Integrated Cyber Defense (ICD) Conceptual Reference Model: White Paper

Version 1.0

Alexander P. Lee, JHU/APL
Jared C. Moon, JHU/APL

Website: https://www.iacdautomate.org/ || **E-Mail**: icd@jhuapl.edu
LinkedIn: https://www.linkedin.com/groups/8608114

Version History

Version No.	Modification	Date
0.1	First draft	July 6, 2018
0.2	Adjudicated internal comments	August 3, 2018
0.3	Consolidating the Orchestration, Activities, and Capabilities Models into this document	September 12, 2018
0.4	Received feedback for formal, internal APL review	December 11, 2018
1.0	Approved for public release; Distribution is Unlimited	February 13, 2019

Table of Contents

Figures

1. Strategic Purpose

The Integrated Cyber Defense (ICD) Conceptual Reference Model captures the overarching **capabilities** (an ability provided by a cybersecurity tool or product), **functions** (an action carried out by a cybersecurity tool or product), and **activities** (representing high-level processes that an organization undertakes to satisfy policy and governance requirements) that enable automation of cyber defense using the sharing of cyber threat information, indicators, and intelligence (CTI3). The capabilities, functions, and activities in the accompanying models are not an all-inclusive list, and the models can be modified or tailored to fit an organization's individual needs.

The intent of this document is help to organizations in the follow three ways:

1. Identify capabilities that are either deployed in their environment or available but not currently utilized. Then among the already deployed capabilities, which ones are currently orchestrated. This information can be useful in avoiding redundant purchases of new functions.
2. Identify gaps in implemented capabilities that prevent successful completion of key activities.
3. Identify activities that need updating based on changes to and expansions of existing capabilities.

There are three models that currently comprise the ICD Conceptual Reference Model, each of which incorporates the common guiding principles, technical positions, and patterns used throughout the ICD community. They are also implementation independent, thereby providing system architecture flexibility by establishing the baseline for technology insertion. The models do not provide recommendations on prioritization of capabilities, functions, and activities.

- The **Orchestration Model** presents functions that are used to satisfy an organization's activities in response to CTI3. The orchestrator is critical as it manages the individual capabilities provided by the cybersecurity tools and products in a repeatable, auditable, and scalable manner that satisfies organizational policies that govern the whole process.
- The **Activities Model** presents the ICD capabilities with respect to the CTI3 orchestration and sharing activities within and between the Federation Manager and the Federation Members.
- **Capabilities Model** presents details on the capabilities and their relationships and shows how CTI3 flows within and between the Federation Manager and the Federation Members.

NOTE

*A **Federation Member** is any entity that consumes CTI3 from a Federation Manager. A **Federation Manager** is any entity that receives CTI3 from at least two or more Federation Members, and then consolidates and disseminates the collected CTI3 to subscribing Federation Members. Examples include the Department of Homeland Security (DHS) Automated Indicator Sharing (AIS) program and the domain-specific Information Sharing and Analysis Centers (ISACs)[1] and Information Sharing and Analysis Organizations (ISAOs).[2] Section 4.1 provides additional information.*

[1] List of ISAC Information Sharing Groups: https://www.nationalisacs.org/member-isacs
[2] List of ISAO Information Sharing Groups: https://www.isao.org/information-sharing-groups/

The information used to develop these models was gathered from multiple sources:

- Research and experimentation done internally by the Johns Hopkins University Applied Physics Laboratory's (JHU/APL's) IACD teams
- Internal collaboration between the subject matter experts and members of the various JHU/APL IACD teams
- Examination of publicly available documentation on matters about and related to IACD and ICD

1.1 Comparison between a Conceptual Reference Model and Reference Architecture

A **conceptual reference model** "provides definitions and a formal structure for describing the implicit and explicit concepts and relationships within a system" (Blandin, Frank , Laughton, & Hirata, 2010), which also includes a global description of the ecosystem considerations and concerns. It is technology and standard agnostic, which allows for maximum flexibility.

A **reference architecture**, on the other hand, "is, in essence, a predefined architectural pattern, or set of patterns, possibly partially or completely instantiated, designed, and proven for use in particular business and technical contexts, together with supporting artifacts to enable their use. Often, these artifacts are harvested from previous projects" (IBM, 2008). The focus is on deployment of locally optimal solutions for a specific enterprise and business model. It can state specific technical positions and standards that a deployment of the reference architecture must adhere to in order to be considered a successful instantiation.

A conceptual reference model can be used to create a reference architecture.

1.2 Understanding the Relationship between IACD and ICD

IACD can be summarized as the set of **orchestration services** needed to: *integrate* across multiple, disparate sources of information; *automate* the determination of risk and the decision to act; *synchronize* those machine actions to align with an organization's business rules and operational priorities; and *inform* communities of trust via **secure automated cyber security information exchange** so that other IACD-capable partners can rapidly act on that information.

ICD expands upon the IACD concept by explicitly integrating CTI3-sharing ecosystems with the cyber defense ecosystem, ensuring that the information shared is consumable, usable, and actionable. CTI3-sharing ecosystems include the DHS AIS program, CTI3 feeds from ISACs and ISAOs, and other data feeds.

2. Guiding Principles

Guiding principles convey, at a high level, the foundational concepts that influenced the development of the conceptual reference model. The principles are enduring and seldom modified so long as the environment in which the conceptual reference models operate does not radically change. Two guiding principles were taken into consideration when developing the ICD Conceptual Reference Model: increasing the speed and scale of cyber defense and adherence to IACD tenets.

2.1 Increasing the Speed and Scale of Cyber Defense

The IACD concept was driven by existing and increasingly more critical challenges in cyber defense:

- Current operations, architectures, and solutions cannot scale to complexity, interdependencies, and pervasiveness of threats
- Adversaries already employ re-use, modularization, orchestration and automation
- Acquisition and procurement don't accommodate speed of technology evolution
- Workforce realities demand a different approach – skilled human capital is at a premium

Therefore the structures and relationships defined by the ICD Conceptual Model enable organizations to more efficiently and effectively:

- Use human capital/cyber operators through automation
- Address cyber events as they occur via automated OODA loops - detect intrusions earlier in kill chain
- Increase collective cyber awareness among organizations through enhanced CTI3 sharing
- Force attackers to develop new tools and techniques by degrading their ability to re-use their tools across participating organizations

2.2 Adherence to IACD Tenets

The ICD Conceptual Reference Model observes the five tenets of IACD, which are illustrated in **Figure 1**.

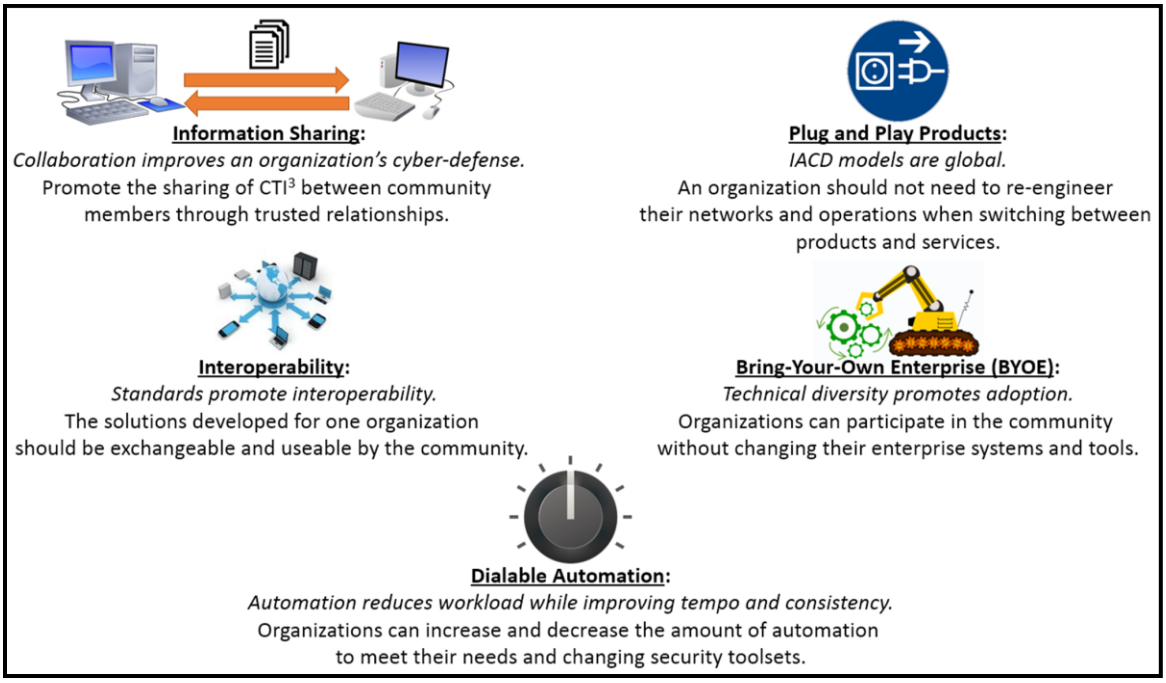

Figure 1 – The Five Tenets of IACD

3. Guiding Technical Positions

Guiding technical positions describe important technical guidance for the ICD domain. Because this is a conceptual reference model and not a reference architecture, such details as specific services, standards, agreements, communication protocols, etc., are not included.

3.1 Sharing and Trust

Collaboration with partners improves an organization's cyber defense.

Individual cyber defense efficiencies are limited to what an organization is able to correctly identify, assess, and respond to using their finite technical and personnel resources. CTI3 sharing between organizations within a community of trust can help mitigate those limitations by offering the following benefits:

- Broader, synthesized perspective for members;
- Defensive actions associated with threats or incidents
- Expanded services to increase trust and confidence

Establishing and maintaining trust within a community, as well as focusing on the sharing of actionable CTI3 is critical to increasing the collective cyber defense; otherwise, an organization will choose not to participate in the CTI3 sharing community or at worst, be overloaded with all the CTI3 they receive without knowing whether any of it is worth acting upon.

The following are a series of considerations that discuss the relationship between the reward/value of sharing CTI3 and associated risks of trusting other organizations when sharing/receiving CTI3.

True collaboration requires value and trust.

When something is shared, all control of that shared item is delegated by the provider to the consumer for as long as the consumer possesses the shared item. When retention of a shared item is trivial (e.g., data, information, knowledge), possession is pragmatically non-retractable.

With regards to CTI3 sharing, what the provider decides to share or expose depends on how they balance the risk that a consumer of their CTI3 will weaponize it to harm other organizations against the benefit of increasing the sharing community's collective cyber security defense posture. Likewise, the consumer's risk-to-reward assessment is based on whether they believe the CTI3 they receive is non-malicious as well as useful and accurate.

Trust is a two-way street.

Actors in this trust relationship take on the roles of the Trustor (provider) and the Trustee (consumer). The consumer accepts the risks of being in a relationship with the provider based on the consumer's perceived value of such a relationship. The provider believes the consumer will honor the applicable CTI3 handling agreements, and the consumer believes the items received from the provider can be employed with some level of confidence. **Figure 2** illustrates how this relationship, and the level of trust between these participants, is directional and totally independent.

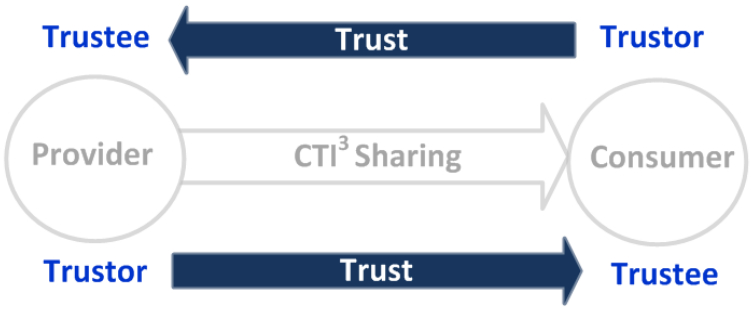

Figure 2 – Trust Roles in Sharing

"Just because I trust you does not mean that you trust me!"

Trust is based on expectations that include assurances from the Trustee (e.g., claims, consents, promises) and evidence acquired actively (monitoring), passively (reporting), directly (firsthand), and indirectly (hearsay).

Trust is not transitive. Just because Party A and Party B trust one another and Party B and Party C trust one another, does not mean that that Party C trusts Party A. It does, however, provide some evidence for developing a trust relationship.

When compared to in-person trust relationships, the complexity of managing digital trust dramatically rises by introducing relationships that are dynamic, transient, and numerous. Within this context, trust must be established adaptively among unacquainted entities (sometimes spontaneously) as well as continuously reevaluated between and during interactions. Solutions must constantly measure and quantify confidence in digital interactions that include:

- Identity claims – authentications
- Access privileges – authorizations
- Anticipated behaviors – trust

The fulfillment of these concerns can be delegated to proxies to facilitate or execute.

3.2 Identity and Access

The digital identity of an entity (whether a person or non-person) is everything known about that entity that is digitally captured in data elements called "attributes." Of particular interest are the core attributes, authentication attributes, entitlement attributes, and preference attributes (Hammer & Waterman, 2007).[3]

The core attributes of an entity are the characteristics that, when combined together, allow for unique identification. This includes locally unique identifiers and all attributes that support identity resolution (e.g., personally identifiable information). The process of formulating the likelihood of uniqueness can occur once those attributes are established (IDPV Identity Resolution Project, 2014).

The remaining attributes include the following:

- **Authentication**: Provides details that support identity claim resolution and identity alignment.

[3] http://colab.cim3.net/file/work/SICoP/DoDCoI/KWaterman05152007.pdf

- **Entitlement**: Provides characteristics that support the resolution of access control policies.
- **Preference**: Provides the entity with rendering choices and consistency across sessions (e.g., how data are presented on a website).

Identity is Global

An entity has one identity within an organization. In fact, this is the rationale for the application of identity resolution. It is also important to note that any entity can have affiliations with numerous disparate organizations, thereby creating a distribution of entitlements and a wealth of user preferences. However, that entity's identity should remain the same among these organizations so long as said entity wants to maintain that consistency.

Access is Local

Entity access to applications and services is governed by the organization that is responsible for controlling said access. Thus, each access point, at a minimum, must enforce their organization's access control policies. Although these policies may differ among entities or services managed within an organization and those managed by partners, they are always controlled and enforced by the hosting organization.

3.3 Interoperability and Diversity

Sharing includes the process for passing items within the payload of a transport mechanism that is supported by all participants and introduces six sharing concerns about utility, possession, authenticity, confidentiality, integrity, and availability. The success of any transaction depends on how well the participants understand and conform to the context defined by the process, syntax, and semantics of the item, payload, transport, and the six sharing concerns. The participants are considered interoperable when the consumer and provider context both align, thereby enabling the consumer to receive and fully appreciate the shared item.

4. Guiding Patterns for ICD Conceptual Reference Model

4.1 Federation

A federation is a group of individuals or organizations motivated by the belief that digitally sharing and collaborating with partners on CTI3 will collectively benefit the community's ability to identify and respond to attacks. The ICD Conceptual Reference Model uses a federation pattern to describe this relationship using two types of entities.

Federation Member

A Federation Member is a consumer of CTI3 who may subscribe to one or more CTI3 feeds provided by multiple Federation Managers. Federation Members may share their own CTI3 with one or more Federation Managers. They may also share it directly with other Federation Members as a peer-to-peer relationship. Being in multiple peer-to-peer relationships does not automatically make a Federation Member a Federation Manager because additional commitments are needed to achieve that distinction.

The Federation Member can incorporate received CTI3 into their Security Operations Center (SOC) activities, and the utility of said CTI3 can be increased if said Federation Member has security orchestration and automated response (SOAR) capabilities that can coordinate the activities between their deployed tools and capabilities. Trends and potential adversarial campaigns can also be identified from the received CTI3.

Federation Manager

The Federation Manager provides sharing and trust services that enable brokered and peer-to-peer transactions. They enforce on the governance decisions about standards, practices, and policies that each Federation Member should follow when providing their CTI3 to the Federation Manager. Close adherence to these standards, practices, and policies minimizes the amount of work the Federation Manager must undertake on the CTI3 before it can be disseminated.

The Federation Manager can be established by any organization in the public (e.g., DHS) or private (ISACs and ISAOs) sector. The focus of the Federation Manager may also vary depending on their constituents. For example, Federation Managers from public sector organizations may have jurisdictional-based cyber security missions, whereas private sector organizations may be more concerned about threats specific to their market (e.g., financials, industrial systems).

Membership management is a key role for the Federation Manager, which includes account provisioning, de-provisioning, and support services. Establishing a means to develop trust between the Federation Manager and Federation Members is critical to robust sharing of CTI3 between parties for the following reasons:

- Federation Members who do not trust the Federation Manager to properly handle (e.g., anonymize) their CTI3 will not share it.
- A Federation Manager who does not trust the accuracy of the CTI3 shared by a Federation Member (e.g., malicious) will be reluctant to accept (and potentially reject) their submission.
- A Federation Manager may also deny membership if an interested organization is not part of the respective Federation Manger's focus area (e.g. a retail store participating in an energy sector ISAC or ISAO).

A Federation Manager that intends to store and enrich CTI3 would be well served by implementing a sharing service with potentially multiple subscription feeds depending on the needs and criteria expressed by their Federation Members (e.g., focus only a subset of indicators, devices).

The organizational structure has no impact on the sovereignty of each member's enterprise, business strategies, or operations, and each member retains total sovereignty over their investment in sharing and collaboration.

4.2 OODA Loop Decision Pattern

IACD seeks to adapt a traditional control and decision approach from the physical world and apply it in cyber space. The OODA loop can, if implemented at speed and scale, reduce cyber operations timelines from months to minutes to milliseconds.

The IACD concept transforms the OODA loop activities into sensing, sense-making, decision making, and acting, and it envisions the sharing of information across these activities through a common messaging system (**Figure 3**). This messaging system likewise shares information with other entities to achieve shared situational awareness.

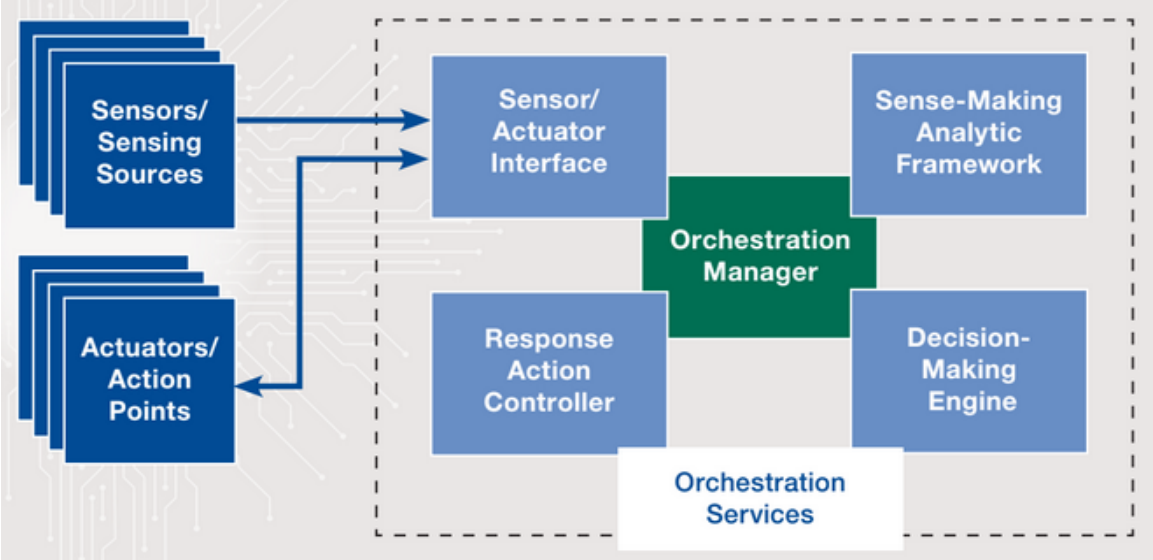

Figure 3 – IACD Orchestration Services

Additional information about the OODA loop decision pattern can be found in the *IACD Baseline Architecture* document located at **https://www.iacdautomate.org/**.

5. Approach for Developing Conceptual Reference Models

A **conceptual model** of the ICD community's operational cyber defense activities identifies and bounds capabilities in a set of **logical models** that, in turn, establish a unifying framework for identifying and comparing **physical models** of specific tools and products. The relationships of these operational activities highlight the importance of plug-and-play interoperability for the capabilities that interact across product boundaries. The product models identify supported capabilities, integration concerns and market-place gaps for person entity (PE) and non-person entity (NPE) actors participating in cyber defense and supporting collaborative relationships.

Capturing the ICD community's vision (**Figure 4**) includes a processing flow with entry and exit data. Any organization can apply this to catalyze the design, development, deployment, and assessment of their ICD system architecture solution. The process can be entered at any step and followed to accomplish the following:

- Develop and refine enterprise system architecture use cases and capabilities.
- Identify enterprise system architecture supporting technologies and standards.
- Assess enterprise system architecture tool and product coverage and alignment.

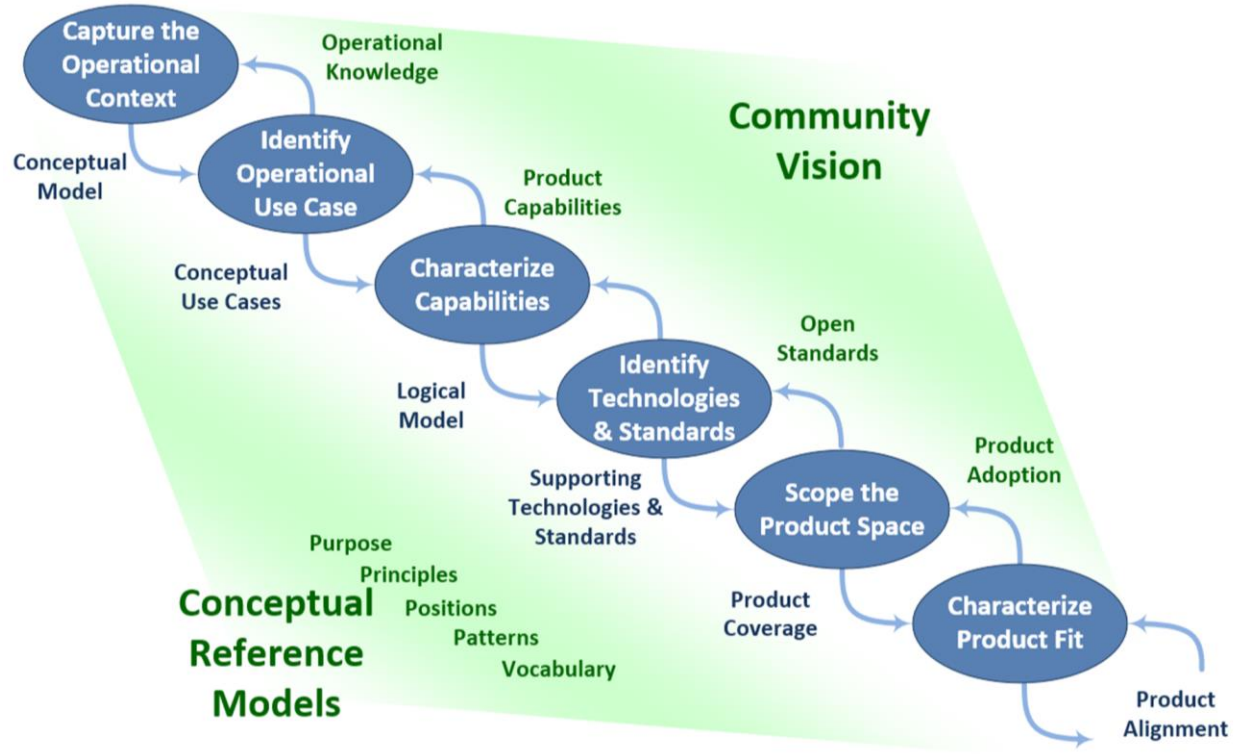

Figure 4 – ICD Conceptual Reference Model Approach

This approach answers the following questions:

- **Conceptually,** what are the problems and objectives?
- **Logically,** what are the capabilities and approaches?
- **Physically,** what are the tools, products, and gaps?

From there, development of conceptual reference models begins development of the following objectives:

- Characterize the set of common operational patterns and activities, cover the necessary sharing relationships, and address stakeholder needs and cyber concerns.
- Extend the conceptual activities to associated capabilities that support each operational activity and pattern.
- Identify tools and products that align with the capabilities.
- Characterize the capability coverage to identify gaps of existing and emerging tools and products.

5.1 Identifying Content for the Conceptual Models

The models that comprise the ICD Conceptual Reference Model were developed in a top-down approach that:

- Focuses on the IACD tenets (**Figure 1**)
- Provides agility by establishing the baseline for technology insertion
- Captures the concepts and relationships that are applicable to the ICD domain in an implementation-independent manner
- Applies collectively to enterprises and across enterprises and federations in the public and private sectors that are unified by the ICD domain and community

Having established the approach, the determination of what content should be contained within the conceptual reference models began. After performing research and reviews of external resources, this Conceptual Reference Model calls the common, organizationally identified concept an **Activity**. Activities represent high-level processes that organizations undertake in the processing of, and in response, to CTI3.

Consideration then moved to the tools and products that enable SOAR. Vendors create and market tools and products to the community that are designed to provide security **Functions** (e.g. provide alerts and identify malware), with each security function enabling part or all of a **Capability** (**Figure 5**).

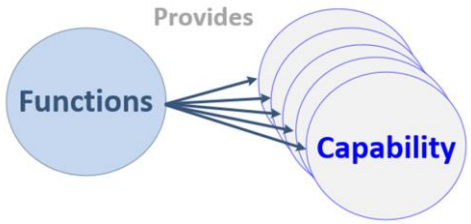

Figure 5 – Security Functions Comprise Capabilities

Capabilities can be combined to compose and satisfy the needs of an **Activity** (**Figure 6**). The usage and sequence of said capabilities is detailed in the process that is tailored to the needs of an organization.

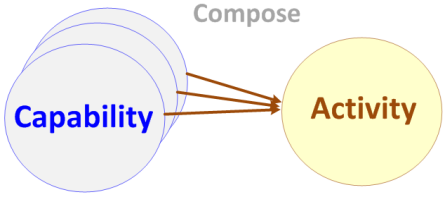

Figure 6 – Multiple Capabilities Can Compose an Activity

An example to illustrate the relationship is "an entity throwing a baseball," which is the activity. For an entity to throw a ball, it must conduct, at a minimum, the three capabilities illustrated in **Figure 7**. **Figure 8** presents another example showing possible capabilities provided by security tools and products an organization may have in their network that make up the organizationally defined **monitoring** activity.

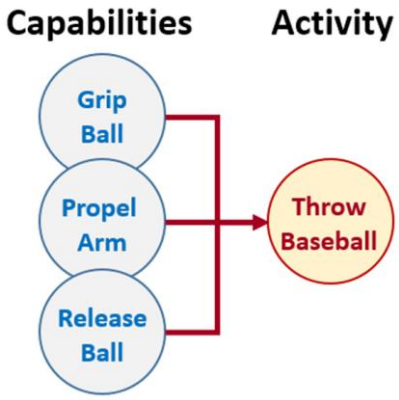

Figure 7 – Capability and Activity Example Relationship – Throwing a Baseball

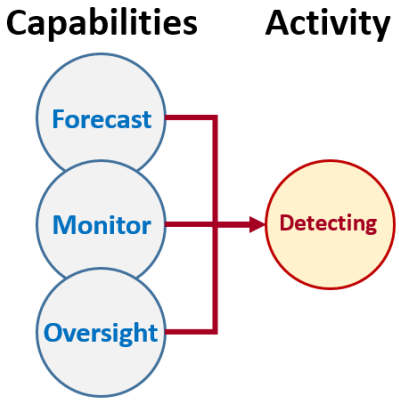

Figure 8 – Capabilities that Comprise the Monitoring Activity

Lastly, the actions and outcomes of a **capability** compose multiple **activities** and are implemented by multiple **functions**. Therefore, Capabilities are the bridge that links **activities** to **functions** (**Figure 9**).

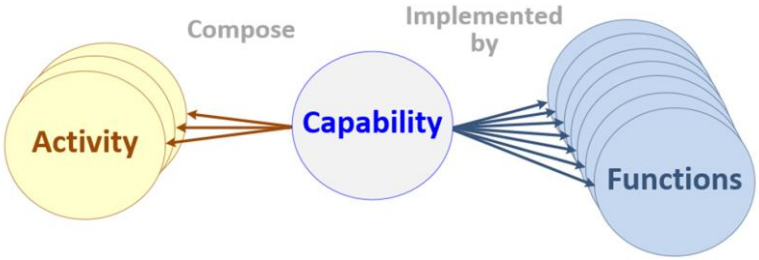

Figure 9 – Multiple Functions Enable a Capability Which Enables Multiple Activities

6. IACD Conceptual Reference Models

Each of the three models that currently comprise the ICD Conceptual Reference Model will now be discussed in further detail along with an individualized glossary for each. To more easily differentiate a capability from an activity, the naming convention of ending all activities with "-ing" was adopted.

6.1 The Orchestration Model

The ICD Conceptual Reference Orchestration Model, as depicted in **Figure 10**, presents functions that are used to satisfy an organization's activities in response to CTI3. The orchestrator is critical as it manages the individual capabilities that are provided by the cybersecurity tools and products in an auditable, consistent, repeatable, and scalable manner that satisfies organizational policies that govern the whole process.

The Orchestration Model is comprised of the following four components. Please note that the items contained within each are not all-inclusive due to the ever-changing nature of the ICD domain, and should be tailored by each organization to fit their individual needs.

- **Functions**: A selection of actions that can be carried out by various cybersecurity tools and products an organization may choose to deploy in their environment.
- **Capabilities**: Abilities provided by a cybersecurity tool or product, which can be orchestrated.
- **Orchestrate**: Represents the security orchestration and automated response (SOAR) product that is responsible for executing the capabilities in a repeatable, auditable, and scalable manner that satisfies organizational policies that govern the whole process. An organization does not need to orchestrate capabilities in their environment; rather, these capabilities can be connected and disconnected to the SOAR product depending on the organization's comfort level and/or current operational situation.
- **Activities**: High level processes than an organization undertakes to satisfy policy and governance requirements.

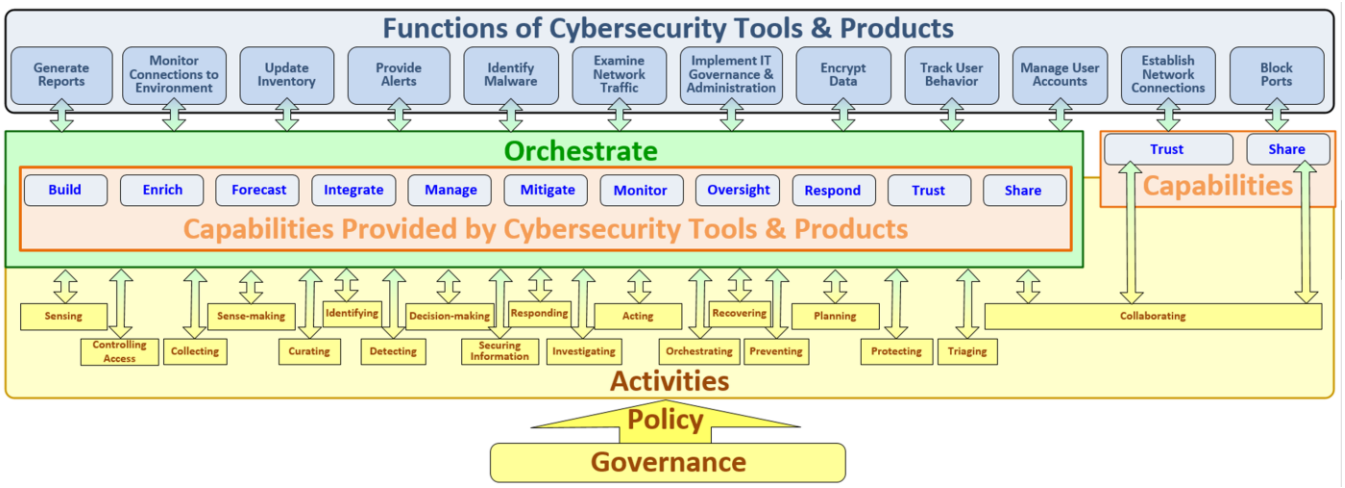

Figure 10 – ICD Conceptual Reference Model: Orchestration Model

The orchestration of capabilities links the concept of a function to an activity. This is because one or more capabilities provided by cybersecurity tools and services comprise a function and one or more functions are carried out to meet the organization's desired activities in response to received CTI3.

6.2 Activities Model

The Activities Model, as depicted in **Figure 11**, presents the capabilities and activities a Federation Member and Federation Manager can conduct to facilitate orchestration, as well as the sharing of CTI3 between parties. An organization does not need the ability to perform every capability and activity to implement some degree of SOAR. It is expected that a Federation Member will deploy more capabilities in their environment and conduct more activities compared to a Federation Manager because they are triaging and protecting themselves using the received CTI3. Conversely, the Federation Manager is predominantly focused on ingesting, curating, and dissemination the CTI3 they receive to their Federation Members. A Federation Manager can also be a Federation Member, in which case they may implement additional capabilities and activities (i.e. a Federation Member who is also a Federation Manager may utilize only a subset of capabilities and activities when acting as a Federation Manager).

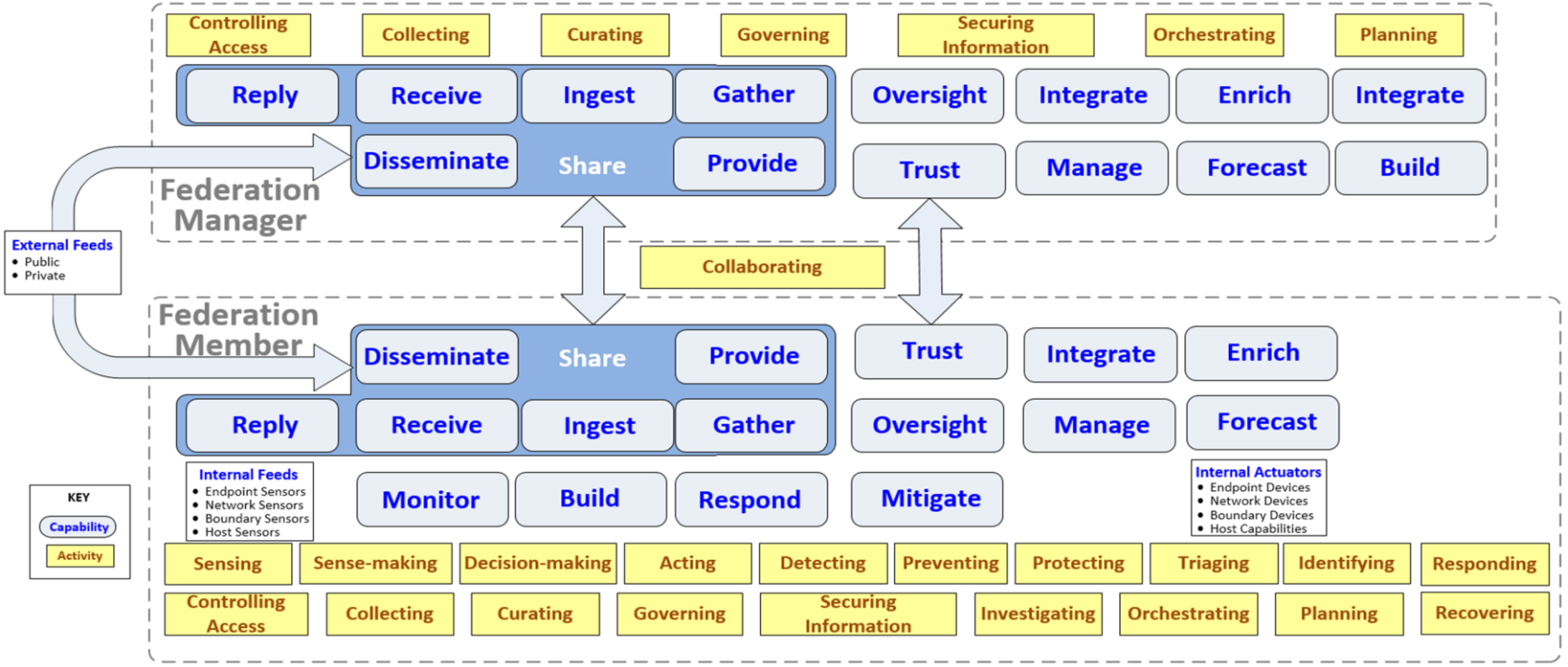

Figure 11– ICD Conceptual Reference Model: Activities Model

6.3 The Capabilities Model

The Capabilities Model, as depicted in **Figure 12**, presents the flow of CTI3 across the range of potential capabilities (which are provided by the various cybersecurity tools and products that an organization can deploy to their environment) both within and between the Federation Manager and Federation Member. It also contains ideas on how each capability can be decomposed further. The capabilities conveyed are not meant to be exhaustive, and said capabilities may contain additional component capabilities not shown here.

An organization can use this model to identify their high-priority capabilities, which can facilitate identification of potential tools to satisfy their needs. Once completed, said organization can then validate whether the prospective product(s) can provide the desired capability in discussion with the vendors. As the tools are deployed and tested, the organization can confirm whether their target capabilities are satisfied and the CTI3 is flowing through their system as expected. Likewise, gaps may be identified that require modification to and/or additional procurement of cybersecurity tools and products.

The Capabilities model can also help facilitate develop of a procurement strategy. Some organizations, for example, may wish to buy the fewest number of tools possible so as to maximize the capabilities within a single suite of products while minimizing cost, potential compatibility issues, and user training requirements. Other organizations may instead be interested in finding only the “best in breed” for their critical capabilities, which makes the number of potential vendors less of a concern.

One final note to facilitate the readability of this model is that a Federation Member can receive CTI3 from one or more of the following possible sources:

- **Various internal sensors** (bottom right of **Figure 12**) deployed across their enterprise
- **A peer-to-peer relationship** directly with other Federation Members to receive and/or share CTI3
- **Federation Managers** who offer CTI3 subscription(s) (be it real time or batch dissemination) with a common interest or potential relationship (e.g., same sector, geographic region)

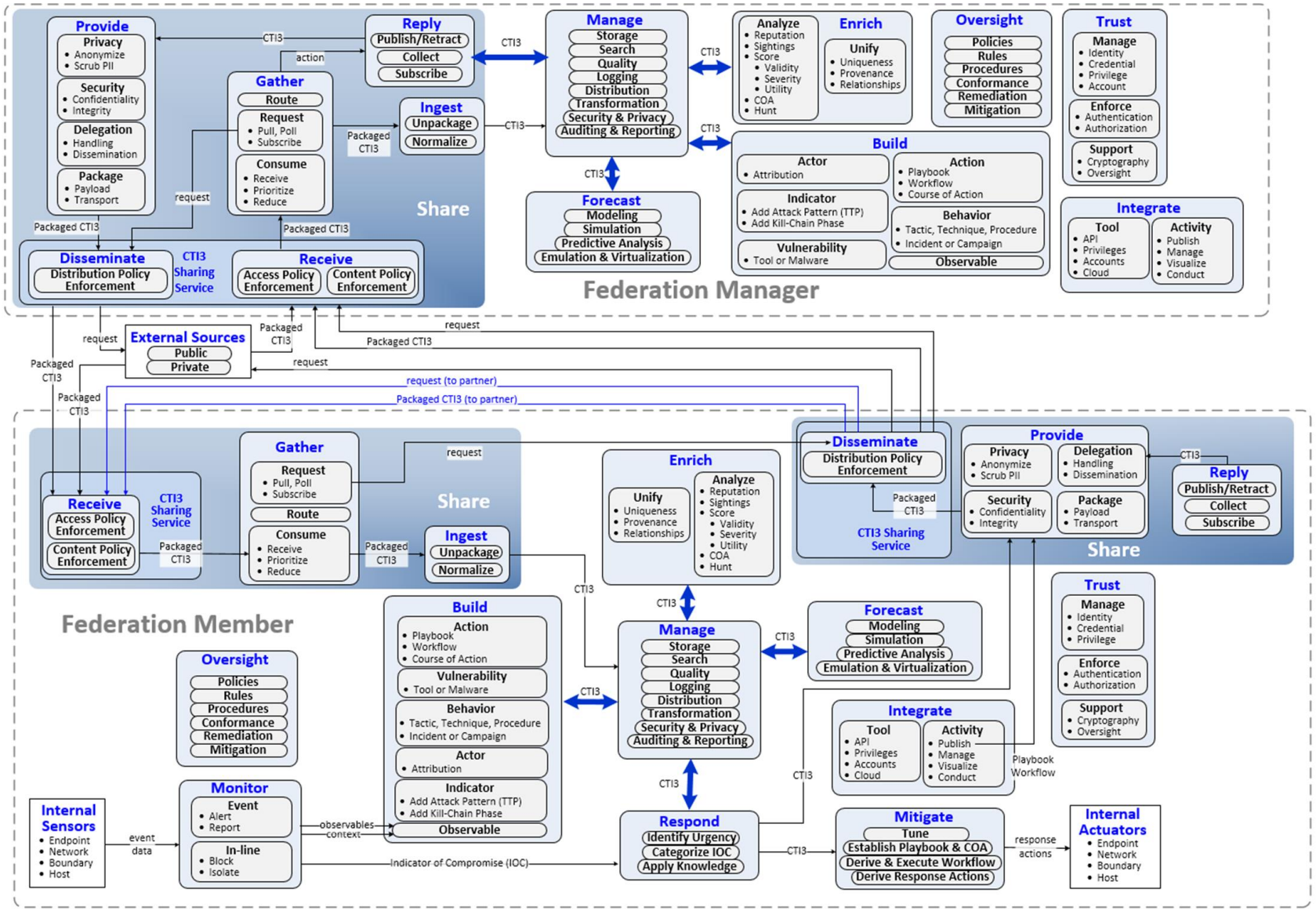

Figure 12 - ICD Conceptual Reference Model: Capabilities Model

6.4 Glossary of Terms

6.4.1. Activities Definitions

Term for Activities	Definition	Federation Manager	Federation Member
Acting	Acting is part of the sense, sense-making, decision-making, and act cycle. Actions taken may be any of the activities defined in this list.		X
Collaborating	Collaborating encompasses all aspects of the process needed for two entities to work together toward a common goal. Entities include people, organizations, and non-person entities. To enable collaboration, a method of securing communications between parties is needed along with establishing the parameters of the communication medium in use.	X	X
Collecting	Collecting information involves gathering data from one or more sources. If multiple sources are used, the data may need real-time process such as formatting, de-duplication, or other data fusion services to be made useful.	X	X
Controlling Access	A subset of Information Security, Controlling Access deals with how users and devices request and receive permission to access a resource. Access control covers all aspects of this process including the issuing of credentials based on identity and attributes, verifying credentials during authentication, approving or denying access during authentication, and controlling or revoking certificates as needed.	X	X
Curating	Curating is the process of storing and making available data for use and discovery by other activities and users. This involves secure storage for sensitive data and enforcing any distribution limitations on said data. Additional functionality to make the data easier to access and understand, such as indexing to enable searching, application of advanced analytics, prioritization, rating, and analysis support, may also be a part of this activity.	X	X
Decision-making	Decision-making is part of the sense, sense-making, decision-making, and act cycle. Decision-making is the process by which an action is chosen to execute based on the information generated by sense-making.		X
Detecting	Detecting is the act of discovering information regarding a cyber-event either in real time or as the result of after-the-fact analysis of evidence. Detecting includes the discovery of information as well as the process of making the appropriate entity (human, hardware, or software) aware of the initial detection and providing any expository information to support further investigations.		X
Governing	Governing is the activity of managing other activities. This includes drafting the policy that determines when other activities are carried out and verifying the proper execution of other activities.	X	X

Term for Activities	Definition	Federation Manager	Federation Member
Identifying	The Identifying activity encompasses the actions taken to inventory existing resources for an organization, including identifying resources such as hardware assets, network devices, user accounts, and services and assigning priority to determine acceptable risk for said resources.		X
Investigating	Investigating consumes data and outputs information that can support the Decision-making activity. Investigation that discovers a cyber-event may trigger the detecting action.		X
Orchestrating	The Orchestrating activity covers all actions taken to coordinate between different security products as well as the automation of security processes.	X	X
Planning	A preparatory action, the Planning activity involves anticipating what activities and events will occur and prepare for them before they happen. This may include the creation or deployment of new security tools.	X	X
Preventing	The Preventing activity prevents attacks before they occur. This includes actions to block attacks from reaching the target or prevent attacks from spreading further.		X
Protecting	Protecting causes attacks to fail by configuring or updating a resource such that it is no longer vulnerable to an attack.		X
Recovering	After an event or incident, Recovering involves actions to restore system function, data, access, or other resource attributes to the state they were in prior to the event.		X
Responding	Responding to an event includes actions that mitigate the impact of the event.		X
Securing Information	A necessary part of other activities, Securing Information encompasses all efforts required to secure and manage access to data.	X	X
Sense-making	Sense-making is part of the sense, sense-making, decision-making, and act cycle. Sense-making interprets the data gathered via sensing to enable decision-making.		X
Sensing	Sensing is part of the sense, sense-making, decision-making, and act cycle. Sensing is the first step of the cycle, and it involves the gathering of data from sensors.		X
Triaging	Triaging is the process of assigning priorities to events, tasks, events, or information.		X

6.4.2. Capabilities Definitions

Term for Capabilities	Definition	Federation Manager	Federation Member
Build	Create sharable information. This includes, but is not limited to, indicators; defensive measures; tactics, techniques, and procedures; vulnerabilities; and other observables. It also includes generation of playbooks, workflows, and courses of action (COAs) for sharing.	X	X
Disseminate	Monitor and control data leaving the enclave. Prevent exfiltration of sensitive data through the enforcement of distribution policies.	X	X
Enrich	Process raw data to produce meaningful intelligence.	X	X
Forecast	Make predictions based on a combination of known information and educated guesses. This includes, but is not limited to, estimating probably likelihood of future events and assessing the impact of technologies, vulnerabilities, or attacks on the organization.	X	X
Gather	Request and receive information for local consolidation.	X	X
Ingest	Receive information and translate to a format usable by local systems.	X	X
Integrate	Coordinate between different security and automation products.	X	X
Manage	Store and make data available for use and discovery by other activities and users. Manage is a key enabler of the Curating activity.	X	X
Mitigate	Identify and implement an appropriate response to detected indicators of compromise (IOCs) or alerts based on stored IACD playbook, COA, and workflow knowledge.		X
Monitor	Receive data from sensors. Potentially alert on predefined thresholds.		X
Oversight	Establish and enforce the policies and rules that determine the acceptable behaviors of the integrated system.	X	X
Provide	Make data available for others to use via information sharing. This includes preparing data for sharing through packaging and formatting, as well as removing sensitive data from shared information prior to sharing. It also includes authentication and authorization of a remote party prior to responding to information-sharing requests.	X	X
Receive	Monitor and control data entering the enclave. Block disallowed content through enforcement of content policies.	X	X
Reply	Collect and publish data periodically and in response to specific requests.	X	X

Term for Capabilities	Definition	Federation Manager	Federation Member
Respond	Use shared CTI3 to act on detection of indicators of compromise to trigger the application of a corresponding IACD playbook or COA.		X
Trust	Support capability that enables secure interaction between components. Includes authentication and authorization of internal and external entities as well as secure storing of credentials and encryption keys.	X	X

7. Bibliography

Blandin, B., Frank , G., Laughton, S., & Hirata, K. (2010). *Interoperability Issues for Systems Managing Competency Information: A Preliminary Study.* Hershey: IGI Global.

Hammer & Waterman. (2007). *Defining User Attributes for Authority-based Access Control.* COI/OAT/DHS.

IBM. (2008). *IBM Rational Unified Process Reference and Certification Guide: Solution Designer.* London: Pearson plc.

IDPV Identity Resolution Project. (2014). *Establishment of Core Identity Attribute Sets and Supplemental Identity Attributes.*