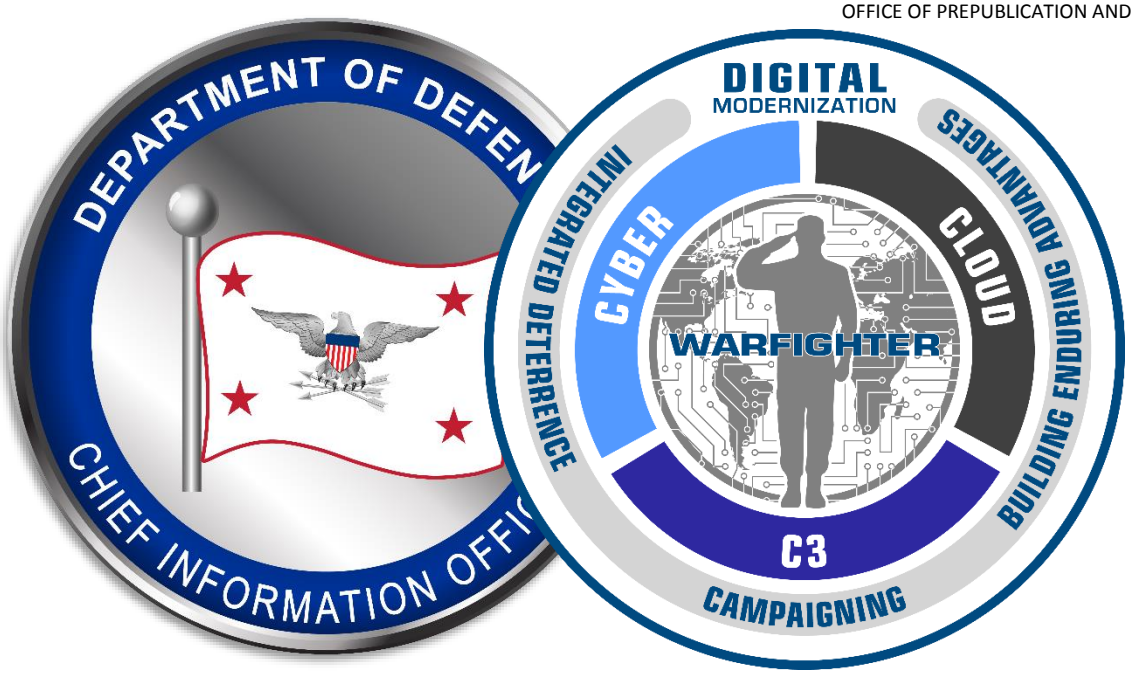
CLEARED
For Open Publication
Feb 07, 2023
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW



Department of Defense (DoD) Cybersecurity Reference Architecture

Version 5.0

January 30, 2023

Prepared By:

DoD CIO Cybersecurity Architecture Division

Table of Contents

Forward to Version 5.0 ..... **4**
Document History **5**
Executive Summary **6**
1. Overview / Summary (AV-1) **7**
1.1. Purpose 7
1.2. Scope 8
1.3. Principles 8
1.4. Assumptions 10
1.5. Constraints 10
1.6. Outcomes for the warfighter supported by Cybersecurity Architecture 10
1.7. Architectural Products 10
1.8. Transition Mapping 11
2. Operational Activities Overview **12**
2.1. A.1: Identify 13
2.1.1. Identify users 13
2.1.2. Identify devices 13
2.1.3. Identify services 13
2.2 A.2: Manage 13
2.2.1. Manage users 14
2.2.2. Manage devices 14
2.2.3. Manage configuration 14
2.3. A.3: Control 14
2.3.1. Macro segment network 14
2.3.2. Micro segment network 14
2.3.3. Macro segment environment 14
2.3.4. Micro segment environment 15
2.4. A.4: Protect 15
2.4.1. Tag Data 15
2.4.2. Encrypt Data 15
2.4.3. Enforce security policies 15
2.5. A.5: Detect 15
2.5.1. Detect anomalous behavior 16

2.5.2. Inspect traffic content 16
2.5.3 Inspect traffic measurements 16
2.6. A.6: Analyze 16
2.6.1. Log inspection results 16
2.6.2. Analyze event data 16
2.7. A.7: Automate 16
2.7.1. Automate policy-based responses 17
2.7.2. Automate event-based responses 17
2.8. A.8: Orchestrate 17
2.8.1. Integrate threat intelligence 17
2.8.2. Integrate automated workflows 17
3. Capabilities Overview 17
3.1. C.1: Identify 18
3.1.1. User enumeration 18
3.1.2. Device enumeration 18
3.2. C.2: Protect 19
3.2.1. Authentication and authorization 19
3.2.2. Data protection 19
3.2.3. Network protection 20
3.2.4. Application security 20
3.3. C.3: Detect 20
3.3.1. Continuous monitoring 20
3.4. C.4: Respond 20
3.4.1. Cyberspace defense 20
3.5. C.5: Recover 21
3.5.1. Cyberspace survivability 21
4.0. Cybersecurity Enhancements 21
4.1. Cloud Computing 21
4.2. Cross Domain 22
4.3. Control Systems 22
4.4. Space Systems 24
Appendix A: Acronyms and Initials 25
Appendix B: References 27

Forward to Version 5.0

In 2020, the DoD Chief Information Officer (CIO) subsumed the Joint Information Environment (JIE) into the broader DoD Digital Modernization Strategy (DMS). The DoD CIO approved the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM) Charter that formalized governance, roles, and responsibilities for implementing select strategy elements of the DMS. JIE architectures aligned to the DoD Information Enterprise Architecture, however; the transition to the DMS also subsumed this historical trend.

In 2021, E.O. 14028 directed the Federal Government to "make bold changes and significant investments" and use zero trust (ZT) to modernize cybersecurity. The Cybersecurity Reference Architecture (CSRA) version 5 will deliver on this imperative for the DoD by aligning to the DMS and integrating ZT principles to define data protection for cloud, traditional, and hybrid information systems.

Version 5 of the CSRA advances DoD's defense business systems, national security systems, and critical infrastructure / key resources through an evolution to integrate ZT principles.

This evolution is the DoD approach to meet the intent described in Section 3 of E.O. 14028, *Improving the Nation's Cybersecurity* and Section 1 of National Security Memorandum 8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* to modernize cybersecurity through adoption of ZT architecture (ZTA).

Document History

CSRA version 4.2, Enterprise Architecture Engineering Panel (EAEP) approval, January 2022.

Space Cyber Defense Reference Architecture (SCDRA) Addendum, approved by DOD Chief Cybersecurity Architect, November 2021.

CSRA version 4.11, EAEP adjudication of v4.1 staff coordination, December 2021.

CSRA version 4.1, included cloud cybersecurity architecture, an IPv6 Appendix and a ZT Appendix, March 2020.

CSRA version 4.0, dated June 2016, provided more detail on SSL traffic inspection, Supervisory Control and Data Acquisition (SCADA) / Industrial Control Systems (ICS), and device security.

CSRA version 3.1, dated August 2015, provided additional fidelity to architecture viewpoints previously stored only in the architecture tool used to develop the CSRA and updates content for concepts such as the Joint Regional Security Stacks (JRSS). Version 3.1 was not submitted to the Enterprise Architecture and Services Board (EASB) for approval due to the nature of the changes.

CSRA version 3.0, dated September 2014, includes multiple changes made to the previous baselines. The title was changed to Cybersecurity instead of Single Security Architecture (SSA) to simplify the name and align the architecture with the revised DoD Instruction 8500.01 Cybersecurity, DoD Instruction 8530.01 Cybersecurity Support to DoD Information Network Operations, and Joint Publication 3-12 Joint Cyberspace Operations. Version 3.0 specifically addresses Cyber Resilience, JRSS, Cyberspace Defense Support Services, and further refines the classified fabric.

SSA RA version 2.0, dated November 2013, includes views for classified security domains, Unified Capabilities, Computer Network Defense, and Enterprise Cross Domain Services. The package was submitted to the DoD Architecture Working Group (AWG) on August 30, 2013 and approved by the Architecture & Standards Review Group (ASRG) on November 19, 2013.

SSA RA version 1.1, dated May 2013, includes some additional content from early Integrated Design Team data and led to formal approval by the JIE EXCOM on May 2, 2013. To facilitate the approval process, the DoD ASRG was given authority to approve all future RAs.

SSA RA version 1.0 pre-dates the current architecture development process and was submitted to the DoD AWG and DoD ASRG/JIE EXCOM simultaneously. The initial capabilities document package was delivered to the DoD Deputy CIO for Cybersecurity on July 13, 2012 and followed with a November 29, 2013 delivery to the AWG and ASRG/EXCOM. It was subsequently informally approved by community consensus on December 15, 2012.

Executive Summary

The Cybersecurity Reference Architecture (CSRA) is a reference framework intended to be used by the DoD to guide the modernization of cybersecurity as required in Section 3 of E.O. 14028, *Improving the Nation's Cybersecurity*[1] and Section 1 of National Security Memorandum on *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* (NSM-8)[2]. The CSRA will advance Defense business systems, DoD national security systems (NSS), and DoD critical infrastructure / key resources (CIKR) – including DoD information technology (IT) and DoD operational technology (OT) – through an evolution to integrate ZT principles. This evolution is necessary to modernize cybersecurity through adoption of ZTA. The CSRA is a threat-informed product through integration of intelligence products and threat-based cybersecurity assessments (e.g., DoD Cybersecurity Analysis Review (DODCAR).

The purpose of the CSRA is to establish characteristics for cybersecurity architecture in the form of principles, fundamental components, capabilities, and design patterns to address threats that exist both inside and outside traditional network boundaries. Alignment of the CSRA to other RAs and solution architectures must include existing command and control (C2) orders and directives. The alignment of C2 and the CSRA will improve cyberspace survivability and enhance resiliency in operations and warfighter support to achieve integrated deterrence.

The CSRA Steering Group (CSRA SG) owns the architecture update effort and partners with stakeholders through a collaborative process involving the DoD EAEP, various NSS and CIKR working groups through the Committee on NSS (CNSS), the DoD Deputy CIO for Cybersecurity, and other DoD personnel from the Combatant Commands, Services, and Agencies (CC/S/A).

The CSRA is intended for the CC/S/A and mission partners who require access to DoD resources on premise or in a cloud environment. It serves as DoD enterprise-level guidance for establishing threshold cybersecurity to support two strategic outcomes: integrated deterrence enabled by automated response actions and enduring advantages enabled by procurement planning alignment.

[1] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

1. Overview / Summary (AV-1)

The DoD CIO is responsible for guiding the modernization of cybersecurity for NSS and CIKR employed by the DoD. As established in National Security Directive 42, the Director, National Security Agency (DIRNSA) is designated the National Manager for NSS. The partnership between the office of the DoD CIO and the NSA enables the evolution of the DoD's approach to modernizing cybersecurity in support of the warfighter.

The Cybersecurity Reference Architecture (CSRA) historically provided cybersecurity guidance for the family of architectures that aligned to the JIE Enterprise Architecture. It was originally developed to convey Enterprise-level technical direction to meet JIE and DoD Information Enterprise cybersecurity goals. The CSRA is now the instrument to modernize cybersecurity for the DoD as directed to the Federal Government in Section 3 of E.O. 14028 and NSM-8.

The key objectives of E.O. 14028 and NSM-8 addressed by the CSRA are adoption of ZTA, accelerate movement to secure cloud services, and centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks.

The JIE initiative reduced the quantity of stove-piped architectures; however, DoD Components continue to provide their own cybersecurity suites, implement customized and often conflicting security policies, provision remote user access with varying levels of security controls, and maintain separate Internet-connected interfaces. These result in complex and disparate architectures, duplicative inspection of network traffic, inability to accurately assess security and risk posture, and exposure to additional threat vectors and vulnerabilities. By evolving the network-centric architecture currently employed to one incorporating data-centric elements based on ZT principles, the CSRA will improve a commander's ability to understand the cybersecurity risk to support calculated mission risk decisions and the mission planner's ability to align modernization to the DoD procurement process.

The DoDAF v2.02 viewpoints and their models may all be used to formulate patterns of operational activities and their resources, service level functionality and resources, and capability attributes to support the Joint Capabilities Integration and Development System (JCIDS) process. Other design patterns will be depicted based on information needs using a meta-model approach. A meta-model describes possible structure of models often including principles and elements, which are also models, to build specific models within a domain of interest. At a minimum, the CSRA will include architecture data to support Net-Ready and Cyber Survivability Key Performance Parameters (KPP) in accordance with the JCIDS Manual.

1.1. Purpose

The purpose of the CSRA is to establish characteristics for cybersecurity architecture in the form of principles, fundamental components, capabilities, and design patterns to address threats that exist both inside and outside traditional network boundaries. The CSRA guides the modernization of cybersecurity implementation through the integration of ZT principles to support threat intelligence driven mitigation and procurement planning alignment. ZT contains the objective characteristics that guide the threshold characteristics contained in the CSRA to ensure that capabilities required by the warfighter meet cyber survivability criteria to support a cyber survivability endorsement (CSE). Cyber resilience considerations are included to support the engineering of cyber survivability required for mission assurance. As organizations adopt ZTA, requirements and acquisition documents will need to define both the cybersecurity and cyber resilience threshold performance requirements to ensure they are contractually binding, measurable and testable.

Alignment of cyber characteristics of a system to the CSRA will support approval of the initial capabilities document (ICD) and the capability development document (CDD). Leveraging the CSRA as a standard to describe cybersecurity attributes is intended to shorten the timeline of material solution acquisition in the JCIDS process.

In the ICD, the Cyber Survivability Risk Category (CSRC) statement can incorporate projected cyber threat and mitigations based on CSRA alignment. This will inform analysis processes to determine if the capability could meet intent of Cyber Survivability Attributes (CSA).

The CSRA can be used to provide guidance in the draft CDD to requirements writers for tailoring a subset of CSAs to support development consistent with the updated CSRC and intelligence cyber threat assessment at Milestone A. A robust cost analysis or analysis of specific performance parameters is not feasible at Milestone A due to insufficient data. A comparative analysis can provide meaningful data, but a standard set of characteristics is necessary. The CSRA can be used to identify which approaches show promise or could reach a desired Technology Readiness Level by the time the program reaches initial production, rather than attempting full technical assessments on all possible solutions from the start.

The CSRA will align to the CSAs to support measurement and testing of the adoption of ZTA. Aligning the CSRA with the CSAs is intended to simplify analysis of source selection criteria and prevent acquisition of capabilities that do not support ZT outcomes.

The three technical outcomes for the CSRA version 5 to drive adoption of ZTA intend to eliminate or reduce Persistence, Privilege Escalation, and Lateral Movement as described in MITRE ATT&CK®. Additional outcomes will be added based on the adoption of ZT.

- Authenticated and authorized access to all resources
- Access control enforcement based on multiple sources of authoritative data
- Automated security responses enable dynamic changes to security controls

1.2. Scope

The CSRA provides the architecture framework for modernizing cybersecurity for DoD and support completion of the Target level for ZTA. The guidance applies to defense business systems, DoD NSS, DoD CIKR, and other DoD IT and OT.

1.3. Principles

Cyber warfare is asymmetrical by nature and as a result, tailored or custom controls are necessary to achieve adequate cybersecurity; however, it is not cost-effective to eliminate all risk in a system. In order to mitigate risk effectively, each mitigation should be selected based on a threat-informed cost-benefit analysis. Balancing the overall effect of a mitigation with the direct cost enables an architect to make an informed determination based on the risk profile. An approach based on an acknowledgement that threats cannot be limited to authorization boundaries and that a cost-benefit analysis of mitigations informed by a threat-based cybersecurity assessment enables a security design that uses the most effective control for a specific threat. This approach aligns to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Rev A, Joint Staff JCIDS CSRC Cyber Survivability Attributes, DoD Instruction (DoDI) 8530.01, and ZT principles described in NIST SP 800-207 and other Federal Government initiatives.

The following cybersecurity architecture principles are recommended to achieve adequate cybersecurity by mitigating risk to an acceptable level to protect DoD data, assets, applications, and services (DAAS). The updated list of principles reflects the DoD’s intent to adopt ZTA pursuant to E.O. 14028 and NSM-8.

Protecting information (while processing, in transit, and in storage) is a core function of any security architecture whether it is performed from a network or data perspective.

- Principle 1: Reduce risk from the inside out – Risk reduction must focus on protection of the DAAS and a secure path to access them.
    - Principle 1.1: Least privilege (CNSSI 4009) – This principle is critical and should be considered at every decision point across all of the ZT pillars and is required to achieve the ZT target state.
    - Principle 1.2: Eliminate unnecessary security controls – Building on least privilege, removing excessive controls in the architecture will reduce the attack surface and increase mission assurance.
    - Principle 1.3: Isolation – Isolation (both logically and physically) enables control through access and policy restrictions to reduce risk to the networks and applications. This includes the use of network segments, application virtualization, and other technology and methods to enable more granular isolation.
- Principle 2: Increase mission assurance through resilience– Resilience is a key concept that helps quantify the ability of a system to maintain effectiveness and recover, especially during an active cyber event. It is critical to keep the number of components, elements, and controls to the lowest level possible for ease-of-use and resilience.
    - Principle 2.1: Deny by default – Evolving the deny all / permit by exception concept beyond network devices and integrating into all aspects of the architecture will mature and modernize the design. Resilience can be increased with greater control over authorized data flows and reducing rogue connections through poor configuration management.
    - Principle 2.2: Assume breach – An assumption that a malicious cyber actors (MCA) has access to the environment is a key concept for the evolution of the CSRA to the ZT target state. This principle builds on deny by default to increase mission assurance through implementation of cryptographic mechanisms for all occurrences of data processing, storage, and transmission.
    - Principle 2.3: Recover – An assumption of breach should be followed by the capability to recover full functionality within a specified mission-relevant timeframe. This principle enables Cyberspace Survivability through integrated and automated workflows and technical security measures to restore access to the DAAS.
- Principle 3: Enable modernization – In order to achieve and maintain cybersecurity superiority, decisive and deliberate steps must be taken.
    - Principle 3.1: Integrate identity, credential, and access management (ICAM) – To engage in responsible, secure information sharing within and across classified and unclassified security domains, ICAM policy and standards must be established. Integrating ICAM among organizations will enable interoperability and restrict access to authorized users.
    - Principle 3.2: Establish and enforce data tagging – The ability to efficiently organize information based on tags is critical to modernizing cybersecurity. Data tagging is necessary to achieve an advanced maturity of all three outcomes listed in Section 1.1.
    - Principle 3.3: Accelerate movement to secure cloud services – The ability to accelerate requires an innovative approach to providing secure access to cloud environments for continuous integration and continuous delivery (CI/CD) in the application/workload pillar. Secure cloud services through integration of ZT principles enable authorized user

access to cloud resources while limiting unauthorized user access to application interfaces.

- Principle 3.4: Standardize and streamline cybersecurity data analytics – To adapt to new threats and emerging technology, security orchestration should be automated and use a common language for development, analysis, and reporting. Full visibility across all layers is required for effective analytics.

1.4. Assumptions

The assumptions listed below reflects the DoD's intent to adopt ZTA pursuant to E.O. 14028 and NSM-8.

- Every user, device, and application are authenticated and authorized
- Policies are dynamic and access control decisions are based on multiple authoritative sources
- External and internal threats exist in the architecture at all times

1.5. Constraints

- Public law and Federal guidance
- NSS policy, instruction, and guidance
- DoD CIO policy, USCYBERCOM orders and directives

1.6. Outcomes for the warfighter supported by Cybersecurity Architecture

The CSRA is intended to support more effective outcomes for the warfighter through two primary ways described in the *2022 National Defense Strategy*.

Integrated deterrence – To improve cyberspace survivability and deter MCAs, the Department must invest in the modernization of key capabilities. Adoption of a ZTA that integrates visibility, analytics, data protection, and other advanced security techniques will reduce complexity and enable automation and orchestration of cyber response actions.

Building enduring advantages – The current procurement process was built to acquire specific systems rather than to solve operational problems. As the Department moves toward rapid experimentation and fielding emerging technology and capability, the intent is better alignment of requirements to resources and acquisition. Adoption of a ZTA designed with interoperability of legacy systems with modern systems will deliver advanced capabilities to the warfighter more efficiently and effectively.

1.7. Architectural Products

Table 1 lists the DoDAF views utilized to document the CSRA purpose and intent.

Product	Short Name	Description
Overview and Summary	AV-1	Defines scope, purpose, intended users, analytical findings, assumption, products, context, tools, and resources
Integrated Dictionary	AV-2	Definitions for capabilities, nodes, activities, systems, and services
Operational Concept Graphic	OV-1	Executive-level operational summary of what the

		architecture is intended to do and how it is intended to do it
Operational Activity Decomposition	OV-5a	Operational activity decomposition tree of the required activities in the architecture
Capabilities Decomposition	CV-2	Capabilities decomposition tree of the required capabilities in the architecture
Capability Phasing	CV-3	Capability phasing in terms of dependency to increase the maturity of outcomes
Capability Dependencies	CV-4	Describes the dependencies between planned capabilities and defines logical groupings of capabilities
Capability to Operational Activities Mapping	CV-6	Mapping between the capabilities required and the activities that enable those capabilities

Table 1: Architecture Products

1.8. Transition Mapping

The Key Components of the previous versions of the CSRA will be integrated into the ZT pillars with several elements aligned through a many-to-many relationship mapping.

Enterprise Perimeter Protection (EPP) – The elements of the EPP will be integrated activities (A.1-A.6).

Core Data Center (CDC) – The elements of the CDC will be integrated through activities (A.4-A.8), and through capabilities Protect (C.2) and Detect (C.3).

Base/Post/Camp/Station (B/P/C/S) – The elements of the B/P/C/S will be integrated through activities (A.1-A.6) and through all capabilities at the top level (C.1-C.5).

JIE Core – The elements of the JIE Core will be integrated through activities (A.2, A.3, and A.5) and through capability Protect (C.2).

Enterprise Cybersecurity Suite – The elements of the Enterprise Cybersecurity Suite will be integrated in all activities (A.1-A.8) and capabilities at the top level (C.1-C.5).

Joint Regional Security Stack (JRSS) – The security functions provided by JRSS will be integrated in all activities (A.1-A.8) and capabilities (C.1-C.5) at the top level. Note: JRSS is approved for removal from the current architecture with a planned end date of fiscal year 2027.

Joint Management Network (JMN) – The elements of the JMN will be integrated through activities (A.2, A.3, A.6, A.7, and A.8) and through capabilities Protect (C.2).

Enterprise Operations Centers (EOC) – The elements of the EOC will be integrated though activities (A.5-A.8).

Controlled Network Interfaces – The controlled network interfaces will continue to exist, but will be described in terms of policy decision points (PDP) and policy enforcement points (PEP).

2. Operational Activities Overview

The CSRA leverages the NSS ZT pillars, the MITRE ATT&CK® Framework[3], and the MITRE D3FEND™[4] to describe the operational activities that should be present in the architecture. The NSS ZT pillars consist of User, Device, Networks/Environments, Applications/Workloads, Data, Orchestration/Automation and Analytics/Visibility. The Orchestration/Automation and Analytics/Visibility pillars are not inherently cybersecurity capabilities and can be provided by other parts of the enterprise architecture. These two pillars are integrated into the CSRA as activities.

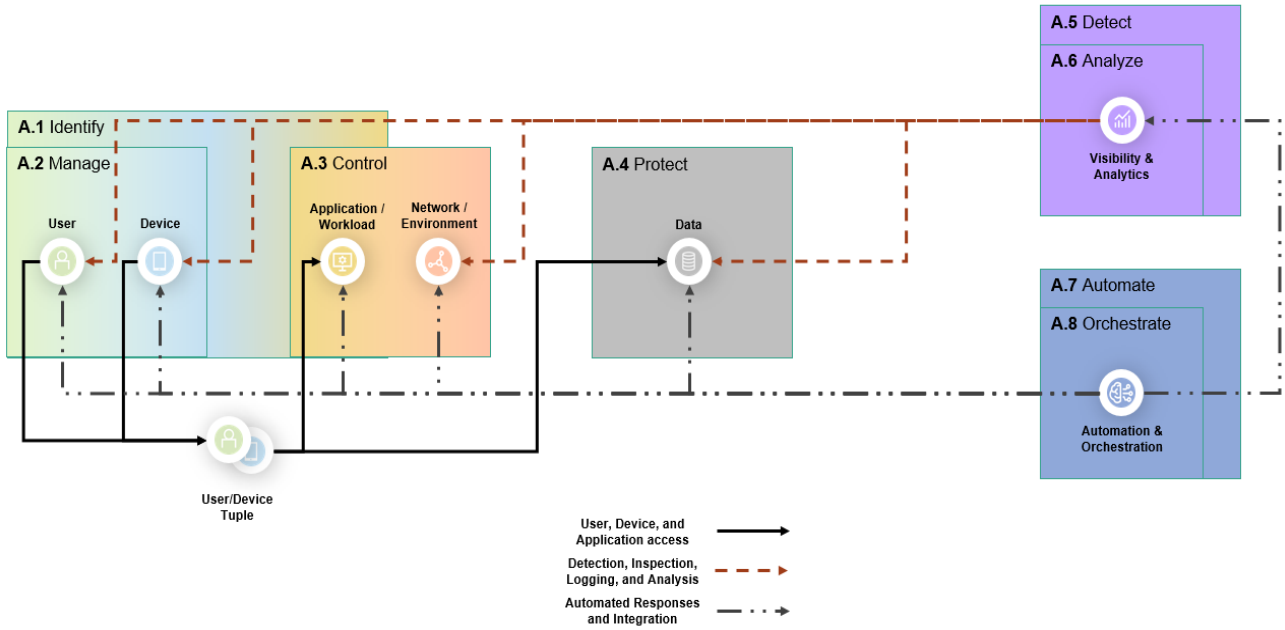


Figure 1: OV-1 Operational Concept

[3] https://attack.mitre.org/
[4] https://d3fend.mitre.org/

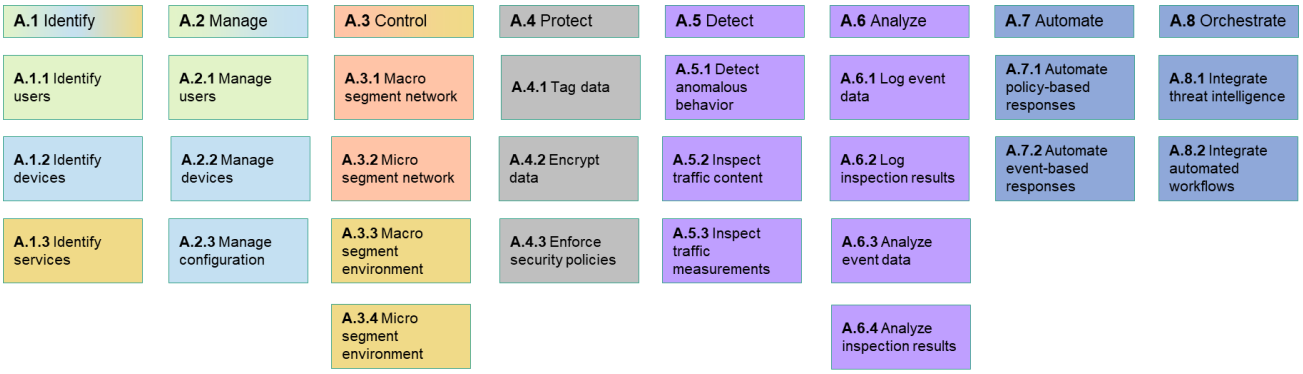


Figure 2: OV-5a Operational Activities Decomposition

2.1. A.1: Identify

The first step in creating a resilient architecture and managing cybersecurity risk is detailed knowledge of the DAAS. This knowledge constitutes the baseline that is required to support other activities in the architecture. Principle 1 is applied by identifying the access points in the environment and establishing a baseline of awareness to manage the risk. Principle 3.1 is critical to identify activities through association of attributes and access rights with each managed user, device, and service. ICAM policy and standards are established in coordination with the CSRA and are contained in a separate reference architecture. Activities described in A.1 and subsequent sections are dependent upon consuming an ICAM architecture and integrating with a DoD identity.

2.1.1. Identify users

Accounts with authorized and privileged access must be enumerated, including accounts not used by humans. This activity should include support for continuous discovery and automated inventory updates.

2.1.2. Identify devices

Devices may be physical or virtual and must be inventoried even if the device is in a powered-down state or is offline. The CSRA supports the use of managed and unmanaged devices which is dependent upon the ability to identify all devices. This activity should include support for continuous discovery and automated inventory updates.

2.1.3. Identify services

Services are transactions and processes that perform functions and must be identified with the same level of importance as users and devices. Modernization of cybersecurity integrates cloud computing which can include internal and external services based on the implementation. Infrastructure without a cloud computing design can also include external services. Identification of services is critical for the prevention and mitigation of lateral movement and privilege escalation. This activity should include support for continuous discovery and automated inventory updates.

2.2 A.2: Manage

Cybersecurity management activities protect the DAAS from MCAs through technical and administrative controls including change control management and patch management. Activities in A.2 are supported by activities in A.1. After users are identified, they should be managed according to the ICAM strategy for the system, supported by Principle 3.1. Managed and unmanaged devices must be able to function together in the same environment to adopt ZTA, but it will require careful application of Principle 1.1 to properly protect the DAAS. In addition to managing the devices directly, the device and service configurations must be managed by applying Principle 1.2 and Principle 2.1.

2.2.1. Manage users

Cybersecurity roles and responsibilities must be aligned with DoD policy for both internal users and external partners. External can mean another Federal organization as in the case of a Cybersecurity Service Provider (CSSP) discussed in DoDI 8530.01or external can mean a commercial organization. Regardless of the affiliation, all users must be managed in accordance with the infrastructure security requirements. This activity should include change control management and automated updates.

2.2.2. Manage devices

Devices can be managed (DoD-owned) and unmanaged (bring-your-own device) and must be able to send and receive security state information. All devices used to access DAAS must be controlled and monitored in accordance with the infrastructure security requirements. This activity should include change control management and automated updates.

2.2.3. Manage configuration

Devices and services must be configured to accept valid credentials and connect authorized data flows. All services must be managed in accordance with the infrastructure security requirements. This activity should include change control management and automated updates.

2.3. A.3: Control

Network and environment segmentation are effective techniques to reduce Reconnaissance, Execution, Defense Evasion, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact as listed in MITRE ATT&CK®. Segmenting networks will also improve Network Isolation as described in MITRE D3FEND™. Network and environment segmentation at the macro and micro levels implements Principle 1.3 by reducing the attack surface for each network and environment. Macro segmentation is a method of creating segments based on groups of systems, functionality, organizational units, and other strategic reasons. Micro segmentation is a method of creating segments based on system, service, application, or other discrete transaction.

2.3.1. Macro segment network

Macro segmentation of networks can consist of physical and virtual network devices such as firewalls and port security. Enhancing network segmentation through macro segmentation will greatly improve Network Isolation, as listed in D3FEND™ and reduce Reconnaissance, Execution, Defense Evasion, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact, as described in ATT&CK®.

2.3.2. Micro segment network

Micro segmentation of networks is typically virtual but may include hardware deployment in the case of a cross domain service. Enhancing network segmentation through micro segmentation will greatly improve Network Isolation, as listed in D3FEND™ and reduce Reconnaissance, Execution, Defense Evasion, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact, as described in ATT&CK®.

2.3.3. Macro segment environment

A common method of macro segmentation of an environment in the DoD is the isolation of test and development environments from production environments. In an operational example, DoD365 implements macro segmentation through the use of tenant organizations. Enhancing network segmentation through macro-segmentation will greatly improve Network Isolation, as listed in D3FEND™ and reduce Reconnaissance, Execution, Defense Evasion, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact, as described in ATT&CK®.

2.3.4. Micro segment environment

In the previous example, micro-segmentation could consist of designing network segments for each application in each test and development environment to further restrict communication pathways. In the same operational example, DoD365 implements micro segment within each tenant organization. Enhancing network segmentation through micro-segmentation will greatly improve Network Isolation, as listed in D3FEND™ and reduce Reconnaissance, Execution, Defense Evasion, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact, as described in ATT&CK®.

2.4. A.4: Protect

Access to DAAS must be controlled when DoD information is processed, stored, displayed, or transmitted. This includes supporting research, development, test and evaluation (T&E), and DoD-controlled DAAS accessed by a contractor or other entity on behalf of the DoD. Principle 1.1 is applied by establishing least privilege through attributes and Principle 2.1 is applied by restricting access to authorized access through cryptographic techniques and policy enforcement based on multiple authoritative sources.

2.4.1. Tag Data

Establishing and enforcing data tagging and labeling is required to achieve advanced maturity, supported by Principle 3.2. Initially, the activities will include manual tagging with automated tracking. Dynamic data tagging and labeling will use a combination of manual and automated analysis methods and adapt quickly to DoD policy reform. Continuous inventory updates with robust tagging and tracking will be enabled with machine learning models and artificial intelligence.

2.4.2. Encrypt Data

Encryption techniques for confidentiality protection must be employed when data is processed, stored, and transmitted. Adequate protection can include full-device, container-based, session-level, and selected data structures such as files, records, or fields. Encryption techniques are required for cloud or remote environments as described in NIST SP 800-171 and internal environments by DoD policy. This activity should include change control management and dynamic enforcement.

2.4.3. Enforce security policies

Access to DAAS using least privilege considers identity, device risk, and other attributes. Policy enforcement actions are dynamic and support techniques such as just-in-time, just-enough, and continual risk-based determinations. Data protections required by policy are enforced by default. This activity must include change control management and dynamic enforcement.

2.5. A.5: Detect

Anomalous activity must be detected and inspected for future analysis of the risk to the DAAS. This includes benign and malicious activity observed by a user, device, or application across the network / environment both internally and externally. Traffic content and measurement inspection can no longer be limited based on OSI layer and current funding streams. Concepts like authorization boundary and network perimeter must evolve to achieve ZT Target state. Holding on to administrative and network-centric ideas without a focus on data and technology evolution enables an MCA tactics including Persistence, Privilege Escalation, and Lateral Movement as described in MITRE ATT&CK®. Principle 2.2 is applied by operating with an assumption that an MCA has access to the environment and continuous detection is required to achieve desired outcomes.

2.5.1. Detect anomalous behavior

Detection of anomalous behavior is directly dependent on the identification of baseline behavior. This activity derives functionality from Identify and Manage (A.1) in order to determine baseline characteristics of users, devices, and applications. In a DoD environment, some of the physical and behavioral detection is performed by counterintelligence and security and is not part of the CSRA; however, it is an integral part that is required to achieve the desired outcomes. External service providers, such as a CSSP, will also perform this activity and share cybersecurity threat intelligence with the owner of the infrastructure. This activity will improve over time through advancement with machine learning models and artificial intelligence.

2.5.2. Inspect traffic content

Traffic content inspection must occur at all layers of the OSI model as appropriate. Deep packet inspection should be available where applicable, including encrypted traffic inspection. This activity is not inherently a cybersecurity activity; it is employed by the CSRA to enable Protect and Defend (A.3).

2.5.3 Inspect traffic measurements

Traffic measurement inspection such as timing, packet size, metadata and other traffic measurements must occur at all possible layers of the OSI model. This applies to both unencrypted traffic and traffic that cannot be decrypted. This activity is not solely a cybersecurity activity; it is employed by the CSRA to enable Protect and Defend (A.3).

2.6. A.6: Analyze

When anomalous activity is detected, it must be analyzed to determine the risk to the DAAS and impact to cyber survivability. Traffic content and measurement inspection results must be logged to facilitate reduction in data storage requirements and accelerate automation and orchestration of responses. Principle 2.2 is applied by operating with an assumption that an MCA has access to the environment and continuous analysis is required to achieve desired outcomes.

2.6.1. Log inspection results

Logging is a separate activity due to the technical ability to inspect traffic without logging. For all traffic content and measurements that are inspected (A.4.2) must also be logged (A.4.3). This activity is not solely a cybersecurity activity; it is employed by the CSRA to enable Protect and Defend (A.3).

2.6.2. Analyze event data

Detected events are analyzed to evaluate risk to DAAS. As the architecture matures, continuous analysis and evaluation must be implemented in a dynamic and granular fashion to streamline cybersecurity data analytics, supported by Principle 3.4. Analysis is required to identify and react to detected events and project the impact of events on access to DAAS. This activity will likely always include a human element and will improve over time through advancement with machine learning models and artificial intelligence.

2.7. A.7: Automate

Event and incident responses and associated functions must be automated to achieve ZT Target state. Principle 3 is applied to achieve and maintain cybersecurity superiority through modernization. Effective implementation of PEPs is dependent on automated responses to coordinate the functions. This also supports CI/CD for authorization decisions.

2.7.1. Automate policy-based responses

This activity will improve over time through advancement with machine learning models and artificial intelligence.

2.7.2. Automate event-based responses

This activity will improve over time through advancement with machine learning models and artificial intelligence.

2.8. A.8: Orchestrate

Effective implementation of PEPs is dependent on orchestration to coordinate the functions. This also supports CI/CD for authorization decisions. Although implementing CI/CD is outside the scope of the CSRA, automation and orchestration is critical to overall modernization of cybersecurity through adoption of ZTA.

2.8.1. Integrate threat intelligence

This activity will improve over time through advancement with machine learning models and artificial intelligence.

2.8.2. Integrate automated workflows

Automated workflows initiated manually constitutes basic functionality; integrated, automated workflows for user, device, application, and network state workflows must be implemented to achieve ZT Target state. This activity will improve over time through advancement with machine learning models and artificial intelligence.

3. Capabilities Overview

The CSRA leverages the NIST Cybersecurity Framework (CSF)[5], the Joint Capability Area (JCA) taxonomy, the MITRE ATT&CK® Framework, and the MITRE D3FEND™ Framework to describe and provide supporting rationale for the capabilities that should be present in the architecture. The NIST CSF contributes Identify, Protect, Detect, Respond, and Recover; the JCA taxonomy augments Protect, Detect, and Recover through the JCA 6.3 Cybersecurity; the MITRE ATT&CK® and D3FEND™ Frameworks provides the foundation to describe the risk in terms of threats, vulnerabilities, and impacts.

[5] https://www.nist.gov/cyberframework/framework

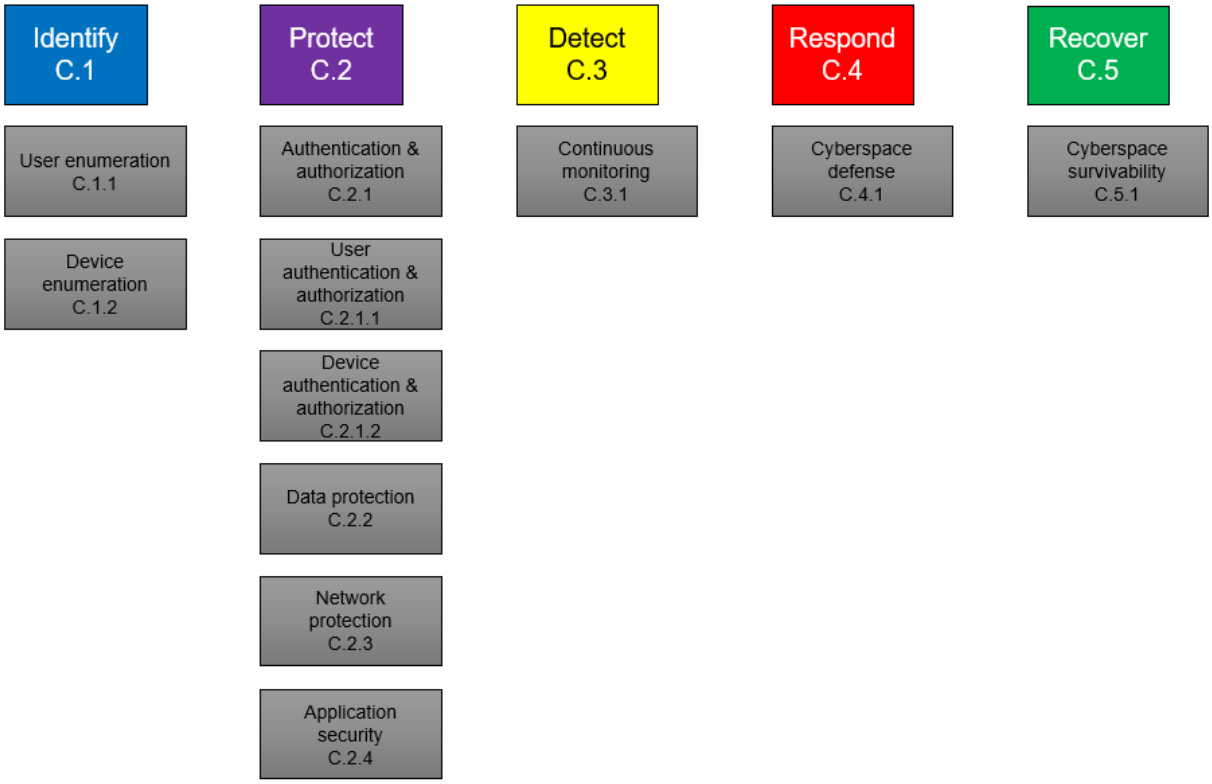


Figure 3: CV-2 Capabilities Decomposition

3.1. C.1: Identify

The NIST CSF Identify function is integrated into the CSRA as the ability to manage cybersecurity risk using technology and processes to identify the DAAS. Principle 1 is applied to the Identify capability to reduce risk, focusing on protection of the DAAS. Alignment of the Asset Management (ID.AM) category aligns the DoD business processes for user and device management consistent with their relative importance to strategic objectives and the DoD's risk strategy. The modernization of the CSRA requires identification of users and devices through enumeration. Enumeration is the process of identifying characteristics of a system such as usernames, device addresses, network addresses, and services.

3.1.1. User enumeration

The NIST CSF does not include any specific user identification support and the 2018 JCA taxonomy does not include this concept either. This is due to network-centric design methodology and requires a change in perspective to modernize cybersecurity for adoption of ZTA. Gather Victim Identity Information (ID: T1589) is a reconnaissance technique listed in the MITRE ATT&CK® Framework and is one of the first actions an MCA might take. Conducting this same technique internally is critical to modernizing cybersecurity. Users must be identified through enumeration on a continuous basis to effectively complete authentication and authorization actions.

3.1.2. Device enumeration

The NIST CSF includes support at the subcategory level for both physical devices and systems (ID.AM-1) and virtual platforms and applications (ID.AM-2). The 2018 JCA taxonomy does not include this concept. Several techniques are described in the MITRE ATT&CK® Framework including Active Scanning ID: T1595), Gather Victim Host Information (ID: T1592), and Gather Victim Network

Information (ID: T1590). Devices must be identified through enumeration on a continuous basis to effectively complete authentication and authorization actions.

3.2. C.2: Protect

The NIST CSF Protect function is integrated into the CSRA as the ability to limit or contain the impact of potential cybersecurity events using security controls and techniques. Principles 1 and 2 are applied to control access to data through the DAAS. At the top level, alignment of the Protect Information Protection Processes and Procedures (PR.IP) category ensure policies, processes, and procedures are maintained and used to support technical protection of the DAAS. The Protect capability maps and consolidates multiple levels of NIST CSF, JCA Taxonomy, and MITRE ATT&CK® to simplify the perspective for the procurement process.

3.2.1. Authentication and authorization

Authentication and authorization are not new terms and the difference with ZTA is a more comprehensive and granular approach that protects the data and means to access it compared to a focus on perimeter-level access to the system. DoD ICAM aligns to both the NIST CSF term of Identity Management, Authentication and Access Control (CSF PR.AC) and the JCA 6.3.4 term of Identity & Access Management. The central concept is to control physical and logical access to information systems authorized users, processes, and devices through decisions based on the risk of unauthorized access to authorized activities and transactions.

3.2.1.1. User authentication and authorization

Identities and credentials must be issued, managed, verified, revoked, and audited for authorized users and processes. (CSF PR.AC-1) This practice addresses the threat of MCAs common practice of misusing credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. (MITRE ATT&CK®, ID: T1078)

Users, and other assets must be authenticated (e.g., two-factor, multi-factor) commensurate with the risk of the transaction (e.g., user security risks and other organizational risks) (CSF PR.AC-7). MCAs may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a system. (MITRE ATT&CK®, ID: T1199)

3.2.1.2. Device authentication and authorization

Identities and credentials must be issued, managed, verified, revoked, and audited for authorized devices and processes. (CSF PR.AC-1) This practice is also necessary for devices to addresses the threat of MCAs common practice of misusing credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. (MITRE ATT&CK®, ID: T1078)

Devices must be authenticated (e.g., two-factor, multi-factor) commensurate with the risk of the transaction (e.g., user security risks and other organizational risks) (CSF PR.AC-7). MCAs may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a system. (MITRE ATT&CK®, ID: T1199)

3.2.2. Data protection

Data Protection is the ability to prevent theft, accidental loss, or corruption of data across applications, networks, and databases. (JCA 6.3.3) This aligns to the NIST CSF definition of data security, information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. (CSF PR.DS)

MCAs attempt to destroy data in specific systems to interrupt availability to systems, services, and network resources (MITRE ATT&CK®, ID: T1485) or manipulate external outcomes to affect a business process, organizational understanding, or decision making. (MITRE ATT&CK®, ID: T1565)

3.2.3. Network protection

Network Protection is the ability to anticipate and prevent successful cyberspace threat incidents on networks. (JCA 6.3.2)

Network integrity is protected through technical controls including network isolation and network segmentation (CSF PR.AC-5) to reduce or eliminate numerous techniques employed by MCAs. A large class of these techniques are contained in the Lateral Movement tactic which consists of techniques that MCAs use to enter and control remote systems on a network. (MITRE ATT&CK®, ID: TA0008)

Communications and control networks must also be protected (CSF PR.PT-4) to prevent MCA compromise of cloud computing environments, dark fiber infrastructure, and cryptographically isolated networks. (MITRE ATT&CK®, ID: T1584)

MCAs may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system. (MITRE ATT&CK®, ID: T1046)

3.2.4. Application security

Application Security is the ability to secure an application by preventing exceptions to the application's security policy or the underlying information system. (JCA 6.3.5) Principle 1.1 is incorporated by configuring systems to provide only essential capabilities. (CSF PR.PT-3)

3.3. C.3: Detect

The NIST CSF Detect function is integrated into the CSRA as the ability to discover MCAs using continuous monitoring. Anomalous activity must be detected to analyze and understand the potential impact of events. (CSF DE.AE)

3.3.1. Continuous monitoring

Security continuous monitoring of DAAS must be accomplished to identify cybersecurity events and verify the effectiveness of protective measures. (CSF DE.CM) This capability is an effective method to prevent and eradicate initial access. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. (MITRE ATT&CK®, ID: TA0001)

3.4. C.4: Respond

The NIST CSF Respond function is integrated into the CSRA as the ability to contain the impact of a cybersecurity event using automated policy and event-based responses.

3.4.1. Cyberspace defense

Cyberspace Defense is the ability to provide defense of networks, to include at the boundary. (JCA 6.4.1)

A running process might be terminated to mitigate its immediate effects if it is exhibiting anomalous, unauthorized, or malicious behavior; such as after detecting anomalous behavior via Administrative Network Activity Analysis, after a failed check from Stack Frame Canary Verification, or after System Call Analysis finds an attempt to execute an unauthorized system call. (MITRE D3FEND™, ID: D3-PT, Process Termination)

Management servers with enterprise policies for account management provide the ability to enable and disable account for given rules. The rules may include specific periods of time (e.g., weekend, plant

shutdown, leave periods), specific user types or groups, or individual users. (MITRE D3FEND™, ID: D3-AL, Account Locking)

3.5. C.5: Recover

The NIST CSF Recover function is integrated into the CSRA as the ability to restore any capabilities or services that were impaired due to a cybersecurity incident using integrated and automated workflows and policy enforcement mechanisms.

An advanced Recover function must integrate technical security solutions to ensure the cybersecurity and cyber resilience of systems and assets, consistent with related policies, procedures, and agreements. Protective technology (CSF PR.PT) integration includes implementation of mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements in normal and adverse situations. (CSF PR.PT-5)

3.5.1. Cyberspace survivability

Cyberspace Survivability – The ability to mitigate effects of MCAs and resulting system degradation by preserving critical functions performance at threshold levels during a cyberspace threat incident, and then after a cyberspace threat incident recover full functionality within a specified mission-relevant timeframe. Systems include, but are not limited to, enterprise and organizational networks, weapons systems, and critical infrastructures. (JCA 6.3.6)

Cybersecurity requirements are universal across DoD systems; however, cyber survivability requirements are not universal. Design requirements for OT systems (e.g., weapon systems, space systems) can often vary greatly from IT systems which can result in different cyber survivability characteristics. Modernization of cybersecurity must include design considerations for cyber resilience based on mission requirements to achieve cyber survivability endorsement and meet mission assurance objectives.

Principle 1 should be used as a foundation for enhancing cyberspace survivability. An architecture focused on data protection and granting access in a limited and granular manner can prevent tactics such as data destruction on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources (MITRE ATT&CK®, ID: T1485).

Principle 2.2 is critical to improving cyber survivability through adoption of ZTA. A design that assumes that an MCA has access to the system provides a more realistic baseline for achieving cybersecurity and cyber resilience outcomes. Traditional tactics used by MCAs such as stopping critical services or processes to inhibit or stop response to an incident or aid in the MCA's overall objectives (MITRE ATT&CK®, ID: T1489) are rendered less effective through a design that micro segments the environment to prevent communication channels previously available.

4.0. Cybersecurity Enhancements

The CSRA includes special topic areas that are of National interest or do not easily align to ZT principles, but are necessary to meet warfighter requirements. Some of these topics were added as addendums in previous versions of the CSRA and will continue as an addendum and others will be integrated in this section.

4.1. Cloud Computing

Pursuant to E.O. 14028, the DoD must “accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS)” to meet modernization goals for cybersecurity. The CSRA will support the accelerated adoption of cloud technology “in a coordinated, deliberate way”, adopting ZT principles and leveraging guidance through

the CNSS Policy 32, *Cloud Security for National Security Systems*, Federal Risk and Authorization Management Program (FedRAMP), and the DoD Cloud Computing Security Requirements Guide (CC SRG). The DoD guidance previously issued "to coordinate and collaborate on cybersecurity and incident response activities related to NSS commercial cloud technologies that ensures effective information sharing among agencies" will be reviewed to ensure ZT principles are integrated.

CNSS Policy 32 establishes the minimum security requirements for NSS migrating to or operating in a cloud environment and will be the primary policy instrument driving cloud security for the DoD.

The FedRAMP guidance will be considered regarding minimum security standards and controls related to unclassified cloud migration and operations for NSS and to "update existing agency plans to prioritize resources for the adoption and use of cloud technology".

The DoD CC SRG will be reviewed to determine the most effective and efficient approach to integrate ZT principles and to modernize the guidance based on mission requirements and industry best practices.

Partnerships with the DoD Components that are leading the way in cloud computing are critical to modernizing the adoption of secure cloud services integrated with ZT principles. Collaboration with these organizations and industry partners providing the services to the DoD is another critical piece to improving and modernizing the way the DoD consumes cloud computing services.

Emerging and critical technology and architecture such as the Cloud Native Access Point (CNAP) provides modernized cybersecurity capabilities based on the DoD ZTRA and serves as a bridge to transition from network-centric to data-centric architecture. By leveraging cloud native security services and tools, a CNAP is efficient in terms of maintenance, management, monitoring, and compliance. It also improves effectiveness in adopting a ZTA by integrating conditional access policies, micro-segmentation, and continuous monitoring.

4.2. Cross Domain

Cross domain technology is a key component of NSM-8 and includes inventory and reporting requirements. Results of the linked Binding Operational Directive (BOD-2022-001) will inform the CSRA about threats and vulnerabilities that need to be addressed at the enterprise level.

Some cross domain services may not closely align to ZT principles due to inherent design differences and integration may require development of architecture and data standards. Interoperability standards will be critical to ensure effective integration of cross domain services into the ZTA to meet information exchange security requirements.

From a ZT perspective, a cross domain services is fundamentally a capability for information exchange security. Information exchange security is defined in JCA 6.3.1 as the ability to secure dynamic information flow within and across domains. Information exchange security is realized through physical and virtual isolation based on data type and operational use. As a design consideration, user compute information exchanges should not traverse the same path as device compute information exchanges. Other information exchanges should be segmented as appropriate based on access control restrictions.

4.3. Control Systems

The DoD is one of the largest owners of real estate, buildings, and industrial control systems (ICS) in the Federal Government with more than 500 installations, 300,000 buildings, and an estimated 2.5 million unique ICSs. While Government-developed control system technology does exist in some DoD critical systems, the majority of this technology is developed by the commercial OT community.

ICS is a general term that encompasses several types of control systems, including SCADA systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the 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).

Supervisory control and data acquisition (SCADA) is a generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite.

Unlike designing cybersecurity for an IT system, an overarching principle for designing ICS security is the separation of the OT from the IT in terms of both data access and network connection. This separation of ICS business application traffic and operations and control application traffic is an important principle. While a standard IT system typically places emphasis on confidentiality or integrity, an OT system must prioritize availability above both confidentiality and integrity. Even within the ICS operations and control network, requirements for security may differ between applications, systems, or locations. It may be necessary to isolate traffic with one set of security requirements from the traffic with a different set of requirements. A baseline configuration of IT/ICS is created and maintained, incorporating security principles (e.g., concept of least functionality). (CSF PR.IP-1)

Further segmentation is achieved at the ICS via network layers, segments or Zones. The seven ICS security layers are:

- External Connections (ICS Layer 7)
- Enterprise DMZ (ICS Layer 6)
- Enterprise (ICS Layer 5)
- Operations DMZs (ICS Layer 4)
- Operations (ICS Layer 3)
- Monitoring /Automation/Control (ICS Layer 2)
- Process / Instrument (ICS Layer 1)

Each layer represents a particular security zone. ICS Layers 1, 2, and 3 can be further segmented by the following security zones:

- SCADA Security Zone for Transmission
- SCADA Security Zone for Distribution
- Synchrophasor Security Zone
- Load Control Security Zone
- Advanced Metering Infrastructure (AMI) Security Zone
- Generation Security Zone

Mission Critical Control Systems (MCCS) are information systems owned by the USG which monitor and/or control physical infrastructures critical to the direct fulfillment of military or intelligence missions. A critical type of MCSS is Mission Critical Facility Related Control Systems (MC-FRCS), a specific set of OT systems required for the continuity of mission essential functions.

Cybersecurity for MCCS, MC-FRCS, and other control systems discussed in the Addendum for control systems in CSRA v4.2 will be integrated into CSRA v5 and include ZT principles.

4.4. Space Systems

While there are numerous CC/S/A efforts, initiatives, and pilots ongoing; a single, overarching view of how cyber protection activities in the DoD Space Enterprise could, or should, relate or be prioritized does not exist. In this context, this DoD Space Cyber Defense Reference Architecture (SCDRA) will provide U.S. Space Force and the Space Community with the necessary level of direction and common structure, from the perspective of "Cyber for Defensive Space Control," to discuss implementations, stressing areas of commonality and relating numerous disparate cyber initiatives across the DoD Space Enterprise.

Appendix A: Acronyms and Initials

Acronym	Definition
ASRG	Architecture & Standards Review Group
AWG	Architecture Working Group
B/P/C/S	Base/Post/Camp/Station
CC/S/A	Combatant Commands, Services, and Agencies
CDC	Core Data Center
CIO	Chief Information Officer
CI/CD	Continuous Integration and Continuous Delivery
CIKR	Critical Infrastructure / Key Resources
C2C	Comply to Connect
CNAP	Cloud Native Access Point
CNSS	Committee on NSS
CSA	Cyber Survivability Attributes
CSF	Cybersecurity Framework
CSRA	Cybersecurity Reference Architecture
CSRA SG	Cybersecurity Reference Architecture Steering Group
DAAS	Data, Assets, Applications, and Services
DoD	Department of Defense
DMI	Digital Modernization Infrastructure
DMS	Digital Modernization Strategy
EAEP	Enterprise Architecture Engineering Panel
EOC	Enterprise Operations Centers
EPP	Enterprise Perimeter Protection
EXCOM	Executive Committee
ICAM	Identity, Credential, and Access Management
ICS	Industrial Control Systems
JCA	Joint Capability Area
JCIDS	Joint Capabilities Integration and Development System

Acronym	Definition
JIE	Joint Information Environment
JRSS	Joint Regional Security Stack
KPP	Key Performance Parameters
KSA	Key System Attributes
MCA	Malicious Cyber Actor
MCCS	Mission Critical Control Systems
MC-FRCS	Mission Critical Facility Related Control Systems
NIST	National Institute of Standards and Technology
NSS	National Security Systems
SCADA	Supervisory Control and Data Acquisition
SCDRA	Space Cyber Defense Reference Architecture
SSA	Single Security Architecture
USG	United States Government
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZTRA	Zero Trust Reference Architecture

Appendix B: References

(a) The White House, Executive Order 14028, "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021

(b) The White House, NSM-8, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022

(c) Department of Defense, "2022 National Defense Strategy," March 28, 2022

(d) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," July 25, 2017

(e) Committee on National Security Systems, CNSSP 32, "Cloud Security for National Security Systems," May 5, 2022

(f) Committee on National Security Systems, CNSSI 4009, "Committee on National Security Systems Glossary, March 7, 2021

(g) National Institute of Standards and Technology, Special Publication 800-190, "Compliance in container environments," June 30, 2021

(h) National Institute of Standards and Technology, Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," January 28, 2021

(i) National Institute of Standards and Technology, Special Publication 800-207, "Zero Trust Architecture," August 10, 2020

(j) Department of Homeland Security, "National Strategy for Information Sharing and Safeguarding," December 2012