user. The status shall be only one of the following values:

- SEPARATED – User no longer actively exists within the agency (a permanent status with no anticipated return).
- ACTIVE – User currently is active within the agency (i.e., employed or contracted).
- SERVICE – Reserved for non-person entities; indicates privileges/accounts associated with this NPE are still in use.
- INACTIVE – Reserved for temporary absences that are coordinated with the agency (e.g., Family and Medical Leave Act absence, sabbatical, detail).
- PENDING – Users who may not be active yet or are in the process of being on-boarded, vetted, trained, or otherwise prepared for duty.

[CDM PMO]

UserType – An attribute that captures a type of user. The value of this attribute shall be one of the following:

- GOVERNMENT – Representing an organization/government person entity (i.e., human being)
- CONTRACTOR – Representing a contractor person entity (i.e., human being)
- NONPERSON – Representing a non-person entity. (See **Non-Person Entity** in Data Model Key Terms for additional context.)
- OTHER GOVT AGENCY – Representing a detailee or other assigned entity from another government agency that has been incorporated into the agency's IT environment on a temporary basis.

[CDM PMO]

UserImpactByIncident – An entity that represents a record of all security-relevant impact information resulting from a confirmed security incident. [CDM PMO]

DescriptionofUserImpact – An attribute that captures a description of the scope of an incident and its impact on user(s) at the agency (e.g., loss of PII, compromised credentials). [CDM PMO]

VulnerabilityOnNetwork – An entity that represents a single discovered vulnerability within an agency, which is further defined as a CVE that exists on software installed on an agency device and detected by a CDM tool or sensor. The scope of applicable CVEs that can constitute a software-based vulnerability includes information available in the NVD. [CDM PMO] [REQUIRED]

DateofVulScan – An attribute that captures the date of the last (most recent) vulnerability scan that found the vulnerability on a device within the agency's network. [CDM PMO] [REQUIRED] (***Note***: *This attribute should reflect the last time that a vulnerability was "seen" or updated through a scanning process. If no new relevant details about a vulnerability are discovered but the vulnerability is still seen, this attribute would be updated with the last date the sensor witnessed the vulnerability.*)

VULID – An attribute that captures a unique identifier referencing a specific discovered vulnerability on an agency's network. [CDM PMO] [REQUIRED]

VulnerableSoftwareInfo – An attribute that captures the information about the software that has an associated discovered CVE **as reported by** the CDM VUL tool/sensor.

Required data for this attribute:

- The CDM PMO recognizes that the CPE standard in its present form, as supported by the vendor community, is not a viable naming schema for the CDM solution. Therefore, it is expected that integrators shall, to the fullest extent possible, rely on the common naming schema as furnished by the CDM dashboard ecosystem **and** include at minimum:
  - Vendor Name
  - Common Product Name
  - Version
  - CVE Detection Signature Identifier – A vendor-provided value that identifies the software module(s) used by the VUL tool to detect the vulnerability.

- Installation File Path – The installation location of the vulnerable software.

[CDM PMO] [REQUIRED]

VULFixText – An attribute provided by the VUL tool that captures the clear and simple description of how to correct the vulnerability; this shall include the version of the software that remediates the vulnerability. [CDM PMO] [REQUIRED]

VULOriginalDiscoveryDate – An attribute that captures the date when the **VulnerabilityOnNetwork** was first discovered. [AWARE Technical Design] [REQUIRED]

VULRemediationDate – An attribute that captures the date a vulnerability was remediated (e.g., vulnerable software patched or removed). [CDM PMO] [CONDITIONALLY REQUIRED] *(**Note:** "Conditionally required" because the vulnerability may not yet be remediated.)*

VULStatus – An attribute that captures the status of a particular **VulnerabilityOnNetwork**. The attribute shall be one of the following:

- OPEN
- RISK ACCEPTED – Vulnerability has currently been accepted and is not expected to be remediated due to some exigent circumstances.
- REMEDIATED – Vulnerability has been remediated and is no longer detected by tool/sensors.

[AWARE Technical Design] [REQUIRED]

APPENDIX A: REFERENCES

2021. "Agency-Wide Adapative Risk Enumeration (AWARE) Design Document." *Version 1.5a.* December.

Barker, Elaine. 2020. "Recommendation for Key Management: Part 1- General." *NIST Special Publication 800-57 Part 1 Revision 5.*

Brant Cheikes (MITRE), David Waltermire (NIST), Karen Scarfone (Scarfone Cybersecurity). 2011. "Managing Information Security Risk: Organization, Mission, and Information System View." *NIST SP 800-39.*

CAPEC. 2021. *CAPEC LIST VERSION 3.9.* October 21. https://capec.mitre.org/data/index.html.

CDM. *CDM Dashboard Data Target.* Accessed August 2023. https://confluence.cdmdashboard.com/display/CDE/Dashboard+Data+Target. (registration required).

CISA. *Cyber Hygiene Services*. Accessed August 2023. https://www.cisa.gov/cyber-hygiene-services.

CISA. 2017. *Federal Incident Notification Guidelines*. April 1. https://www.cisa.gov/incident-notification-guidelines.

CISA. 2021. "FY 2021 CIO FISMA Metrics," Version 1.1. August. https://www.cisa.gov/sites/default/files/publications/FY_2021_FISMA_CIO_Metrics-v1.1.pdf.

CISA. 2023. "FY 2023 CIO FISMA Metrics," Version 2.0. June 2023. https://www.cisa.gov/sites/default/files/2023-06/FY23_FISMA_CIO_Metrics_v2_May-2023-Final_508.pdf.

CISA. 2018. *BOD 18-01*: *Securing High Value Assets.* May 7. https://www.cisa.gov/news-events/directives/bod-18-02-securing-high-value-assets.

CISA. 2019. *BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems.* April 29. https://www.cisa.gov/news-events/directives/bod-19-02-vulnerability-remediation-requirements-internet-accessible-systems.

2017. "Continuous Diagnostics and Mitigation Technical Capabilities." Volume 1: Defining Actual and Desired States.

2021**.** "Continuous Diagnostics and Mitigation Technical Capabilities." Volume Two: Requirements Catalog," Version 2.4.

D. Cooper NIST, S. Santesson. 2008. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." Internet Standards.

2017. *Federal Incident Notification Guidelines.* April 1. https://www.cisa.gov/federal-incident-notification guidelines.

Fenton, Paul A. Grassi Michael E. Garcia James L. 2017. "Digital Identity Guidelines." *NIST Special Publication 800-63-3.*

2004. "FIPS Pub 199." *Standards for Security Categorization of Federal Incident Notification Guidelines .* February.

FORCE, JOINT TASK. 2022. "Assessing Security and Privacy Controls in Information Systems and Organizations." *NIST Special Publication 800-53A.*

FORCE, JOINT TASK. 2018. "Risk Management Framework for Information Systems and Organizations."

FORCE, JOINT TASK. 2013. "Security and Privacy Controls for Federal Information Systems." *NIST Special*

Publication 800-53.

Handbook, Department of Homeland Security Sensitive Policy. 2023. *DHS Sensitive Systems Policy Documents (4300A).* May 31.

Initiative, Joint Task Force Transformation. 2019. “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. *NIST SP 800-37.*

Initiative, Joint Task Force Transformation. 2011. "Managing Information Security Risk: Organization, Mission, and Information System View." *NIST SP 800-39.*

Initiative, Joint Task Force Transformation. 2012. "NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments."

Kelley Dempsey (NIST), Nirali Chawla (PwC), L. Johnson (NIST), Ronald Johnston (DoD), Alicia Jones (BAH), Angela Orebaugh (BAH), Matthew Scholl (NIST), Kevin Stine (NIST). 2011. "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations." 80.

2017. *Malware Attribute Enumeration and Characterization.* October 9. https://maecproject.github.io/.

Marianne Swanson (NIST), Joan Hash (NIST), Pauline Bowen (NIST). 2006. "Guide for Developing Security Plans for Federal Information Systems."

Paul Cichonski. Tom Millar, Tim Grance, Karen Scarfone. 2012. "Recommendations of the National Institute of Standards and Technology." *Computer Security Handling Guide.*

Veris. n.d. *the vocabulary for event recording and incident sharing.* Accessed July 2023. https://verisframework.org/.

APPENDIX B: THREAT ACTION VALUES

ThreatActionVariety Values for **ThreatActionCategory** = "MALWARE"

ThreatActionVariety Value	Description
ADMINWARE	System or network utilities (e.g., PsTools, Netcat). [VERIS]
ADWARE	Any software that is funded by advertising. Adware may also gather sensitive user information from a system. [VERIS] [MAEC]
APPENDER	File-infecting malware that places its code at the end of the files it infects, adjusting the file's entry point to cause its code to be executed before that in the original file. [MAEC]
BACKDOOR	Malware which, once running on a system, opens a communication vector to the outside so the computer can be accessed remotely by an attacker. [VERIS] [MAEC]
BOOT-SECTOR-VIRUS	Malware that infects the master boot record of a storage device. [MAEC]
BRUTE FORCE	Brute force attack. [VERIS]
CAPTURE APP DATA	Capture data from application or system process. [VERIS]
CAPTURE STORED DATA	Capture data stored on system disk. [VERIS]
CAVITY-FILLER	A type of file-infecting virus that seeks unused space within the files it infects, inserting its code into these gaps to avoid changing the size of the file and thus not alerting integrity-checking software to its presence. [MAEC]
CLICKER	A Trojan that makes a system visit a specific web page, often very frequently and usually with the aim of increasing the traffic recorded by the site and thus increasing revenue from advertising. Clickers may also be used to carry out DDoS attacks. [MAEC]
COMPANION-VIRUS	A virus that takes the place of a particular file on a system instead of injecting code into it. [MAEC]
CLIENT-SIDE ATTACK	Client-side or browser attack (e.g., redirection, XSS, MitB). [VERIS]
CLICK FRAUD	Click fraud or Bitcoin mining. [VERIS]
C2	Command and control (C2). [VERIS]
DATA-DIDDLER	A type of malware that makes small, random changes to data, such as data in a spreadsheet, to render the data contained in a document inaccurate and in some cases worthless. [MAEC]
DESTROY DATA	Destroy or corrupt stored data. [VERIS]
DISABLE CONTROLS	Disable or interfere with security controls. [VERIS]
DDOS/DOS	A tool used to perform a distributed denial of service attack. [VERIS] [MAEC]
DOWNLOADER	Downloader (pull updates or other malware): malware programmed to download and execute other files, usually more complex malware. [VERIS] [MAEC]
DROPPER	A type of Trojan that deposits an enclosed payload onto a destination host computer by loading itself into memory, extracting the malicious payload, and then writing it to the file system. [MAEC]

ThreatActionVariety Value	Description
EXPLOIT-KIT / EXPLOIT VULN	A software toolkit to target common vulnerabilities. [VERIS] [MAEC]
EXPORT DATA	Export data to another site or system. [VERIS]
FILE-INFECTOR-VIRUS	A virus that infects a system by inserting itself somewhere in existing files; this is the "classic" form of virus. [MAEC]
FILE-LESS	Malware that is file-less, i.e., executes through some other mechanism such as PowerShell. [MAEC]
FORK-BOMB	A simple form of malware, a type of rabbit which launches more copies of itself. Once a fork-bomb is executed, it will attempt to run several identical processes, which will do the same, the number growing exponentially until the system resources are overwhelmed by the number of identical processes running, which may in some cases bring the system down and cause a denial of service. [MAEC]
GREYWARE	Software that, while not definitely malicious, has a suspicious or potentially unwanted aspect. [MAEC]
IMPLANT	Code inserted into an existing program using a code patcher or other tool. [MAEC]
KEYLOGGER	A type of program implanted on a system to monitor the keys pressed and thus record any sensitive data, such as passwords, entered by the user. [MAEC] [VERIS]
KLEPTOGRAPHIC-WORM	A worm that encrypts information assets on compromised systems so they can only be decrypted by the worm's author; also known as information-stealing worm. [MAEC]
MACRO-VIRUS	A virus that uses a macro language, for example in Microsoft Office documents. [MAEC]
MALWARE-AS-A-SERVICE	Malware that is sold or produced as a service. [MAEC]
MASS-MAILER	A worm that uses email to propagate across the internet. [MAEC]
METAMORPHIC-VIRUS	A virus that changes its own code with each infection. [MAEC]
MULTIPARTITE-VIRUS	Malware that infects boot records, boot sectors, and files. [MAEC]
MID-INFECTOR	A type of file-infecting virus which places its code in the middle of files it infects. It may move a section of the original code to the end of the file, or simply push the code aside to make space for its own code. [MAEC]
MOBILE-CODE	Either (a) code received from remote, possibly untrusted systems, but executed on a local system or (b) software transferred between systems (e.g., across a network) and executed on a local system without explicit installation or execution by the recipient. [MAEC]
MULTIPARTITE-VIRUS	Malware that infects boot records, boot sectors, and files. [MAEC]
PARENTAL-CONTROL	A program that monitors or limits machine usage. Such programs can run undetected and can transmit monitoring information to another machine. [MAEC]
PACKET SNIFFER	Packet sniffer (capture data from network). [VERIS]
PASSWORD-STEALER / PASSWORD DUMPER	A type of Trojan designed to steal passwords (or extract credential hashes), personal data and details, or other sensitive information from an infected system. [VERIS] [MAEC]

ThreatActionVariety Value	Description
POLYMORPHIC-VIRUS	A type of virus that encrypts its code differently with each infection (or with each generation of infections). [MAEC]
PREMIUM-DIALER-SMSER	A type of malware whose primary aim is to dial (or send SMS messages to) premium rate numbers. [MAEC]
PREPENDER	A file-infecting virus that inserts code at the beginning of the files it infects. [MAEC]
RAM SCRAPER	Ram scraper or memory parser (capture data from volatile memory). [VERIS]
RANSOMWARE	Ransomware (encrypt or seize stored data): malware that encrypts files on a victim's system, demanding payment of ransom in return for the access codes required to unlock files. [VERIS] [MAEC]
REMOTE-ACCESS-TROJAN (RAT)	A remote access Trojan program, or RAT, is a Trojan horse capable of controlling a machine through commands issued by a remote attacker. [MAEC]
RESOURCE-EXPLOITER	A type of malware that steals a system's resources (e.g., CPU cycles), such as a bitcoin miner. [MAEC]
ROGUE-SECURITY-SOFTWARE	A fake security product that demands money to clean phony infections. [MAEC]
ROOTKIT	Rootkit (maintain local privileges and stealth): A method of hiding files or processes from normal methods of monitoring; often used by malware to conceal its presence and activities. [VERIS] [MAEC]
SCAN NETWORK	Scan or footprint network. [VERIS]
SCAREWARE	A program that reports false or significantly misleading information on the presence of security risks, threats, or system issues on the target computer. [MAEC]
SCREEN-CAPTURE	A type of malware used to capture images from the target systems screen, used for exfiltration and command and control. [MAEC]
SECURITY-ASSESSMENT-TOOL	A program that can be used to gather information for unauthorized access to computer systems. [MAEC]
SHELLCODE	Either (a) a small piece of code that activates a command-line interface to a system that can be used to disable security measures, open a backdoor, or download further malicious code or (b) a small piece of code that opens a system up for exploitation, sometimes by not necessarily involving a command-line shell.
SPAM	Send spam. [VERIS]
SPYWARE	Software that gathers information and passes it to a third-party without adequate permission from the owner of the data. It may also refer to software that makes changes to a system or any of its component software, or which makes use of system resources without the full understanding and consent of the system owner. [MAEC] [VERIS]
SQL INJECTION	SQL injection attack. [VERIS]
TRACKWARE	Malware that traces a user's path on the internet and sends information to third parties. Compare to spyware, which monitors system activity to capture confidential information such as passwords.
TROJAN	Malware disguised as something inert or benign. [VERIS]

ThreatActionVariety Value	Description
VIRUS	Self-replicating malware that requires human interaction to spread; also, self-replicating malware that runs and spreads by modifying and inserting itself into other programs or files. [MAEC]
WEB-BUG	Code embedded in a web page or email that checks whether a user has accessed the content (e.g., a tiny, transparent GIF image). [MAEC]
WIPER	Malware that deletes files or entire disks on a machine. [MAEC]
WORM	Self-replicating malware that propagates across a network either with or without human interaction. [VERIS] [MAEC]
UNKNOWN	Unknown [VERIS]
OTHER	Other [VERIS]

ThreatActionMethod Values for **ThreatActionCategory** = "MALWARE"

ThreatActionMethod Value	Description
AUTO-EXECUTING-MEDIA	The malware instance or family was delivered via media that automatically executes. [MAEC]
DIRECT INSTALL [VERIS] / ACTIVE ATTACKER [MAEC]	Directly installed or inserted by threat agent/attacker (after system access). [VERIS] [MAEC]
DOWNLOAD BY MALWARE [VERIS] / DOWNLOADER [MAEC]	Downloaded and installed by local malware, delivered by downloader. [VERIS] [MAEC]
DROPPER	The malware instance or family was delivered via dropper.
EMAIL AUTOEXECUTE	Email via automatic execution. [VERIS]
EMAIL LINK	Email via embedded link. [VERIS]
EMAIL ATTACHMENT	Email via user-executed attachment. [MAEC] [VERIS]
EXPLOIT-KIT-LANDING-PAGE	The malware instance or family was delivered via an exploit kit landing page. [MAEC]
FAKE-WEBSITE	The malware instance or family was delivered via a fake website. [MAEC]
INSTANT MESSAGING	Instant messaging [VERIS]
JANITOR-ATTACK	The malware instance or family was delivered via a janitor attack. [MAEC]
MALICIOUS-IFRAMES	The malware instance or family was delivered via malicious iframes. [MAEC]
MEDIA-BAITING	The malware instance or family was delivered via media baiting. [MAEC]
NETWORK PROPAGATION	Network propagation [VERIS]
PHARMING	The malware instance or family was delivered via pharming. [MAEC]
PHISHING	The malware instance or family was delivered via phishing. [MAEC]
REMOTE INJECTION	Remotely injected by agent (i.e., via SQLi). [VERIS]
REMOVABLE MEDIA	Removable storage media or devices. [VERIS]
TROJANIZED-LINK	The malware instance or family was delivered via a trojanized link. [MAEC]
TROJANIZED-SOFTWARE	The malware instance or family was delivered via trojanized software. [MAEC]
WEB DRIVE-BY [VERIS] / MALVERTISING [MAEC]	Web via auto-executed or "drive-by" infection (e.g., delivered via malvertising.) [VERIS] [MAEC]
WEB DOWNLOAD	Web via user-executed or downloaded content. [VERIS]
WATERING-HOLE	The malware instance or family was delivered via a watering hole. [MAEC]
UNKNOWN	Unknown [VERIS]
USB-CABLE-SYNCING	The malware instance or family was delivered via USB cable syncing. [MAEC]
OTHER	Other [VERIS]

ThreatActionVariety Values for **ThreatActionCategory** = "HACKING" [VERIS]

ThreatActionVariety Value	Description
ABUSE OF FUNCTIONALITY	Abuse of functionality
BRUTE FORCE	Brute force or password guessing attacks
BUFFER OVERFLOW	Buffer overflow
CACHE POISONING	Cache poisoning
SESSION PREDICTION	Credential or session prediction
CSRF	Cross-site request forgery
XSS	Cross-site scripting
CRYPTANALYSIS	Cryptanalysis
DOS	Denial of service
FOOTPRINTING	Footprinting and fingerprinting
FORCED BROWSING	Forced browsing or predictable resource location
FORMAT STRING ATTACK	Format string attack
FUZZ TESTING	Fuzz testing
HTTP REQUEST SMUGGLING	HTTP request smuggling
HTTP REQUEST SPLITTING	HTTP request splitting
INTEGER OVERFLOWS	Integer overflows
LDAP INJECTION	LDAP injection
MAIL COMMAND INJECTION	Mail command injection
MITM	Man-in-the-middle attack
NULL BYTE INJECTION	Null byte injection
OFFLINE CRACKING	Offline password or key cracking (e.g., rainbow tables, Hashcat, JtR)
OS COMMANDING	OS commanding
PATH TRAVERSAL	Path traversal
RFI	Remote file inclusion
REVERSE ENGINEERING	Reverse engineering
ROUTING DETOUR	Routing detour
SESSION FIXATION	Session fixation
SESSION REPLAY	Session replay
SOAP ARRAY ABUSE	Soap array abuse
SPECIAL ELEMENT INJECTION	Special element injection
SSI INJECTION	SSI injection
URL REDIRECTOR ABUSE	URL redirector abuse
USE OF BACKDOOR OR C2	Use of backdoor or C3
USE OF STOLEN CREDS	Unauthorized use of credentials
XML ATTRIBUTE BLOWUP	XML attribute blowup
XML ENTITY EXPANSION	XML entity expansion
XML EXTERNAL ENTITIES	XML external entities

ThreatActionVariety Value	Description
XML INJECTION	XML injection
XPATH INJECTION	XPath injection
XQUERY INJECTION	Xquery injection
VIRTUAL MACHINE ESCAPE	Virtual machine escape
UNKNOWN	Unknown
OTHER	Other

ThreatActionMethod Values for **ThreatActionCategory** = "HACKING" [VERIS]

ThreatActionMethod Value	Description
3RD PARTY DESKTOP	Third-party online desktop sharing (LogMeIn, Go2Assist)
BACKDOOR OR C2	Backdoor or command and control channel
DESKTOP SHARING	Graphical desktop sharing (RDP, VNC, PCAnywhere, Citrix)
PHYSICAL ACCESS	Physical access or connection (i.e., at keyboard or via cable)
COMMAND SHELL	Remote shell
PARTNER	Partner connection or credential
VPN	VPN
WEB APPLICATION	Web application
UNKNOWN	Unknown
OTHER	Other

ThreatActionVariety Values for **ThreatActionCategory** = "SOCIAL" [VERIS]

ThreatActionVariety Value	Description
BAITING	Baiting (planting infected media)
BRIBERY	Bribery or solicitation
ELICITATION	Elicitation (subtle extraction of info through conversation)
EXTORTION	Extortion or blackmail
FORGERY	Forgery or counterfeiting (fake hardware, software, documents, etc.)
INFLUENCE	Influence tactics (leveraging authority or obligation, framing, etc.)
SCAM	Online scam or hoax (e.g., scareware, 419 scam, auction fraud)
PHISHING	Phishing (or any type of *ishing)
PRETEXTING	Pretexting (dialogue leveraging invented scenario)
PROPAGANDA	Propaganda or disinformation
SPAM	Spam (unsolicited or undesired email and advertisements)
UNKNOWN	Unknown
OTHER	Other

ThreatActionMethod Values for **ThreatActionCategory** = "SOCIAL" [VERIS]

ThreatActionMethod Value	Description
DOCUMENTS	Documents
EMAIL	Email
IN-PERSON	In-person
IM	Instant messaging
PHONE	Phone
REMOVABLE MEDIA	Removable storage media
SMS	SMS or texting
SOCIAL MEDIA	Social media or networking
SOFTWARE	Software
WEBSITE	Website
UNKNOWN	Unknown
OTHER	Other

ThreatActionVariety Values for **ThreatActionCategory** = "MISUSE" [VERIS]

ThreatActionVariety Value	Description
KNOWLEDGE ABUSE	Abuse of private or entrusted knowledge
PRIVILEGE ABUSE	Abuse of system access privileges
EMBEZZLEMENT	Embezzlement, skimming, and related fraud
DATA MISHANDLING	Handling of data in an unapproved manner
EMAIL MISUSE	Inappropriate use of email or IM
NET MISUSE	Inappropriate use of network or web access
ILLICIT CONTENT	Storage or distribution of illicit content
UNAPPROVED WORKAROUND	Unapproved workaround or shortcut
UNAPPROVED HARDWARE	Use of unapproved hardware or devices
UNAPPROVED SOFTWARE	Use of unapproved software or services
UNKNOWN	Unknown
OTHER	Other

ThreatActionMethod Values for **ThreatActionCategory** = "MISUSE" [VERIS]

ThreatActionMethod Value	Description
PHYSICAL ACCESS	Physical access within corporate facility
LAN ACCESS	Local network access within corporate facility
REMOTE ACCESS	Remote access connection to corporate network (i.e., VPN)
NON-CORPORATE	Non-corporate facilities or networks
UNKNOWN	Unknown
OTHER	Other

ThreatActionVariety Values for **ThreatActionCategory** = "ERROR" [VERIS]

ThreatActionVariety Value	Description
CLASSIFICATION ERROR	Classification or labeling error
DATA ENTRY ERROR	Data entry error
DISPOSAL ERROR	Disposal error
GAFFE	Gaffe (social or verbal slip)
LOSS	Loss or misplacement
MAINTENANCE ERROR	Maintenance error
MISCONFIGURATION	Misconfiguration
MISDELIVERY	Misdelivery (direct or deliver to wrong recipient)
MISINFORMATION	Misinformation (unintentionally giving false info)
OMISSION	Omission (something intended, but not done)
PHYSICAL ACCIDENTS	Physical accidents (e.g., drops, bumps, spills)
CAPACITY SHORTAGE	Poor capacity planning
PROGRAMMING ERROR	Programming error (flaws or bugs in custom code)
PUBLISHING ERROR	Publishing error (private info to public doc or site)
MALFUNCTION	Technical malfunction or glitch
UNKNOWN	Unknown
OTHER	Other

ThreatActionMethod Values for **ThreatActionCategory** = "ERROR" [VERIS]

ThreatActionMethod Value	Description
RANDOM ERROR	Random error (no reason, no fault)
CARELESSNESS	Carelessness
INADEQUATE PERSONNEL	Inadequate or insufficient personnel
INADEQUATE PROCESSES	Inadequate or insufficient processes
INADEQUATE TECHNOLOGY	Inadequate or insufficient technology resources
UNKNOWN	Unknown
OTHER	Other

ThreatActionVariety Values for **ThreatActionCategory** = "PHYSICAL" [VERIS]

ThreatActionVariety Value	Description
ASSAULT	Assault (threats or acts of physical violence)
SABOTAGE	Sabotage (deliberate damaging or disabling action)
SNOOPING	Snooping (sneak about to gain info or access)
SURVEILLANCE	Surveillance (monitoring and observation)
TAMPERING	Tampering (alter physical form or function)
THEFT	Theft (taking assets without permission)
WIRETAPPING	Wiretapping (physical tap to comms line)
UNKNOWN	Unknown
OTHER	Other

ThreatActionMethod Values for **ThreatActionCategory** = "PHYSICAL" [VERIS]

ThreatActionMethod Value	Description
PRIVILEGED ACCESS	Held privileged access to location
VISITOR PRIVILEGES	Given temporary visitor access
BYPASSED CONTROLS	Bypassed physical barriers or controls
DISABLED CONTROLS	Disabled physical barriers or controls
UNCONTROLLED LOCATION	The location was uncontrolled (public)
UNKNOWN	Unknown
OTHER	Other

ThreatActionVariety Values for **ThreatActionCategory** = "ENVIRONMENTAL" [VERIS]

ThreatActionVariety Value	Description
DETERIORATION	Deterioration and degradation
EARTHQUAKE	Earthquake
EMI	Electromagnetic interference (EMI)
ESD	Electrostatic discharge (ESD)
TEMPERATURE	Extreme temperature
FIRE	Fire
FLOOD	Flood
HAZMAT	Hazardous material
HUMIDITY	Humidity
HURRICANE	Hurricane
ICE	Ice: Ice and snow
LANDSLIDE	Landslide
LIGHTNING	Lightning
METEORITE	Meteorite
PARTICULATES	Particulate matter (e.g., dust, smoke)
PATHOGEN	Pathogen
POWER FAILURE	Power failure or fluctuation
TORNADO	Tornado
TSUNAMI	Tsunami
VERMIN	Vermin
VOLCANO	Volcanic eruption
LEAK	Water leak
WIND	Wind
UNKNOWN	Unknown
OTHER	Other

APPENDIX C: RELEASE NOTES FOR THIS VERSION

This appendix provides detailed, itemized lists of changes that were made for this version of the CDM Data Model Document (DMD) as compared to the previous publicly available release. It provides the audience with a mechanism to focus on the most recent relevant changes without having to review the document in its entirety.

General

1. Made requested updates that did not make it into CDM DMD v4.1.1.
2. Updates align with latest FY23 FISMA Metrics, which included major changes to metrics and query considerations.

Section 3 Data Model Key Terms

1. Updated definition of **AWARE** risk posture scoring methodology description and use within document to be more consistent with the AWARE Technical Design Document v1.5 (revised "risk scoring" to "risk posture scoring").
2. Added IoT, OT, and ICS.
3. NCATS references changed to CyHy (Cyber Hygiene) to reflect updated convention.
4. Updated definition of ***System*** to include description of "subsystem" information capture.
5. Updated definitions of Authorizing Official, AWARE, Certificates, Event, and NIST Security Control.
6. Added Critical Software and Known Exploited Vulnerabilities (KEVs).
7. Deleted Device Manager, Device Operator, and Security Content Automation Protocol (SCAP) Validation.

Section 4 Data Dictionary for the Logical Data Model

1. Updated entity ***CCEDictionary.***
    a. Updated attribute ***BenchmarkSettingsCount.***
    b. Added attributes ***BenchmarkName***, ***BenchmarkRelease***, and ***BenchmarkVersion.***
2. Updated entity **CVEDictionary.**
    a. Added attribute ***KEVDateAdded***.
    b. Added attribute ***KEVDescription.***
    c. Added attribute ***KEVDueDate.***
    d. Added attribute ***KEVInCatalogue.***
    e. Added attribute ***KEVRequiredAction.***
    f. Added attribute ***KEVNotes.***
3. Removed ***DeviceManager*** and ***DeviceOperator*** entities.
4. Updated entity ***DeviceOnNetwork*** (including update of ***DeviceCategory*** and ***DeviceType*** based on FY24 CIO FISMA Metrics).
    a. Added attribute ***DeviceOS.***

b. Updated attribute ***DeviceStatus.***

5. Updated entity ***DeviceScan.***
    a. Updated attribute ***CSMSettingsCount.***
    b. Updated attribute ***DeviceScanAuthOutcome.***
    c. Added attribute ***DeviceScanMethod.***
    d. Updated attribute ***DeviceScanType*** (included MTD and EMM).
    e. Added attribute ***ScanBenchmarkName.***
    f. Added attribute ***ScanBenchmarkRelease.***
    g. Added attribute ***ScanBenchmarkVersion.***
6. Updated entity ***SystemBoundary.***
    a. Updated attribute ***AuthorizationDecisionType*** with more accurate type list.
    b. Updated attribute ***AuthorizationDecisionExpirationDate*** to conditionally required.
    c. Added attribute ***AuthorizationType.***
    d. Added attribute ***AuthorizingOfficial.***
    e. Added attribute ***HVAFlag.***
    f. Added attribute ***Subsystem.***
    g. Added attribute ***SystemBoundaryName.***
    h. Added attribute ***SystemOwner.***
7. Updated entity ***UniqueSoftware.***
    a. Removed attribute ***CPEInfo.***
    b. Added attribute ***Critical.***
    c. Added attribute ***SoftwareEdition.***
8. Updated entity ***VulnerabilityOnNetwork.***
    a. Updated attribute ***VulnerableSoftwareInfo*** to describe capture of Plugin information.
    b. Updated attribute ***VULFixText*** to more accurate description of attribute.