ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

CYBERSECURITY ZERO TRUST MODEL ARCHITECTURE

Main Category:	Electrical Engineering
Sub Category:	-
Course #:	ELE-157
Course Content:	170 pgs
PDH/CE Hours:	6

OFFICIAL COURSE/EXAM

(SEE INSTRUCTIONS ON NEXT PAGE)

WWW.ENGINEERING-PDH.COM
TOLL FREE (US & CA): 1-833-ENGR-PDH (1-833-364-7734)
SUPPORT@ENGINEERING-PDH.COM

ELE-157 EXAM PREVIEW

- TAKE EXAM! -

Instructions:

- At your convenience and own pace, review the course material below. When ready, click "Take Exam!" above to complete the live graded exam. (Note it may take a few seconds for the link to pull up the exam.) You will be able to re-take the exam as many times as needed to pass.
- Upon a satisfactory completion of the course exam, which is a score of 70% or better, you will be provided with your course completion certificate. Be sure to download and print your certificates to keep for your records.

Exam Preview:

1. Zero Trust assumes continued and mandated use of communication encryption to the least extent possible protecting confidentiality and integrity and providing source authentication.
    a. True
    b. False
2. Using Figure 2: High-Level Operational Concept (OV-1), which of the following concepts does NOT belong in the data-centric enterprise segment of the diagram?
    a. Resource Authorization Decision Point
    b. Application Authorization Decision Point
    c. Data Authorization Decision Point
    d. Logging (SIEM)
3. According to the reference material, the concept of Zero Trust has five major tenets. Which of the following tenets matches the description: All resources are consistently accessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources?
    a. Presume Breach
    b. Assume a Hostile Environment
    c. Scrutinize Explicitly
    d. Apply Unified Analytics
4. User Authorization is defined as the ability to grant or deny device access to data, assets, applications, or services after a prerequisite check.
    a. True
    b. False

5. A Pillar is a key focus area for implementation of Zero Trust controls. Using Figure 4: Zero Trust Pillars, which of the following Pillars contains the following capabilities: Authentication, Authorization, and Compliance?
    a. Network/Environment
    b. Device
    c. Application & Workload
    d. User
6. State-funded hackers are well trained, well-resourced, and persistent. The use of new tactics, techniques, and procedures combined with more invasive malware can enable motivated malicious personas to move with previously unseen speed and accuracy.
    a. True
    b. False
7. Using the Vocabulary section of the reference material, which of the following terms matches the definition: refers to a class of solutions that help secure, control, manage and monitor privileged access to critical assets?
    a. Policy Decision Point (PDP)
    b. Policy Information Policy (PIP)
    c. Privileged Access Management (PAM)
    d. Privileged Access Workstation (PAW)
8. Zero Trust supports a mass migration approach to cybersecurity with an end state of an interoperable, fully functioned, optimized cybersecurity architecture that secures our critical assets and data from intentional or unintentional malicious activity.
    a. True
    b. False
9. _____ is the practice of creating logical network zones to isolate segments. These segments are secured by enabling granular access control, whereby users, applications, workloads, and devices are segmented based on logical attributes.
    a. Micro segmentation
    b. Macro segmentation
    c. Segmentation gateway
    d. (Network) Segmentation
10. Using Section 3.1 Standards Profile, which of the following standards corresponds to the description: a client/server protocol used to access and manage directory information. It reads and edits directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer?
    a. Guidelines for the Secure Deployment of IPv6
    b. Secret Key Transaction Authentication for DNS
    c. Lightweight Directory Access Protocol (LDAP)
    d. Common Information Model (CIM) Infrastructure

Department of Defense (DOD)
Zero Trust Reference Architecture

Version 1.0

February 2021

Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

February 2021

Document Approval

Document Approved By	Date Approved
Name: Joseph Brinker	FEB 2021
DISA Portfolio Manager, Security Enablers Portfolio (ID2)	

Revision History

VERSION	DATE	PRIMARY AUTHOR(S)	REVISION/CHANGE	PAGES AFFECTED
0.8	27 Aug 2020	Joint DISA/NSA Zero Trust Engineering Team	Added Vocabulary & Updated Template- submitted for internal DISA/NSA/USCC review	All
0.9	04 Nov 2020	Joint DISA/NSA Zero Trust Engineering Team	Adjudication of internal feedback and submission to EAEP for review	All
0.95	24 Dec 2020	Joint DISA/NSA Zero Trust Engineering Team	Adjudication of feedback from EAEP	All
0.96	30 Dec 2020	Joint DISA/NSA Zero Trust Engineering Team	Final review and classification header update	All
1.0	04 Feb 2021	Joint DISA/NSA Zero Trust Engineering Team	Prepared for DMI EXCOM Approval – Removed CS RA location description. Removal of CV-3, SvcV8, and SvcV-9 for classification purposes.	All

Table of Contents

1 STRATEGIC PURPOSE (AV-1, CV-1, CV-2, OV-1) 1
1.1 Introduction **1**
1.2 Purpose **1**
1.3 Scope **2**
1.3.1 Stakeholders 2
1.3.2 Architecture Development 2
1.3.3 Timeframe 3
1.4 Vision and Goals **3**
1.4.1 Vision and High-Level Goals (CV-1) 3
1.4.2 Strategy 5
1.4.3 Capability Taxonomy (CV-2) 6
1.5 High Level Operational Concept (OV-1) **7**
1.5.1 Decision Points, Components, and Capabilities 7
1.6 Intended Uses and Audience **13**
1.7 Assumptions **13**
1.8 Constraints **14**
1.9 Linkages to Other Architectures **14**
1.9.1 DOD Cyber Security Reference Architecture (CS RA) Integration 14
1.9.2 DOD ICAM Reference Design (RD) 15
1.9.3 NIST Special Publication 800-207 Zero Trust Architecture 16
1.10 Tool Environment **17**
1.11 Maturity Model **17**
2 PRINCIPLES 18
2.1 Overview **18**
2.1.1 Concept and Tenets of Zero Trust 18
2.1.2 Principles, Pillars & Capabilities 19

3 TECHNICAL POSITIONS (STDV-1, STDV-2) 21
3.1 Standards Profile (StdV-1) 21
3.2 Standards Forecast (StdV-2) 49
4 PATTERNS 55
4.1 Capability Dependencies (CV-4) 55
4.2 Capabilities to Operational Activities Mapping (CV-6) 57
4.3 Capabilities to Services Mapping (CV-7) 71
4.4 Operational Resource Flow Description (OV-2) 78
4.5 Operational Activity Model (OV-5b) 81
4.5.1 Authentication Request Simplified 82
4.5.2 Device Compliance 84
4.5.3 User Analytics 86
4.5.4 Data Rights Management (DRM) 88
4.5.5 Macro Segmentation 90
4.5.6 Micro Segmentation 92
4.5.7 Privileged Access 94
4.5.8 Application Delivery 96
5 VOCABULARY (AV-2) 98
5.1 Glossary of Terms 98
5.2 Activities Definitions 106
5.3 Services Definitions 150
5.4 Acronym List 155
APPENDIX A: CAPABILITY TAXONOMY & DESCRIPTIONS (CV-2) 159
APPENDIX B: REFERENCES 163

LIST OF TABLES

Table 1: Standards Profile (StdV-1) 22
Table 2: Standards Forecast (StdV-2) 49
Table 3: Capability to Operational Activities Model (CV-6) 57
Table 4: Capability to Services Mapping (CV-7) 71
Table 5: Integrated Dictionary (AV-2) 98
Table 6: Activities Definitions (AV-2) 106
Table 7: Services Definition (AV-2) 150
Table A-1: Capability Taxonomy and Descriptions (CV-2) 159

LIST OF FIGURES

Figure 1: Capabilities Taxonomy (CV-2) 7
Figure 2: High-Level Operational Concept (OV-1) 12
Figure 3: Zero Trust Maturity Model 17
Figure 4: Zero Trust Pillars 20
Figure 5: Capability Dependencies (CV-4) 56
Figure 6: Operational Resource Flow Description – Policy (OV-2) 79
Figure 7: Operational Resource Flow Description – Authentication (OV-2) 80
Figure 8: Operational Activity Model – Authentication Request (OV-5b) 83
Figure 9: Operational Activity Model – Device Compliance (OV-5b) 85
Figure 10: Operational Activity Model – Analytics (OV-5b) 87
Figure 11: Operational Activity Model – Data Rights Management (OV-5b) 89
Figure 12: Operational Activity Model – Macro Segmentation (OV-5b) 91
Figure 13: Operational Activity Model – Micro Segmentation (OV-5b) 93
Figure 14: Operational Activity Model – Privileged Access (OV-5b) 95
Figure 15: Operational Activity Model – Application Delivery (OV-5b) 97

1 STRATEGIC PURPOSE (AV-1, CV-1, CV-2, OV-1)

1.1 Introduction

"Zero Trust is the term for an evolving set of cybersecurity paradigms that move defenses from status, network-based perimeters to focus on users, assets, and resources. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the Internet) or based on asset ownership (enterprise or personally owned)." [1]Zero Trust requires designing a simpler and more secure architecture without impeding operations or compromising security. The classic perimeter/defense-in-depth cybersecurity strategy repeatedly shows to have limited value against well-resourced adversaries and is an ineffective approach to address insider threats.

The Department of Defense (DOD) next generation cybersecurity architecture will become data centric and based upon Zero Trust principles. Zero Trust supports the 2018 DOD Cyber Strategy, the 2019 DOD Digital Modernization Strategy and the DOD Chief Information Officer's (CIO) vision for creating "a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat."[2] Zero Trust should be used to re-prioritize and integrate existing DOD capabilities and resources, while maintaining availability and minimizing temporal delays in authentication mechanisms, to address the DOD CIO's vision.

1.2 Purpose

Zero Trust (ZT) is a cybersecurity strategy and framework that embeds security throughout the architecture to prevent malicious personas from accessing our most critical assets. It provides zones for visibility and information technology (IT) mechanisms positioned throughout the architecture to secure, manage and monitor every device, user, application, and network transaction occurring at the perimeter and/or within a network enclave. Zero Trust is an enterprise consideration and is written from the perspective of cybersecurity. The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction.

---

1 NIST SP 800-207 Zero Trust Architecture, August 2020

2 DOD Digital Modernization Strategy, June 2019.

1.3 Scope

The DOD Zero Trust Engineering Team is developing this Zero Trust Reference Architecture to align with the DOD definition: “Reference Architecture is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.”[3]

The content was built to align with the DOD Information Enterprise Architecture (IEA) for consistent mapping of terminology and ease of use as an implementation reference. The scope of the DOD Zero Trust Architecture (ZTA) effort is specifically to determine capabilities and integrations that can be used to successfully advance the Department of Defense Information Network (DODIN) into an interoperable Zero Trust end state. The architecture focused on data-centric design, while maintaining loose coupling across services to maximize interoperability. Other initiatives (e.g. ICAM, Public Key Infrastructure (PKI), etc.) to protect the DODIN are not the subject of this reference architecture but may be shown in some cases to provide additional context for ZTA alignment with DOD IEAs.

This Reference Architecture describes Enterprise standards and capabilities. Single products/suites can be adopted to address multiple capabilities. Integrated vendor suites of products rather than individual best of breed components will assist in reducing cost and risk to the government. This document will evolve as requirements, technology, and best practices evolve and mature. Zero Trust promotes individual journey to a collaborative goal of continuous Zero Trust enhancements, while also incorporating best practices, tools, and methodologies of industry.

1.3.1 Stakeholders

The DOD Zero Trust RA will be used by DOD Mission Owners (MOs) to guide and constrain the evolution of existing DOD IT and Enterprise Networks. MOs are individuals/organizations responsible for the overall mission environment, ensuring that the functional and cyber security requirements of the system are being met.

The Zero Trust RA provides an end-state vision and framework for Mission Owners across the DOD to utilize in order to strengthen cybersecurity capabilities and guide the evolution of existing cybersecurity capabilities focusing on a data centric strategy.

1.3.2 Architecture Development

This document is structured to provide a logical progression of information about the Zero Trust Reference Architecture in DOD. It consists of five sections and an appendix:

- Section 1: Provides an introduction that describes the purpose, background, approach, and structure for this document.

3 DOD Reference Architecture Description – June 2010

- Section 2: Discusses the core concepts and tenets of Zero Trust and provides detail regarding the Zero Trust Pillars.
- Section 3: The standards that are used within this Zero Trust Reference Architecture are provided in the Standards Profile Table (StdV-1) and the emerging, mandated, retired, and active Standards are described in the Standards Forecast Table (StdV-2).
- Section 4: Provides patterns for the DOD-wide Zero Trust Reference Architecture. This section describes and discusses the elements of a Zero Trust implementation and includes the following DoDAF views:
  - Capability Dependencies (CV-4) – Describes the dependencies between planned capabilities
  - Capability to Operational Activities Mapping (CV-6) – Describes the mapping between the capabilities and operational activities
  - Capability to Services Mapping (CV-7) – Describes the mapping between the capabilities and services
  - Operational Resource Flow Description (OV-2) – Defines capability requirements within an operational context
  - Operational Activity Model (OV-5b) – Describes the operations that are conducted within a Zero Trust Architecture
- Section 5: Defines the overall terms, activities used in the CV-6, services used in CV-7, and an acronym list that are used throughout this document.
- Appendices A: Provides the table associated with the Capability Taxonomy and Descriptions (CV-2).

1.3.3 Timeframe

Using the following general timeline and milestones in developing the Zero Trust RA v1.0

- 30 September 2020: Initial Zero Trust RA v0.9 Submitted for review by DISA, NSA, DoD CIO, and US Cyber Command
- 04 Nov 2020: Zero Trust RA v0.9 submitted to Enterprise Architecture Engineering Panel (EAEP) for feedback
- 04 Dec 2020: Zero Trust Joint Engineering Team receive feedback and begin adjudication
- 24 Dec 2020: Submission of Zero Trust RA v0.95 submitted to EAEP for CATMS Tasker
- 04 Jan 2021: CATMS Assessment Begins
- 11 Feb 2021: DMI EXCOM Approval of Zero Trust RA v1.0
- Calendar Year 2022: Zero Trust RA v1.5

1.4 Vision and Goals

1.4.1 Vision and High-Level Goals (CV-1)

View Definition: The CV-1 defines the strategic context for a group of capabilities described in the Architectural Description by outlining the vision for a capability area over a bounded period.

View Purpose/Intended Usage: The Zero Trust A CV-1 Version 1.0 describes the Zero Trust A mission, vision, and strategy and identifies key goals and outcomes. It is intended to be used with the CV-2 capability taxonomy to provide a capability basis for describing the Zero Trust future vision.

View Structure: The Zero Trust A CV-1 Version 1.0 is structured as a narrative.

Vulnerabilities exposed by data breaches inside and outside DOD demonstrate the need for a new and more robust cybersecurity model that facilitates well informed risk-based decisions. Zero Trust is a cybersecurity strategy and framework that embeds security principles throughout the Information Enterprise (IE) to prevent, detect, respond, and recover from malicious cyber activities. This security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes, and shifts to multi-attribute-based confidence levels that enable authentication and authorization policies based on the concept of least privileged access. Implementing Zero Trust requires designing a simpler and more efficient architecture without impeding operations to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services viewed as compromised.

Zero Trust focuses on protecting critical data and resources, not just the traditional network or perimeter security. Zero Trust implements continuous multi-factor authentication, micro-segmentation, encryption, endpoint security, analytics, and robust auditing to DAAS seven pillars to deliver cyber resiliency. As the Department evolves to become a more agile, more mobile, cloud-instantiated workforce, collaborating with multiple federal and non-governmental organizations (NGO) entities for a variety of missions, a hardened perimeter defense can no longer suffice as an effective means of enterprise security. In a world of increasingly sophisticated threats, a Zero Trust framework reduces the attack surface, reduces risk, and ensures that if a device, network, or user/credential is compromised, the damage is quickly contained and remediated.

State-funded hackers are well trained, well-resourced, and persistent. The use of new tactics, techniques, and procedures combined with more invasive malware can enable motivated malicious personas to move with previously unseen speed and accuracy. Any new security capability must be resilient to evolving threats and effectively reduce threat vectors, internal and external.

Zero Trust end-user capabilities improve visibility, control, and risk analysis of infrastructure, application and data usage. This provides a secure environment for mission execution. Enabling Zero Trust capabilities address the following high-level goals:

- **Modernize Information Enterprise to Address Gaps and Seams.** Over time, DOD networks have been decentralized and arguably underfunded, as each Service component and organization faces competing financial priorities. Usability and security challenges stem from years of building infrastructure along organizational, operational and doctrinal boundaries, with multiple security and support tiers, enclaves and networks. Capabilities developed in silos have inevitably resulted in disconnects and

gaps in the command structure and processes that preclude establishing a comprehensive, dynamic, and near-real time common operating picture (COP). Adversaries have exploited these logical, technological, and organizational gaps and seams.

- **Simplify Security Architecture**. A fragmented approach to information technology and cybersecurity has led to excessive technical complexity, which creates vulnerabilities in our cyber hygiene, inadequately addresses internal and lateral threats and results in high levels of latency. Complex security techniques render the user experience painfully unresponsive and unusable.
- **Produce Consistent Policy.** This is a critical lesson-learned from industry that automated cybersecurity policies must be consistently applied across environments (on/off premises) for maximum effectiveness. Technology leaders have relied on perimeter defense systems that fetter access and grant implicit trust based on network location. Waivers and exceptions to written policies, based on short term operational needs, have led to inconsistently managed, reconfigured, and/or disabled security systems, thereby making them porous and ineffective.
- **Optimize Data Management Operations** The success of DOD missions, ranging from payroll to missile defense, are increasingly dependent on structured and tagged data. Advanced analytics also depend on this. While data standards and policy exist, they are disparate and inconsistently implemented. This results in:
    - Interoperability challenges between applications, organizations, and with external partners,
    - Inherent system inefficiencies and vulnerabilities,
    - Poor/frustrating user experience, and
    - Hampered abilities to fully leverage the benefits of cloud computing, data analytics, machine learning, and artificial intelligence
- **Provide Dynamic Credentialing and Authorization.** Persona based identities, credentials, and attributes are not dynamic or context aware and come from disparate sources. Two factor authentications, in the form of the Common Access Card (CAC), has not kept pace with multi-factor authentication advances in industry. Non-person identities are not widely addressed, nor are identities for bots and the Internet of Things (IoT). The ICAM Reference Design will provide further specifics on credentialing implementations consumed by Zero Trust Architectures.

1.4.2 Strategy

Zero Trust will reconfigure, re-prioritize, and augment existing DOD capabilities, portfolios and resources to evolve towards a next generation security architecture. It instantiates tenets of the 2019 DOD Digital Modernization Strategy, the 2018 DOD Cyber
Strategy Lines of Effort, and the 2019 Cybersecurity Risk Reduction Strategy.
It supports the DOD vision of “a more secure, coordinated, seamless, transparent, and cost-

effective IT architecture… that ensures dependable mission execution in the face of a persistent cyber threat."[4]

Zero Trust supports an incremental migration approach to cybersecurity with an end state of an interoperable, fully functioned, optimized cybersecurity architecture that secures our critical assets and data from intentional or unintentional malicious activity. [5]The desired outcome is the roll out of an employable set of enterprise Zero Trust capabilities each consisting of standards, devices, and processes that are measurable, repeatable, supportable, and extensible, to any organization on the DODIN, and federated across the DODIN.

1.4.3 Capability Taxonomy (CV-2)

View Definition: A DODAF Capability Taxonomy (CV-2) is a hierarchy of capabilities which specifies all the capabilities that are referenced throughout the architectural description. A Capability is the ability to achieve a Desired Effect under specified (performance) standards and conditions through combination of ways and means (activities and resources) to perform a set of activities.

View Purpose/Intended Usage: The Zero Trust RA CV-2 Version 1.0 is used to identify capability requirements aligned to the DOD IEA CV-2 and provide reference capabilities for solutions architectures.

View Structure: The Zero Trust RA CV-2 Version 1.0 is structured as a hierarchy of capabilities, with the most general at the root and the most specific at the leaf-level. Each capability node (blue) includes the capability name and number. The numbering convention indicates the position of the capability within the hierarchy. The CV-2 also depicts high-level connections between the Zero Trust capabilities and DOD IEA capabilities (green). The hierarchy is followed by a table that provides additional detail for each capability node which can be found in Appendix D.

ID: The numerical identifier for each capability node

Zero Trust Architecture Capability Name: The full name of the capability. The name label on the hierarchy may be truncated for space considerations.

Zero Trust Architecture Capability Description: The authoritative description/definition of the capability as found in the Zero Trust RA CV-2.

As seen in CV-1, this framework calls for enterprises to leverage micro-segmentation based on user's risk profiles to determine whether to grant a user, machine or application seeking access to a part of the enterprise. To do this, Zero Trust draws on technologies such as multifactor authentication, ICAM, orchestration, analytics, scoring and file system permissions. Zero Trust

---

4 DOD IT Environment – Way Forward to Tomorrow's Strategic Landscape, August 2016 – Posted at http://DODcio.defense.gov/; DOD Digital Modernization Strategy is the DOD's 5 year IT plan, and is posted publicly here: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

5 DOD Zero Trust Strategy, Predecisional

also calls for governance policies such as giving users the least amount of access they need to accomplish a specific task.

The CV-2 capabilities are centered around the Zero Trust pillars which are User, Device, Network/Environment, Application & Workload, Data, Visibility & Analytics and Automation & Orchestration as defined below in Figure 1.

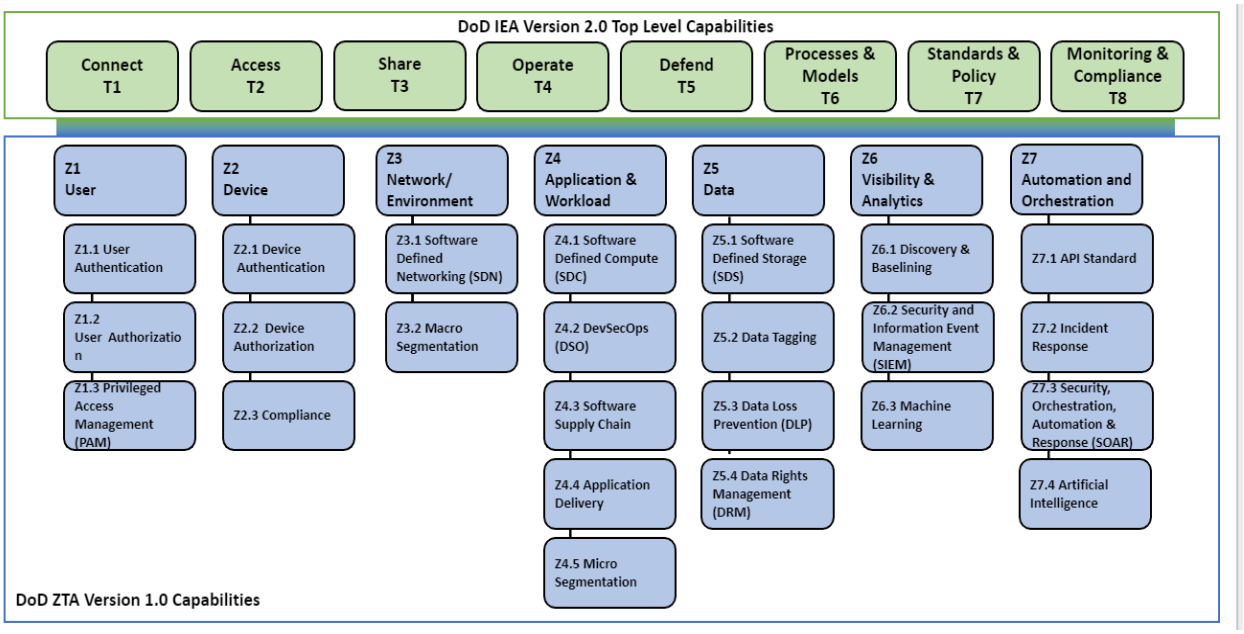

Figure 1: Capabilities Taxonomy (CV-2)

1.5 High Level Operational Concept (OV-1)

The Zero Trust RA High Level Concept provides an operational view on how security measures would be implemented within the architecture. Non-Person Entity (NPE) identity and user identity are tracked independently allowing for separate paths of validating confidence levels across enforcement points. Authentication and authorization activities will occur at numerous but focused points throughout the enterprise to include clients, proxies, applications and data. At each enforcement point, logs are sent to the SIEM and analytics are performed to develop a confidence level. Confidence levels of the device and user are independently developed and then aggregated where appropriate for policy enforcement. If the non-person entity or user has a confidence score above a measured threshold, then they are authorized to view the requested data. Data is protected along the way by Data Loss Prevention (DLP) which also feeds the SIEM to ensure the data is being used properly.

1.5.1 Decision Points, Components, and Capabilities

The following bullets provide additional detail on the decision points, components, and capabilities that are depicted within the OV-1. The capabilities identified below are representative of an end-state Zero Trust implementation. Controlling access to resources

based on the risk of the user and devices is the baseline requirement for Zero Trust and is possible without implementation of all identified capabilities.

- **Defense Enterprise Identity, Credential, and Access Management (ICAM):** which includes Identity Provider (IDP), Automatic Account Provisioning (AAP) and a Master User Record (MUR), identifies and manages the roles, access privileges, and the circumstances in which users are granted or denied privileges.
    - IDP: A system that performs direct authentication and optionally can provide authorization data on behalf of one or more information systems. This system also provides authentication for NPE's.
    - AAP: Provides identity governance services such as user entitlement management, business role auditing and enforcement and account provisions and deprovisioning based on identity data produced during DOD people-centric activities such as on and off-boarding, continuous vetting, talent management and readiness training.
    - MUR: Enables DOD-wide knowledge, audit, and data rollup reporting of who has access to what system or applications. MUR will also provide support in identifying insider and external threats.
- **Client and Identity Assurance:**
    - Authentication Decision Point: This evaluates the identity of the user, NPE, and or device as access is attempted to applications and data. Devices may also be evaluated as to whether they are managed or unmanaged. Additional use cases for non-user NPE and user assisted NPE are available in the ICAM Reference Design.
    - Authorization Decision Point: A system entity that makes authorization decisions for entities that request such access decisions. It examines requests to access resources and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the requester who issued the request under consideration. The client and device authorizations are the first stage in conditional access to resources, applications, and ultimately the data.
    - Capabilities:
        - Comply-to-Connect (C2C): Enforcing patches and hardened configuration(s) are applied to devices before they can connect to the internal network and updated continually with their status.
        - Privileged Access Management (PAM): Refers to a class of solutions that help secure, control, manage and monitor privileged access to critical assets. This includes administrative access of systems, applications and services.
- **Data-Centric Enterprise:**
    - Resource Authorization Decision Point: This is an intermediary decision point which will evaluate the combined NPE and user to authorize the request for

access. Like previous decision points, this will leverage the confidence level and defined policies to determine if access is warranted.

- Capabilities:
  - Macro Segmentation - Macro-segmentation, the concept of dividing a network into smaller, controlled segments with different attributes, can be achieved through the application of additional hardware or VLANs.
  - Application Delivery Control (Proxy) - An application delivery controller is a device that is typically placed in a data center between the firewall and one or more application servers (an area known as the DMZ). Application delivery controllers primarily perform application acceleration and handle enterprise-level load balancing between servers. Earlier generations of Application Delivery Controllers can handle a variety of tasks including, but not limited to, content-caching, SSL offload and acceleration services, data compression as well some intrusion prevention services.
- Application Authorization Decision Point: This is an intermediary decision point which will evaluate the combined NPE and user to authorize the request for access. Like previous decision points, this will leverage the confidence level and defined policies to determine if access is warranted.
- Capabilities:
  - Micro segmentation - This is the practice of creating logical network zones to isolate segments. These segments are secured by enabling granular access control, whereby users, applications, workloads, and devices are segmented based on logical attributes. This also provides an advantage over traditional perimeter security, as the smaller segments present a reduced attack surface (for malicious personas). In a Zero Trust Architecture, security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted. Segmentation Gateways and API access decision points can limit access on a per identity basis to explicitly allowed API invocations, with allowance granularity down to the "verb" level.
  - DevSecOps Application Development – DevSecOps is a set of software development practices that combines software development (Dev), security (Sec), and information technology operations (Ops) to secure the outcome and shorten the development lifecycle. Software features, patches, and fixes occur more frequently and in an automated fashion. Security is applied at all phases of the software lifecycle. Adoption of DevSecOps applies to application development and production environments equally
  - Data Authorization Decision Point: Data owners use Data Reference Architecture to apply tagging to data via orchestrator or DLP/DRP Servers.

- Capabilities:
  - Data Rights Management – Set of access control technologies that prevent the unauthorized access, modification and redistribution of data. Enforcement consists of encrypted data and its key is tied to policy defined by data owner. The encryption key will be tied to the security policy of the data to enforce least privilege authorization.
- Data: The final step in the process is access to the data and applications. Data tagging will be used to ensure proper classification levels for all data are used to help prevent spillage.
  - Capabilities:
    - Data Tagging – Tagging of data is critical to policy development as these attributes will be aligned to determine conditional access. With the scale and breadth of data in DOD, automation along with machine learning and artificial intelligence will need to be phased in as associated capabilities to assist with the tagging process.

- **Dynamic Access Control Plane:**
  - Policy Engine & Automation (SOAR): These terms are used to define technologies that handle threat management, incident response, policy enforcement and security policy automation. A Zero Trust Architecture will require dynamic policy enforcement and automation. SOAR will work in concert with analytics and policy engines to develop confidence levels and automate the delivery of policy to enforcement points.
  - Capabilities:
    - Automated Policy Deployment - Policy will be automatically deployed by Engine/Orchestrator based on analytics and implemented at enforcement points.
    - Endpoint Detection and Response (EDR): This is an analysis tool that provides real-time monitoring and detection of malicious events on endpoints. EDR allows you to visualize threats in a detailed timeline while instantaneous alerts keep you informed if an attack occurs.
    - User Activity Monitoring (UAM): UAM can monitor all types of user activity, including all system, data, application, and network actions that users take such as their web browsing activity, whether users are accessing unauthorized or sensitive files.
  - Analysis & Confidence Scoring: These technologies perform continuous assessments of entities, attributes and configurations to adapt and risk-optimize security policy for deployments. Confidence scores are leveraged in authorization activities.
  - Capabilities

        - Entity Behavior Analysis – analyzes data from the SIEM to determine the level of access. This is based on a set of attributes (e.g. device, identity, location, and time of day) and a formula used to generate the confidence level.
        - Data Loss Prevention - Detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use, in motion and at rest. Zero Trust Architecture will allow determination of data history and how it will be accomplished. This will provide log access and changes to data for potential use with forensic analysis, confidence scoring and policy automation.
    - Logging utilizing Security Information and Event Management: Activity data is aggregated and stored within the SIEM which provides both a security information management (SIM) and security event management (SEM) capability.
    - Capabilities:
        - Entity Activity Auditing – A Zero Trust Architecture will require logging of all activities to ensure proper analytics and confidence scoring. Each enforcement point along with user and entity behavior analysis will provide operational context for making access decisions.

Additional Zero Trust Concepts that were taken into consideration in developing the OV-1:

- **Define Mission Outcomes.** A Zero Trust design is derived from organization specific mission requirements and analysis that identify the critical protect surfaces - Data/Assets/Applications/Services (DAAS)
- **Architect from the inside out.** First, focus on protecting the DAAS. Second, secure a path to access them.
- **Define high level groups.** For users, devices, and applications/workloads.
- **Determine who/what needs access.** To create and apply local security policies consistently across all environments (Local Area Network (LAN), Wide Area Network (WAN), Endpoint, Perimeter, Mobile, etc.).
- **Inspect and log all traffic and events necessary to answer Commanders Critical Information Requirements (CCIRs) derived from mission analysis.** Full visibility across all layers is required for analytics.

View Definition: A DODAF High-Level Operational Context Graphic (OV-1) provides a pictorial and textual description of the operational concepts addressed in the architecture.

View Purpose/Intended Usage: The Zero Trust RA OV-1 Version 1.0 is used to convey core operational and functional concepts to high level decision makers. It provides a quick, high-level description of all key Zero Trust RA elements to include what the architecture is supposed to do and how it is supposed to do it.

View Structure: The Zero Trust RA OV-1 Version 1.0 is structured as a graphic with an accompanying narrative to describe the key concepts.

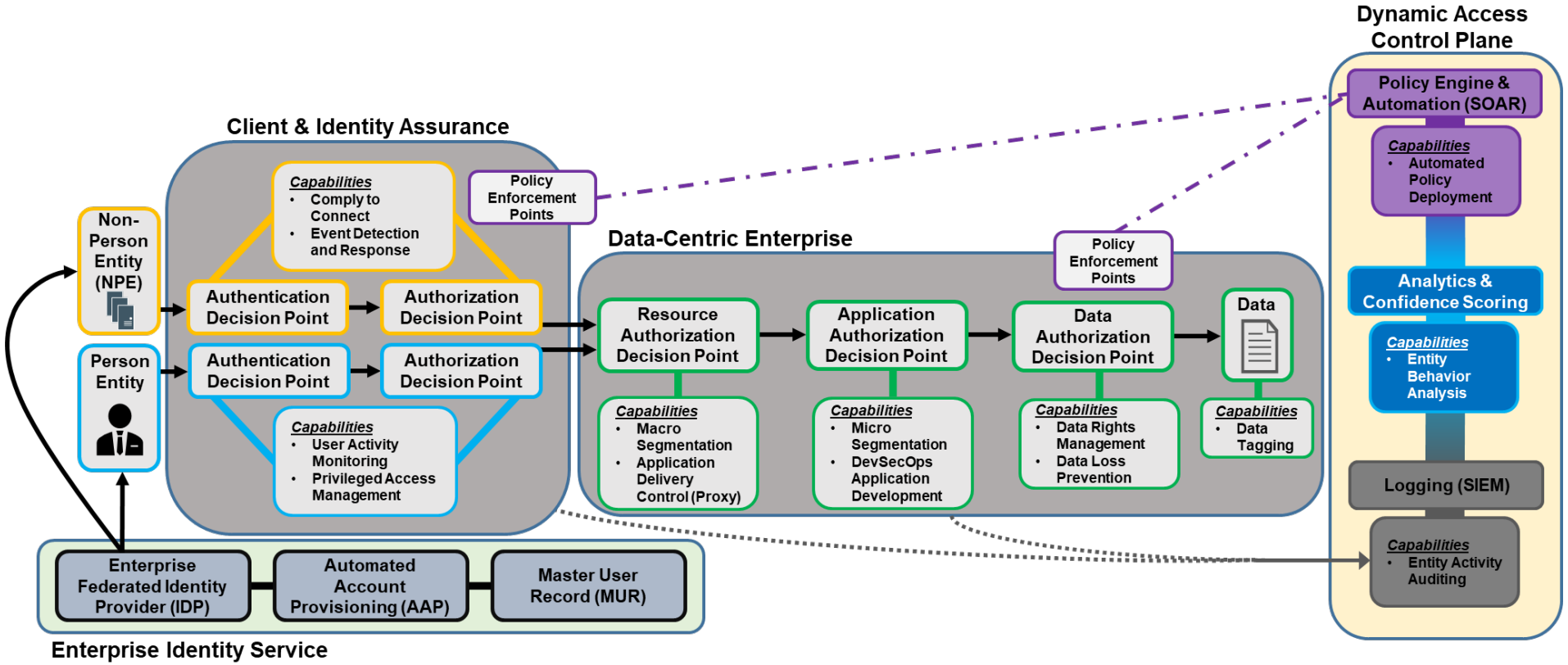

Figure 2: High-Level Operational Concept (OV-1)

1.6 Intended Uses and Audience

Zero Trust is a cybersecurity strategy and framework that embeds security principles throughout the architecture for the purpose of protecting data and service operations, preventing, detecting, responding, and recovering from malicious cyber activities. The perspective of the Zero Trust RA is to guide the developer, operator, manager, and user of Zero Trust in the development of solutions to implement a Zero Trust framework within an existing environment.

This Zero Trust RA's intent is to:

- Provide stakeholders with operational context needed to better understand principles and rules when applying a ZTA
- Define capabilities required to enable a ZTA
- Provide baseline description of Zero Trust for use in managing change and risk associated with evolving operational needs

1.7 Assumptions

Zero Trust assumes continued and mandated use of communication encryption to the greatest extent possible protecting confidentiality and integrity and providing source authentication. The following core assumptions drive planning, risks assessment, and justification of DOD investment in Zero Trust[6]:

- DOD faces threats that demand a transformational shift in current security paradigms to protect critical assets and information.
- Technologies will exist, will be mature, and available/implementable to achieve a DOD Zero Trust migration across the information enterprise.
- Enough resources will be provided to execute this revised security strategy over the next several years.
- Zero Trust assumes continued and mandated use of communication encryption to the greatest extent possible.
- Multiple decentralized Service pilots and proof-of-concepts will require integration and synchronization to work in a centralized manner towards a common, objective Zero Trust end-state.
- No single device or capability produces a Zero Trust framework. Zero Trust is a holistic approach to domain/enterprise security that leverages several different technologies to derive a robust, critical asset-based architecture.
- Broad security policies will be universally and consistently automated and orchestrated at the macro level for the DOD enterprise. More granular security policies and access controls will be automated and orchestrated at the micro level by mission owners.

6 Department of Defense Zero Trust Strategy – Predecisional, July 2020.

1.8 Constraints

Zero Trust assumes continued and mandated use of communication encryption to the greatest extent possible. The following core constraints drive planning, risks assessment, and justification of DOD investment in Zero Trust

- Limited testing due to current environmental constraints has been completed on the capabilities that support the Zero Trust RA version 1.0. Additional development and refinement stages will be completed to produce DOD Zero Trust RA version 2.0.

1.9 Linkages to Other Architectures

1.9.1 DOD Cyber Security Reference Architecture (CS RA) Integration

1.9.1.1 Architecture Description

The CS RA describes the capabilities, services, activities, principles, functions, and technical infrastructure necessary to successfully operate and defend the Department of Defense Information Network (DODIN). This RA is not static but provides a baseline (or standard) list of cybersecurity capabilities. Technology and architecture will be configured to support any interim, transitional, or objective cyberspace command and control (C2) model selected for implementation by the DOD. The CS RA will serve as a primary source of guidance for RAs, solution architectures, and programs necessary to achieve the vision of the Joint Information Environment (JIE) and will be used to assess compliance of security architecture to established standards.

1.9.1.2 Architecture Usage

The CS RA will be used by DOD Components as the basis for development of Component-specific solution architectures, engineering documentation, and implementation plans. This document will serve as a source of input for funding justification, acquisition planning documents, testing and evaluation plans, and information technology portfolio management decisions. The CS RA should also be considered for relevance to existing and new programs.

1.9.1.3 Linkage

The CS RA provides an architectural frame of reference for implementations but does not currently incorporate Zero Trust (as of version 4.1). As a result, DOD Zero Trust Reference Architecture will be authoritatively referenced in the Zero Trust addendum of the DOD CS RA which will include other non-infrastructure considerations. This document will account for critical security considerations around identity, automation and data security while the CS RA will account for higher level security and engineering concepts.

1.9.2 DOD ICAM Reference Design (RD)

1.9.2.1 Reference Design Description

The purpose of this Identity, Credential, and Access Management (ICAM) Reference Design (RD) is to provide a high-level description of ICAM from a capability perspective, including transformational goals for ICAM in accordance with the Department of Defense (DoD) Digital Modernization Strategy. As described in Goal 3, Objective 2 of the DoD Digital Modernization Strategy, ICAM "creates a secure and trusted environment where any user can access all authorized resources (including [services, information systems], and data) to have a successful mission, while also letting the Department of Defense (DoD) know who is on the network at any given time." [7]This objective focuses on managing access to DoD resources while balancing the responsibility to share with the need to protect. ICAM is not a single process or technology but is a complex set of systems and services that operate under varying policies and organizations.

1.9.2.2 Reference Design Usage

This document is not intended to mandate specific technologies, processes, or procedures. Instead, it is intended to:

- Aid mission owners in understanding ICAM requirements and describing current and planned DoD enterprise ICAM services to enable them to make decisions ICAM implementation so that it meets the needs of the mission, including enabling authorized access by mission partners.
- Support the owners and operators of DoD enterprise ICAM services so that these services can effectively interface with each other to support ICAM capabilities.
- Support DoD Components in understanding how to consume DoD enterprise ICAM services and how to operate DoD Component, COI, or local level ICAM services when DoD enterprise services do not meet mission needs.

Each mission owner is responsible for ensuring ICAM is implemented in a secure manner consistent with mission requirements. Conducting operational, threat representative cybersecurity testing as part of ICAM implementation efforts is a mechanism that needs to be used to check secure implementation.

1.9.2.3 Linkage

The DOD ZT RA leverages concepts and lexicon from the ICAM RD to provide a unified and consistent approach to implementing Zero Trust Architecture. This document will not include exhaustive references to ICAM use cases but will acknowledge critical concepts as enablers to Zero Trust. References to the ICAM RD are included throughout the DOD ZT RA, however more in depth ICAM specific use cases are only available in the ICAM RD.

---

7 DOD ICAM Reference Design, June 2020

1.9.2.4 Artifact Availability

The ICAM Reference Design is accessible on via the DOD CIO Library at:

https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf

1.9.3 NIST Special Publication 800-207 Zero Trust Architecture

1.9.3.1 Architecture Description

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.[8]

1.9.3.2 Linkage

The DOD ZT RA leverages concepts and lexicon from the NIST guidance to provide a unified and consistent approach to implementing Zero Trust Architecture. References to the NIST 800-207 are included throughout the DOD ZT RA.

1.9.3.3 Artifact Availability

The NIST Special Publication 800-207 Zero Trust Architecture is available from the NIST Computer Security Resource Center:

https://csrc.nist.gov/publications/detail/sp/800-207/final

8 NIST SP 800-207 Zero Trust Architecture, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

1.10 Tool Environment

The tools used to develop the ZT RA include common office productivity and technical drawing commercial software solutions.

1.11 Maturity Model

The approach to full Zero Trust implementation begins with preparatory discovery and assessment tasks. The initial discovery process will identify data on access and authorization activity within the architecture. Relationships between workloads, networks, devices and users must be discovered.

The end state Zero Trust Architecture requires the implementation of security policies tied back to specific authorization attributes and the confidence level of the user and entity. Prerequisite assessment of the environment will determine the compliance state, privilege account levels and validate implementation of existing security controls.

Prior to designing a Zero Trust Architecture, a baseline protection level must be implemented which is in compliance with existing IT security policies and standards. It is possible to mature aspects of the Zero Trust design without hitting all capabilities and controls.

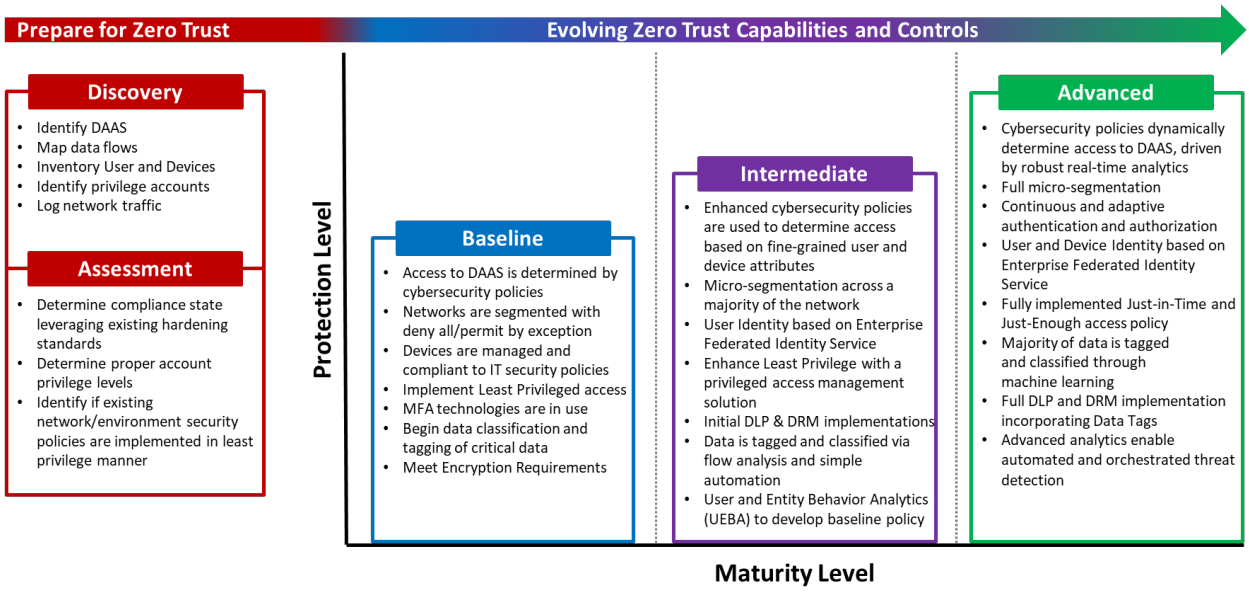

Figure 3: Zero Trust Maturity Model

2 PRINCIPLES

2.1 Overview

Zero Trust Security "is an emerging initiative that DOD CIO is exploring in concert with DISA, US Cyber Command (USCYBERCOM), and the National Security Agency (NSA). Zero Trust is a cybersecurity strategy developing an architecture that requires authentication or verification before granting access to sensitive data or protected resources at a financial cost by reducing data loss and preventing data breaches. This security model eliminates the idea of trusted networks, devices, personas or processes, and shifts to multi-attribute and multi-checkpoint based confidence levels that enable authentication and authorization policies under the concept of least privileged access. Implementing Zero Trust requires rethinking how we utilize existing infrastructure to implement security by design in a simpler and more efficient way while enabling unimpeded operations."[9]

While straightforward in principle, the actual implementation and operationalization of Zero Trust incorporates several areas which need to be smartly integrated and that include software defined networking, data tagging, behavioral analytics, access control, policy orchestration, encryption, automation, as well as end-to-end identity, credential, and access management (ICAM). Enterprise level considerations include identifying which data, applications, assets, and services to protect, and mapping transaction flows, policy decisions, and locations of policy enforcement. Apart from the advantages to securing our architecture in general, there are additional cross-functional benefits of Zero Trust regarding cloud deployments, Security Orchestration and Automation (SOAR), cryptographic modernization and cybersecurity analytics.

2.1.1 Concept and Tenets of Zero Trust

The Zero Trust security model re-thinks how to implement security access to resources and is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attribute. Confidence levels are built from multiple attributes of the subject being authenticated (identity, location, time, device security posture) and allow a much more thorough evaluation of access requests beyond credential verification.

Zero Trust has five major tenets:

- **Assume a Hostile Environment.** There are malicious personas both inside and outside the network. All users, devices, and networks/environments are treated as untrusted.
- **Presume Breach.** There are hundreds of thousands of attempted cybersecurity attacks against DOD networks every day. Consciously operate and defend resources with the

9 DOD Digital Modernization Strategy, June 2019

assumption that an adversary has presence within your environment. Enhanced scrutiny of access and authorization decisions to improve response outcomes.

- **Never Trust, Always Verify**. Deny access by default. Every device, user, application/workload, and data flow are authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.
- **Scrutinize Explicitly**. All resources are consistently accessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources. Access to resources is conditional and access can dynamically change based on action and confidence levels resulting from those actions.
- **Apply Unified Analytics.** Apply unified analytics for Data, Applications, Assets, Services (DAAS) to include behavioristics, and log each transaction

Zero Trust assumes continued and mandated use of communication encryption to the greatest extent possible. The use of mutual authentication of users with client certificates to web applications has long been the effective standard. The DOD is making strides to improve access to data by approving multiple authenticators and authorization schemes to better improve usability and access while maintaining security and visibility.

2.1.2 Principles, Pillars & Capabilities

In alignment with common industry and academic Zero Trust principles, the following pillar and capability model has been developed (see Figure 4). A Pillar is a key focus area for implementation of Zero Trust controls. Capabilities are the ability to achieve a Desired Effect under specified (performance) standards and conditions through combinations of ways and means (activities and resources) to perform a set of activities. Pillars align with capabilities such as identity authentication and software defined enterprise. Sub-Capabilities such as enterprise identity provider or Just-In-Time analytics support capabilities. Capabilities and sub-capabilities as defined reflect the current technologies that are applicable in Zero Trust and are subject to change in future iterations of the Zero Trust Reference Architecture. This layered approach allows for flexibility in implementing Zero Trust controls. Overarching governance will be required to achieve proper integration across pillars and capabilities. The pillar and capabilities enable maximum visibility and protection of data, which are the key focuses of any implementation of Zero Trust.

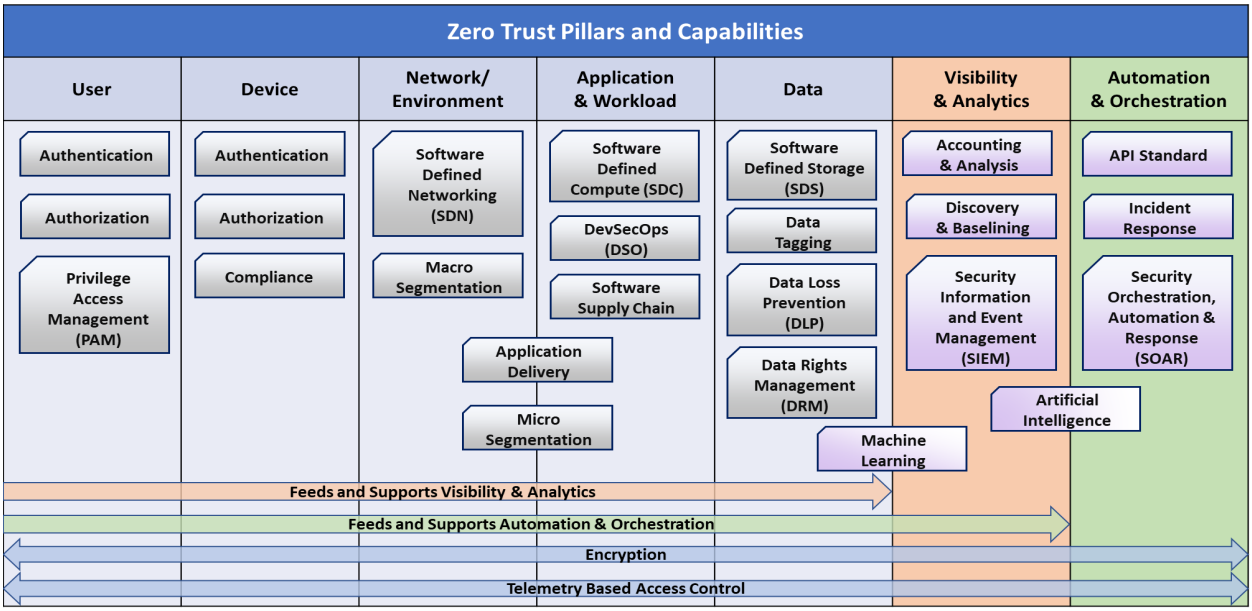

Figure 4: Zero Trust Pillars

The Seven Zero Trust pillars assist with the categorization of capabilities and technologies that can perform Zero Trust functions in an environment. The seven pillars in the DOD Zero Trust Architecture include:

User: Securing, limiting, and enforcing person, non-person, and federated entities' access to DAAS encompasses the use of ICAM capabilities such as multi-factor authentication (MFA) and continuous multi-factor authentication (CMFA). Organizations need the ability to continuously authenticate, authorize, and monitor activity patterns to govern users' access and privileges while protecting and securing all interactions. RBAC and ABAC will apply to policies within this pillar to authorize users towards access of applications and data.

Device: Having the ability to identify, authenticate, authorize, inventory, isolate, secure, remediate, and control all devices is essential in a Zero Trust approach. Real-time attestation and patching of devices in an enterprise are critical functions. Some solutions such as Mobile Device Managers or Comply to Connect programs provide data that can be useful for device confidence assessments. Other assessments should be conducted for every access request (e.g. examinations of compromise state, anomaly detection, software versions, protection status, encryption enablement, etc.).

Network/Environment: Segment (both logically and physically), isolate, and control the network/environment (on-premises and off-premises) with granular access and policy restrictions. As the perimeter becomes more granular through macro-segmentation, micro-segmentation provides greater protections and controls over DAAS. It is critical to (a) control privileged access, (b) manage internal and external data flows, and (c) prevent lateral movement.

Applications and Workload: Applications and workloads include tasks on systems or services on-premises, as well as applications or services running in a cloud environment. Zero Trust workloads span the complete application stack from application layer to hypervisor. Securing and properly managing the application layer as well as compute containers and virtual machines is central to Zero Trust adoption. Application delivery methods such as proxy technologies, enable additional protections to include Zero Trust decision and enforcement points. Developed Source Code and common libraries are vetted through DevSecOps development practices to secure applications from inception.

Data: Zero Trust protects critical data, assets, applications and services. A clear understanding of an organization's DAAS is critical for a successful implementation of a zero trust architecture. Organizations need to categorize their DAAS in terms of mission criticality and use this information to develop a comprehensive data management strategy as part of their overall Zero Trust approach. This can be achieved through the categorization of data, developing schemas, and encrypting data at rest and in transit. Solutions such as DRM, DLP, Software Defined Storage and granular data-tagging are relevant in protecting critical data.

Visibility and Analytics: Vital, contextual details provide greater understanding of performance, behavior and activity baseline across other Zero Trust pillars. This visibility improves detection of anomalous behavior and provides the ability to make dynamic changes to security policy and real-time access decisions. Additionally, other monitoring systems, such as sensor data in addition to telemetry will be used, will help fill out the picture of what is happening with the environment and will aid in the triggering of alerts use for response. A Zero Trust enterprise will capture and inspect traffic, looking beyond network telemetry and into the packets themselves to accurately discover traffic on the network and observe threats that are present and orient defenses more intelligently

Automation and Orchestration: Automate manual security processes to take policy-based actions across the enterprise with speed and at scale. SOAR improves security and decreases response times. Security orchestration integrates Security Information and Event Management (SIEM) and other automated security tools and assists in managing disparate security systems. Automated security response requires defined processes and consistent security policy enforcement across all environments in a Zero Trust enterprise to provide proactive command and control.

3 TECHNICAL POSITIONS (STDV-1, STDV-2)

3.1 Standards Profile (StdV-1)

Table C-1 details the listing of standards that apply to the solution elements of each ZT pillar. This list includes Technical standards (TECH); relevant Laws, Regulations, or Policies (LRP); and Tactics, Techniques and Procedures (TTP).

Table 1: Standards Profile (StdV-1)

#	Standard Identifier	Standard Title	Abstract	Type
1	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008	RFC 5280 profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet. An overview of this approach and model is provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described, and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is described in detail along with standard and Internet-specific extensions. An algorithm for X.509 certification path validation is described. An ASN.1 module and examples are provided in the appendices.	TECH
2	IETF RFC 6187	X.509v3 Certificates for Secure Shell Authentication	X.509 public key certificates use a signature by a trusted certification authority to bind a given public key to a given digital identity. This document specifies how to use X.509 version 3 public key certificates in public key algorithms in the Secure Shell protocol.	TECH
3	IETF RFC 2845	Secret Key Transaction Authentication for DNS (TSIG), May 2000	IETF RFC 2845 (TSIG) allows for transaction level authentication using shared secrets and one-way hashing. It can be used to authenticate dynamic updates as coming from an approved client, or to authenticate responses as coming from an approved recursive name server.	TECH
4	IETF RFC 2865	Remote Authentication Dial in User Services (RADIUS), June 2000	This describes a protocol for carrying authentication, authorization, and configuration information between Network Access Servers that authenticate links through a shared Authentication Server. Managing dispersed serial line	TECH

			and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are a link to the outside world, they require careful attention to security, authorization and accounting. This can be best achieved by managing a single "database" of users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user (for example, SLIP, PPP, telnet, rlogin). RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.	
5	IETF RFC 4511	Lightweight Directory Access Protocol (LDAP), June 2006	Lightweight Directory Access Protocol (LDAP) is a client/server protocol used to access and manage directory information. It reads and edits directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer. It was originally developed as a front end to X.500 Directory Access Protocol.	TECH
6	SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	OASIS SAML 2.0 defines the syntax and semantics for XML-encoded assertions about authentication, attributes and authorization, and for the protocol that conveys this information. The specifications define the syntax and semantics for XML-encoded SAML assertions, protocol requests, and protocol responses. These constructs are typically embedded in other structures for transport using SOAP 1.1 over HTTP. SAML v2.0 introduces a number of new features, including: - Pseudonyms (a key privacy-enabling technology) - Identifier management (for managing pseudonyms) - Metadata (for expressing configuration and trust-related data to make deployment of SAML systems	TECH

			easier) - Encryption (so that attribute statements, name identifiers, or entire assertions can be encrypted in place) - Attribute profiles - Session management (for single logout) - Mobile device support (to better address their challenges and opportunities) - Identity provider discovery (for deployments having more than one identity provider)	
7	SAML V2.0 Attribute Sharing Profile for X.509 A-BS	SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Committee Specification 01	The SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems describes the use of the SAML V2.0 Assertion Query and Request Protocol [SAMLCore] in conjunction with the SAML V2.0 SOAP Binding [SAMLBind] to retrieve the attributes of a principal who has authenticated using an X.509 certificate. There are two modes of operation specified in the deployment profile: Basic Mode and Encrypted Mode. The Basic Mode deployment profile extends the SAML V2.0 Assertion Query/Request Profile [SAMLProf]. The Encrypted Mode deployment profile specifies the use of encryption to protect the privacy of the principal. The Encrypted Mode deployment profile is of interest to the Intelligence Community, as it supports the integrity and confidentiality requirements necessary for the exchange of identity and attribute information between IC Agencies. [SAMLCore] S. Cantor et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf. [SAMLBind] S. Cantor et al. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf. [SAMLProf] S. Cantor et al. Profiles for the OASIS	TECH

			Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.	
8	XACML 2.0 OASIS	eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 February 2005	OASIS XACML 2.0 defines the syntax and semantics for XML-encoded access control policies. XACML defines three top-level policy elements: "Rule", "Policy" and "PolicySet". The "Rule" element contains a Boolean expression that can be evaluated in isolation, but that is not intended to be accessed in isolation by a PDP. So, it is not intended to form the basis of an authorization decision by itself. It is intended to exist in isolation only within an XACML PAP, where it may form the basic unit of management, and be re-used in multiple policies. The "Policy" element contains a set of "Rule" elements and a specified procedure for combining the results of their evaluation. It is the basic unit of policy used by the PDP, and so it is intended to form the basis of an authorization decision. The "PolicySet" element contains a set of "Policy" or other "PolicySet" elements and a specified procedure for combining the results of their evaluation. It is the standard means for combining separate policies into a single combined policy.	TECH
9	FIPS Pub 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013	This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems. The standard contains two major sections. Part one describes the minimum requirements for a Federal personal identity verification	TECH

			system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, Interfaces for Personal Identity Verification. Similarly, the interfaces and data formats of biometric information are specified in Special Publication 800-76, Biometric Data Specification for Personal Identity Verification. This standard does not specify access control policies or requirements for Federal departments and agencies.	
10	IETF RFC 6421	Crypto-Agility Requirements for Remote Authentication Dial-In User Service (RADIUS), November 2011	IETF RFC6421 formalizes crypto-agility requirements for RADIUS. In this informational memo, crypto-agility is defined as the ability of a protocol to adapt to evolving cryptography and security requirements. In the context of the RADIUS protocol and implementations, crypto-agility is defined as the ability of RADIUS implementations to automatically negotiate cryptographic algorithms. RADIUS uses cryptographic algorithms to integrity protect and authenticate RADIUS packets and to hide certain RADIUS attributes. RADIUS packets, excluding the Access-Request and Status-Server packets, are protected by MD5 message integrity check (MIC). HMAC-MD5 provides authentication and	TECH

			integrity protection to RADIUS packets utilizing the Message-Authenticator Attribute. Confidentiality of entire packets is not supported by RADIUS; however, certain values, e.g. User Password, Tunnel-Password, and some vender defined attributes, are encrypted using a stream cipher based on a key stream from a MD5 digest. IETF RFC6421 also defines a two-phase submission process for publishing RADIUS crypto-agility solutions. The initial submission of a crypto-agility solution is published as an Experimental IETF RFC. Solutions that are selected by the RADIUS Extensions (RADEXT) Working Group (WG) proceed to the standards track. Solutions are not restricted to using existing technology referenced in other IETF RFCs, e.g. "RADIUS and IPv6, RFC3162, which is available for use. On the contrary, the RADEXT WG is expecting solutions that present new techniques.	
11	DOD IdAM DD v1.0	DOD Identity and Access Management (IdAM) Data Dictionary, Version 1.0, August 14, 2013	The DOD IdAM Data Dictionary, Version 1.0, dated August 14, 2013, defines the full scope of DOD Enterprise attributes utilized by DOD Enterprise Directory Services (EDS) on both the Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet). The purpose of this document is to enable the standardization of DOD Identity and Access Management (IdAM) data. The emergence of this standardization allows for the abilities of data consistency, data uniformity, and reduced system integration costs. The attributes defined in this document apply to all DOD person entities, along with Non-Person Entities (NPEs) not entirely controlled by, and for the exclusive use of, a single DOD organization. This guidance should be followed by all DOD Combatant Commands, Services, and Agencies (CC/S/A) and is primarily	LRP

			provided for DOD digital identity engineers and architects.	
12	DODI 8520.03	DOD Instruction 8520.03, “Identity Authentication for Information Systems”, May 13, 2011	Implements policy that assigns responsibilities, and prescribes procedures for implementing identity authentication of all entities to DOD information systems.	LRP
13	SP 800-171 Rev. 2	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations are of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions. This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.	TECH
14	NIST Special Publication 800-76-2	Biometric Data Specification for Personal	Homeland Security Presidential Directive HSPD-12, Policy for a Common Identification Standard for Federal	TECH

		Identity Verification, July 2013	Employees and Contractors [HSPD-12], called for Homeland Security Presidential Directive HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors [HSPD-12], called for new standards to be adopted governing interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) standard for Federal Employees and Contractors, Federal Information Processing Standard Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201), was developed to define procedures and specifications for issuance and use of an interoperable identity credential. This document, Special Publication 800-76 (SP 800-76), is a companion document to FIPS 201. It describes technical acquisition and formatting specifications for the PIV system, including the PIV Card itself. It also establishes minimum accuracy specifications for deployed biometric authentication processes. The approach is to enumerate procedures and formats for collection and preparation of fingerprint, iris and facial data, and to restrict values and practices included generically in published biometric standards. The primary design objective behind these specifications is to enable high performance and universal interoperability. The introduction of iris and face specifications into the current edition adds alternative modalities for biometric authentication and extends coverage to persons for whom fingerprinting is problematic. The addition of on-card comparison offers an alternative to PIN-mediated card activation as well as an additional authentication method.	

15	IATA-STD-030-WAC-V1.0	Information Assurance Technical Authority (IA TA) Wireless Access Control (WAC) Standard Version 1.0 9/19/2017	This Standard is one of many that outline specific DFIA-required Cybersecurity protections. Compliance with the DFIA and applicable IA TA requirements enables a more transparent and secure system that meets applicable DOD and DON guidance and policy.	TECH
16	IEEE Std 802.1X-2020	CIEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control	Port-based network access control allows a network administrator to restrict the use of IEEE 802 LAN service access points (ports) to secure communication between authenticated and authorized devices. This standard specifies a common architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and that secure communication between the ports, including the media access method independent protocols that are used to discover and establish the security associations used by IEEE 802.1AE MAC Security.	TECH
17	NIST Special Publication (SP) 800-37 Rev. 2	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy October 2, 2018	NIST Special Publication (SP) 800-37 Rev. 2 is the updated version of Risk Management Framework (RMF) for DoD Information Technology (IT) it provides guidelines for applying the Risk Management Framework (RMF) to information systems and organizations. The RMF includes a disciplined, structured, and flexible process for organizational asset valuation; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.	TECH
18	NIST SP 800-119	Guidelines for the Secure Deployment of IPv6, December 2010	NIST 800-119 is intended to be used as guidance publication for implementers about IPv6 features and the security impacts of the features. It also gives a comprehensive survey of mechanisms that can be used during the deployment phase of IPv6. NIST 800-119 in generally lays out a strategic plan for moving to an	TECH

			IPv6 environment. IPv6 is not backwards compatible with IPv4, which means that implementers will have to change their existing infrastructure and systems to deploy IPv6. This CR for NIST SP 800-119 will increase the understanding of risk of deploying IPv6, as well as strategies to mitigate such risk. Detailed planning to deploy IPv6, which NIST 800-119 specifies, would allow implementation processes to operate securely and as intended.	
19	NIST SP 800-160 Volume I	Systems Security Engineering (SSE) Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, November 2016 (Including updates as of 03-21-2018)	With the continuing frequency, intensity, and adverse consequences of cyber-attacks, disruptions, hazards, and other threats to federal, state, and local governments, the military, businesses, and the critical infrastructure, the need for trustworthy secure systems has never been more important to the long-term economic and national security interests of the United States. Engineering-based solutions are essential to managing the growing complexity, dynamicity, and interconnectedness of today's systems, as exemplified by cyber-physical systems and systems-of-systems, including the Internet of Things. This publication addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems. It starts with and builds upon a set of well-established International Standards for systems and software engineering published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE) and infuses systems security engineering methods, practices, and techniques into those systems and	TECH

			software engineering activities. The objective is to address security issues from a stakeholder protection needs, concerns, and requirements perspective and to use established engineering processes to ensure that such needs, concerns, and requirements are addressed with appropriate fidelity and rigor, early and in a sustainable manner throughout the life cycle of the system.	
20	NIST SP 800-160 Volume 2	Developing Cyber Resilient Systems: A Systems Security Engineering Approach November 2019	This publication is used in conjunction with ISO/IEC/IEEE 15288:2015, Systems and software engineering-Systems life cycle processes, NIST Special Publication 800-160, Volume 1, Systems Security Engineering-Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, and NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations-A System Life Cycle Approach for Security and Privacy. It can be viewed as a handbook for achieving the identified cyber resiliency outcomes based on a system engineering perspective on system life cycle processes in conjunction with risk management processes, allowing the experience and expertise of the organization to help determine what is correct for its purpose. Organizations can select, adapt, and use some or all the cyber resiliency constructs (i.e., objectives, techniques, approaches, and design principles) described in this publication and apply the constructs to the technical, operational, and threat environments for which systems need to be engineered. The system life cycle processes and cyber resiliency constructs can be used for new systems, system upgrades, or repurposed systems; can be employed at any stage of the system life cycle; and can take advantage of any system or software development methodology including, for example,	TECH

			waterfall, spiral, or agile. The processes and associated cyber resiliency constructs can also be applied recursively, iteratively, concurrently, sequentially, or in parallel and to any system regardless of its size, complexity, purpose, scope, environment of operation, or special nature. The full extent of the application of the content in this publication is guided and informed by stakeholder protection needs, mission assurance needs, and concerns with cost, schedule, and performance. The tailorable nature of the engineering activities and tasks and the system life cycle processes ensure that systems resulting from the application of the security and cyber resiliency design principles, among others, have the level of trustworthiness deemed enough to protect stakeholders from suffering unacceptable losses of their assets and associated consequences. Trustworthiness is made possible, in part, by the rigorous application of the security and cyber resiliency design principles, constructs, and concepts within a structured set of systems life cycle processes that provides the necessary traceability of requirements, transparency, and evidence to support risk-informed decision-making and trades.	
21	IATA-STD-013-ITAM-V1.0	Information Technology Asset Management Standard Version 1.0 26 April 2016	This Standard defines the requirements for Information Technology Asset Management (ITAM) implementation as an integral part of computing environment protection and overall security of the DOD Information Network and the Department of the Navy (DON) Naval Enterprise Networks. This Standard specifies the requirements and activities necessary for standardized implementation and configuration of ITAM as part of the Defense-in-Depth Functional Implementation Architecture (DFIA).	TECH

22	NIST SP 800-204	Security Strategies for Microservices-based Application Systems	Microservices architecture is increasingly being used to develop application systems since its smaller codebase facilitates faster code development, testing, and deployment as well as optimization of the platform based on the type of microservice, support for independent development teams, and the ability to scale each component independently. Microservices generally, communicate with each other using Application Programming Interfaces (APIs), which requires several core features to support complex interactions between a substantial number of components. These core features include authentication and access management, service discovery, secure communication protocols, security monitoring, availability/resiliency improvement techniques (e.g., circuit breakers), load balancing and throttling, integrity assurance techniques during induction of new services, and handling of session persistence. Additionally, the core features could be bundled or packaged into architectural frameworks such as API gateways and service mesh. The purpose of this document is to analyze the multiple implementation options available for each individual core feature and configuration options in architectural frameworks, develop security strategies that counter threats specific to microservices, and enhance the overall security profile of the microservices-based application.	TECH
23	NIST SP 800-204A	Building Secure Microservices-based Applications Using Service-Mesh Architecture	The increasing trend in building microservices-based applications calls for addressing security in all aspects of service-to-service interactions due to their unique characteristics. The distributed	TECH

			cross-domain nature of microservices needs secure token service (STS), key management and encryption services for authentication and authorization, and secure communication protocols. The ephemeral nature of clustered containers (by which microservices are implemented) calls for secure service discovery. The availability requirement calls for: (a) resiliency techniques, such as load balancing, circuit breaking, and throttling, and (b) continuous monitoring (for the health of the service). The service mesh is the best-known approach that can facilitate specification of these requirements at a level of abstraction such that it can be uniformly and consistently defined while also being effectively implemented without making changes to individual microservice code. The purpose of this document is to provide deployment guidance for proxy-based Service Mesh components that collectively form a robust security infrastructure for supporting microservices-based applications.	
24	ICS 500-201	Tagging of Intelligence and Intelligence-Related Information		TECH
25	DODI 8170.01	DOD Instruction 8170.01, Online Information Management and Electronic Messaging	In accordance with the authority in DOD Directive (DODD) 5144.02, this issuance: • Establishes policy, assigns responsibilities, and prescribes procedures for: o Conducting, establishing, operating, and maintaining electronic messaging services (including, but not limited to, e-mail) to collect, distribute, store, and otherwise process official DOD information, both unclassified and classified, as applicable. o Managing official DOD information on the DOD Information Network and other networks, i.e.,online.	LRP

			o Provides a compendium of policies and procedures critical to successful online information management and electronic messaging.	
26	DODI 8230.07	DOD Instruction 8230.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense	Describes or references key enablers necessary for sharing data, information, and IT services and ensuring data, information, and IT services are visible, accessible, understandable, trustworthy, and interoperable. Key enablers include, but are not limited to, concepts, processes, governance forums, standards, models, and shared vocabularies. For the purposes of the instruction, data sharing and information sharing are equivalent terms. Service and IT service, are used interchangeably throughout this instruction. IT services include DOD Enterprise Services; however, not all IT services are DOD Enterprise Services.	LRP
27	DSP0004 v2.7.0	Common Information Model (CIM) Infrastructure, Version 2.7.0, 2012-04-22	Distributed Management Task Force's (DMTF) Common Information Model Infrastructure specification provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. CIM's common definitions enable vendors to exchange semantically rich management information between systems throughout the network. CIM is composed of a schema and multiple specifications. The schema provides the actual model descriptions, while the different specifications defines the details for integration with other management models. The schema specification is defined in DISR012013 and this Change Request is concerning the Infrastructure specification.	TECH
28	IATA-STD-021-CDS-V1.0	Information Sharing Cross Domain Solution (CDS) Standard, 15 January 2017	This Standard defines the requirements that support Cross Domain Solution (CDS) implementation as an integral part of computing environment protection and	TECH

			overall security of the Defense Information Systems Network and the Department of the Navy (DON) Naval Enterprise Networks. This Standard does not make a security control "required" for any system; rather, this Standard is designed to specify the requirements and activities necessary for standardized implementation and configuration of applicable security controls as part of the Defense-in-Depth Functional Implementation Architecture (DFIA).	
29	FIPS Pub 140-3	Security Requirements for Cryptographic Modules	This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operating environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks. This standard supersedes FIPS 140-2, Security Requirements for Cryptographic Modules, in its entirety.	TECH
30	Executive Order 13859	Maintaining American Leadership in Artificial Intelligence	Emphasizing the importance of artificial intelligence (AI) to the future of the U.S. economy and national security, on February 11, 2019, the President issued an Executive Order (EO 13859) directing	LRP

			Federal agencies to ensure that the nation maintains its leadership position in AI. Among its objectives, the EO aims to "Ensure that technical standards…reflect Federal priorities for innovation, public trust, and public confidence in systems that use AI technologies…and develop international standards to promote and protect those priorities."	
31	NIST SP 1500-4r2	NIST Big Data Interoperability Framework: Volume 4, Security and Privacy Version 3	Big Data is a term used to describe the large amount of data in the networked, digitized, sensor-laden, information-driven world. While opportunities exist with Big Data, the data can overwhelm traditional technical approaches and the growth of data is outpacing scientific and technological advances in data analytics. To advance progress in Big Data, the NIST Big Data Public Working Group (NBD-PWG) is working to develop consensus on important, fundamental concepts related to Big Data. The results are reported in the NIST Big Data Interoperability Framework (NBDIF) series of volumes. This volume, Volume 4 contains an exploration of security and privacy topics with respect to Big Data. The volume considers new aspects of security and privacy with respect to Big Data, reviews security and privacy use cases, proposes security and privacy taxonomies, presents details of the Security and Privacy Fabric of the NIST Big Data Reference Architecture (NBDRA), and begins mapping the security and privacy use cases to the NBDRA.	TECH
32	NIST SP 800-18 Rev. 1	Guide for Developing Security Plans for Federal Information Systems	The objective of system security planning is to improve protection of information system resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The completion of system security plans	TECH

			is a requirement of the Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources,” and” Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA).	
33	NIST SP 800-60 Vol. 1 Rev. 1	Guide for Mapping Types of Information and Information Systems to Security Categories	This guideline has been developed to assist Federal government agencies to categorize information and information systems. The guideline’s objective is to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system.	TECH
34	NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	The purpose of this guideline is to assist organizations in the development of an ISCM strategy and the implementation of an ISCM program that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of deployed security controls. The ISCM strategy and program support ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance, as well as the ability to provide the information needed to respond to risk in a timely manner.	TECH
35	FIPS Pub 199	Standards for Security Categorization of Federal Information and Information Systems, February 2004	The E-Government Act of 2002 (Public Law 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with	TECH

			responsibilities for standards and guidelines, including the development of: - Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels; - Guidelines recommending the types of information and information systems to be included in each category; and - Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category. FIPS Publication 199 addresses the first task cited-to develop standards for categorizing information and information systems.	
36	NIST SP 800-115	Technical Guide to Information Security Testing and Assessment	The purpose of this document is to provide guidelines for organizations on planning and conducting technical information security testing and assessments, analyzing findings, and developing mitigation strategies. It provides practical recommendations for designing, implementing, and maintaining technical information relating to security testing and assessment processes and procedures, which can be used for several purposes—such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements. This guide is not intended to present a comprehensive information security testing or assessment program, but rather an overview of the key elements of technical security testing and assessment with emphasis on specific techniques, their benefits and limitations, and recommendations for their use.	TECH

37	IATA-STD-019-CCM-V1.0	Cyber Configuration Management Standard 15 January 2017	This Standard defines the requirements that support Cyber Configuration Management (CCM) implementation as an integral part of computing environment protection and overall security of the Defense Information Systems Network (DISN) and the Department of the Navy (DON) Naval Enterprise Networks.	TECH
38	OGF GFD-P-R.221	Open Grid Forum (OGF) - Grid Final Document (GFD) - Open Cloud Computing Interface (OCCI) 221 - Core, September 19, 2016	The OCCI is an open RESTful protocol and Application Programming Interface (API) for cloud computing services. The OCCI-Core provides a solid foundation for the remote management of compute, network, and storage resources offered in cloud computing environment.	TECH
39	IEEE Std 802.1Q-2018	IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks, July 2018.	This standard specifies how the Media Access Control (MAC) Service is supported by Bridged Networks, the principles of operation of those networks, and the operation of MAC Bridges and VLAN Bridges, including management, protocols, and algorithms.	TECH
40	IATA-STD-009-BP-V2.0	Boundary Protection Standard, Version 2.0, 12 Feb 2018	This standard defines the security requirements that support Boundary Protection (BP) implementation as an integral part of computing environment protection and overall security of the DOD Defense Information Networks, and the Department of the Navy (DON) Naval Enterprise Networks and weapon systems.	TECH
41	IETF RFC 2784	Generic Routing Encapsulation (GRE) March 2000	This document specifies a protocol for encapsulation of an arbitrary network layer protocol over another arbitrary network layer protocol. It supports both IPv4 and IPv6 tunneling.	TECH
42	IETF RFC 3007	Secure DNS Dynamic Update, November 2000	RFC 3007 proposes a method for performing secure Domain Name System (DNS) dynamic updates. The method described here is intended to be flexible and useful while requiring as few changes to the protocol as possible. The authentication of the dynamic update message is separate from later DNSSEC	TECH

			validation of the data. Secure communication based on authenticated requests and transactions is used to provide authorization.	
43	IETF RFC 3198	Terminology for Policy-Based Management, November 2001	This document is a glossary of policy-related terms. It provides abbreviations, explanations, and recommendations for use of these terms. The document takes the approach and format of RFC 2828, which defines an Internet Security Glossary. The intent is to improve the comprehensibility and consistency of writing that deals with network policy, particularly Internet Standards documents (ISDs).	TECH
44	IETF RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002	This document describes the User-based Security Model (USM) for Simple Network Management Protocol (SNMP) version 3 for use in the SNMP architecture. It defines the Elements of Procedure for providing SNMP message level security. This document also includes a Management Information Base (MIB) for remotely monitoring/managing the configuration parameters for this Security Model. This document obsoletes RFC 2574.	TECH
45	IETF RFC 3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model, June 2004	This document describes a symmetric encryption protocol that supplements the protocols described in the User-based Security Model (USM), which is a Security Subsystem for version 3 of the Simple Network Management Protocol for use in the SNMP Architecture. The symmetric encryption protocol described in this document is based on the Advanced Encryption Standard (AES) cipher algorithm used in Cipher Feedback Mode (CFB), with a key size of 128 bits.	TECH
46	IETF RFC 3948	UDP Encapsulation of IPsec ESP Packets, January 2005	This protocol specification defines methods to encapsulate and decapsulate IP Encapsulating Security Payload (ESP) packets inside UDP packets for traversing Network Address Translators. ESP encapsulation, as defined in this	TECH

			document, can be used in both IPv4 and IPv6 scenarios. Whenever negotiated, encapsulation is used with Internet Key Exchange (IKE).	
47	IETF RFC 4120	The Kerberos Network Authentication Service (V5), July 2005	This document provides an overview and specification of Version 5 of the Kerberos protocol, and it obsoletes RFC 1510 to clarify aspects of the protocol and its intended use that require more detailed or clearer explanation than was provided in RFC 1510. This document is intended to provide a detailed description of the protocol, suitable for implementation, together with descriptions of the appropriate use of protocol messages and fields within those messages.	TECH
48	IETF RFC 4448	Encapsulation Methods for Transport of Ethernet over MPLS Networks, April 2006	An Ethernet pseudowire (PW) is used to carry Ethernet/802.3 Protocol Data Units (PDUs) over an MPLS network. This enables service providers to offer "emulated" Ethernet services over existing MPLS networks. This document specifies the encapsulation of Ethernet/802.3 PDUs within a pseudowire. It also specifies the procedures for using a PW to provide a "point-to-point Ethernet" service.	TECH
49	IETF RFC 4577	OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs), June 2006	Many Service Providers offer Virtual Private Network (VPN) services to their customers, using a technique in which customer edge routers (CE routers) are routing peers of provider edge routers (PE routers). The Border Gateway Protocol (BGP) is used to distribute the customer's routes across the provider's IP backbone network, and Multiprotocol Label Switching (MPLS) is used to tunnel customer packets across the provider's backbone. This is known as a "BGP/MPLS IP VPN". The base specification for BGP/MPLS IP VPNs presumes that the routing protocol on the interface between a PE router and a CE router is BGP. This document extends that specification by allowing the routing	TECH

			protocol on the PE/CE interface to be the Open Shortest Path First (OSPF) protocol. This document updates RFC 4364.	
50	IETF RFC 4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN, September 2006	This document describes a method by which a Service Provider may use its packet-switched backbone to provide Virtual Private Network (VPN) services for its IPv6 customers. This method reuses, and extends where necessary, the "BGP/MPLS IP VPN" method for support of IPv6. In BGP/MPLS IP VPN, "Multiprotocol BGP" is used for distributing IPv4 VPN routes over the service provider backbone, and MPLS is used to forward IPv4 VPN packets over the backbone. This document defines an IPv6 VPN address family and describes the corresponding IPv6 VPN route distribution in "Multiprotocol BGP".	TECH
51	IETF RFC 5246	The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008	This document specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.	TECH
52	IETF RFC 6241	Network Configuration Protocol (NETCONF), June 2011	The Network Configuration Protocol (NETCONF) defined in this document provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages. The NETCONF protocol operations are realized as remote procedure calls (RPCs).	TECH
53	IETF RFC 6242	Using the NETCONF Protocol over Secure Shell (SSH), June 2011	This document describes a method for invoking and running the Network Configuration Protocol (NETCONF) within a Secure Shell (SSH) session as an SSH subsystem.	TECH

54	IETF RFC 6353	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), July 2011	RFC 6353 describes a Transport Model for Simple Network Management Protocol (SNMP) that uses either Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) protocols. The TLS and DTLS protocols provide authentication and privacy services for SNMP applications. RFC 6353 describes how the TLS Transport Model (TM) implements the required features of an SNMP transport subsystem making this protection possible in an interoperable way. This TM is designed to meet the security and operational needs of network administrators. RFC 6353 supports the sending of SNMP messages over TLS/TCP (Transmission Control Protocol) and DTLS/UDP (User Datagram Protocol). TLS mode can make use of TCP's improved support for larger packet sizes and DTLS mode provides potentially superior operation in environments where a connectionless (e.g., UDP) transport is preferred. TLS and DTLS integrate into existing public keying infrastructures (PKI). RFC 6353 also defines a portion of the Management Information Base (MIB) for use with network management protocols. It defines objects for managing the TLS TM for SNMP.	TECH
55	IETF RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 2013	This document specifies a protocol useful in determining the current status of a digital certificate without requiring Certificate Revocation Lists (CRLs). Additional mechanisms addressing PKIX (Public-Key Infrastructure X.509) operational requirements are specified in separate documents. This document obsoletes RFCs 2560 and 6277.	TECH
56	IETF RFC 8040	RESTCONF Protocol, January 2017	RESTCONF, which is based on NETCONF functionality, provides standard mechanisms to allow Web applications to access the configuration data, state data, data-model-specific	TECH

			Remote Procedure Call (RPC) operations, and event notifications within a networking device, in a modular and extensible manner. RESTCONF also defines configuration datastores and a set of Create, Read, Update, Delete (CRUD) operations that can be used to access these datastores. RESTCONF uses HTTP methods to provide CRUD operations on a conceptual datastore containing YANG-defined data, which is compatible with a server that implements NETCONF datastores. Like NETCONF, RESTCONF uses the YANG language to define the syntax and semantics of datastore content, configuration, state data, RPC operations, and event notifications.	
57	ISO/IEC 19941:2017	Information technology -- Cloud computing -- Interoperability and portability, 2017	The ISO/IEC 19941:2017 document specifies cloud computing interoperability and portability types, the relationship and interactions between these two cross-cutting aspects of cloud computing and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services.	TECH
58	IETF RFC 4684	Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs), November 2006	This document defines Multi-Protocol BGP (MP-BGP) procedures that allow BGP speakers to exchange Route Target reachability information. This information can be used to build a route distribution graph in order to limit the propagation of Virtual Private Network (VPN) Network Layer Reachability Information (NLRI) between different autonomous systems or distinct clusters of the same autonomous system. This document updates RFC 4364.	TECH
59	IETF RFC 8446	Transport Layer Security (TLS) 1.3, August 2018	This RFC specifies version 1.3 of the Transport Layer Security protocol. The TLS protocol provides secure communications over the Internet and supersedes the Secure Socket Layer (SSL) protocol. The TLS protocol allows web client/server applications to	TECH

			communicate securely by preventing eavesdropping.	
60	NIST SP 800-207	Zero Trust Architecture, August 2020	Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary. Zero trust focus on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.	TECH
61	NIST SP 800-63A	Enrollment & Identity Proofing, June 2017	NIST SP 800-63-A addresses how applicants can prove their identities and become enrolled as valid subscribers within an identity system. It provides requirements by which applicants can both identity proof and enroll at one of three different levels of risk mitigation in both remote and physically-present scenarios.	TECH
62	NIST SP 800-63B	Authentication and Lifecycle Management, June 2017	This document provides recommendations on types of authentication processes, including choices of authenticators, that may be used at various Authenticator Assurance	TECH

			Levels (AALs). It also provides recommendations on the lifecycle of authenticators, including revocation in the event of loss or theft.	
63	NIST SP 800-63C	Federation and Assertions, June 2017	This document, SP 800-63C, provides requirements to identity providers (IdP) and relying parties (RPs) of federated identity systems. Federation allows a given IdP to provide authentication attributes and (optionally) subscriber attributes to a number of separately administered RPs through the use of assertions. Similarly, RPs may use more than one IdP.	TECH

3.2 Standards Forecast (StdV-2)

The Standard Forecast (StdV-2) details the technology related standards, operational standards, or business standards and conventions that are mapped to the capabilities within each Zero Trust pillar. The following definitions are for the status of the standard:

- Emerging – May be implemented but shall not be used in lieu of a mandated standard. An Emerging Standard is expected to be elevated to mandated status within 3 years.
- Mandated – Must be considered during selections of standards by the Program of Record. Must be used in lieu of a competing or similar standard. The standard is required for the management, development, and acquisition of new or improved DOD systems.
- Retired – Should not be used in a new or upgraded system.
- Active (information guidance) – Documents affecting multiple organizations provide a means to further clarify standards and identify relevant policies and procedures. Types of documents include IT-related best practices, information standards, manuals, policy, procedures, and handbooks. Policy does not mandate these documents be cited or used.

Table 2: Standards Forecast (StdV-2)

Pillar Name	Capability Mapping	Standard Identifier	Standard Title	Status
All	All	NIST SP 800-207	Zero Trust Architecture, August 2020	Emerging
User	Authentication	IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008	Mandated
User	Authentication	IETF RFC 6187	X.509v3 Certificates for Secure Shell Authentication	Active
User	Authentication	IETF RFC 2845	Secret Key Transaction Authentication for DNS (TSIG), May 2000	Mandated
User	Authentication	IETF RFC 2865	Remote Authentication Dial In User Services (RADIUS), June 2000	Mandated
User	Authentication, Authorization	SAML 2.0 OASIS	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005	Mandated

User	Authentication, Authorization	SAML V2.0 Attribute Sharing Profile for X.509 A-BS	SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Committee Specification 01	Mandated
User	Authorization	XACML 2.0 OASIS	eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 February 2005	Mandated
User	Authentication	FIPS Pub 201-2	Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013	Mandated
User	Authentication, Authorization	IETF RFC 6421	Crypto-Agility Requirements for Remote Authentication Dial-In User Service (RADIUS), November 2011	Active
User	Authentication, Authorization	DOD IdAM DD v1.0	DOD Identity and Access Management (IdAM) Data Dictionary, Version 1.0, August 14, 2013	Active
Device	Authentication	DODI 8520.03	DOD Instruction 8520.03, “Identity Authentication for Information Systems”, May 13, 2011	Active
Device	Authentication	NIST Special Publication 800-76-2	Biometric Data Specification for Personal Identity Verification, July 2013	Mandated
Device	Authentication, Authorization	IATA-STD-030-WAC-V1.0	Information Assurance Technical Authority (IA TA) Wireless Access Control (WAC) Standard Version 1.0 9/19/2017	Active
Device	Authentication, Authorization	IEEE Std 802.1X-2020	CIEEE Standard for Local and Metropolitan Area	Mandated
Device	Compliance	NIST Special Publication (SP) 800-37 Rev. 2	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy October 2, 2018	Active

Device	Compliance	NIST SP 800-119	Guidelines for the Secure Deployment of IPv6, December 2010	Active
Device	Compliance	NIST SP 800-160 Volume I	Systems Security Engineering (SSE) Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, November 2016 (Including updates as of 03-21-2018)	Active
Device	Compliance	NIST SP 800-160 Volume 2	Developing Cyber Resilient Systems: A Systems Security Engineering Approach November 2019	Active
Device	Compliance	IATA-STD-013-ITAM-V1.0	Information Technology Asset Management Standard Version 1.0 26 April 2016	Active
Network/Environment	Macro segmentation	IEEE Std 802.1X-2020	CIEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control	Mandated
Network/Environment	Macro segmentation	IEEE Std 802.1Q-2018	IEEE Standard For Local and metropolitan area networks -- Bridges and Bridged Networks, July 2018.	Mandated
Network/Environment	Macro segmentation	IATA-STD-009-BP-V2.0	Boundary Protection Standard, Version 2.0, 12 Feb 2018	Active
Network/Environment	Software Defined Network (SDN)	IETF RFC 2784	Generic Routing Encapsulation (GRE) March 2000	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 3007	Secure DNS Dynamic Update, November 2000	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 3198	Terminology for Policy-Based Management, November 2001	Active
Network/Environment	Software Defined Network (SDN)	IETF RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002	Mandated

Network/Environment	Software Defined Network (SDN)	IETF RFC 3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model, June 2004	Mandated
Network/Environment	Application Delivery	IETF RFC 3948	UDP Encapsulation of IPsec ESP Packets, January 2005	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 4120	The Kerberos Network Authentication Service (V5), July 2005	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 4448	Encapsulation Methods for Transport of Ethernet over MPLS Networks, April 2006	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 4577	OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs), June 2006	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN, September 2006	Mandated
Network/Environment	Application Delivery	IETF RFC 5246	The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 6241	Network Configuration Protocol (NETCONF), June 2011	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 6242	Using the NETCONF Protocol over Secure Shell (SSH) , June 2011	Mandated
Network/Environment	Application Delivery	IETF RFC 6353	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), July 2011	Mandated
Network/Environment	Application Delivery	IETF RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 2013	Mandated
Network/Environment	Software Defined Network (SDN)	IETF RFC 8040	RESTCONF Protocol, January 2017	Mandated
Network/Environment	Software Defined Network (SDN)	ISO/IEC 19941:2017	Information technology -- Cloud computing --	Mandated

			Interoperability and portability, 2017	
Network/Environment	Software Defined Network (SDN)	IETF RFC 4684	Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs), November 2006	Mandated
Network/Environment	Application Delivery	IETF RFC 8446	Transport Layer Security (TLS) 1.3, August 2018	Mandated
Application & Workload	Micro segmentation	NIST SP 800-204	Security Strategies for Microservices-based Application Systems	Active
Application & Workload	Micro segmentation	NIST SP 800-204A	Building Secure Microservices-based Applications Using Service-Mesh Architecture	Active
Data	Data Tagging	ICS 500-201	Tagging of Intelligence and Intelligence-Related Information	Active
Data	Data Loss Prevention	DODI 8170.01	DOD Instruction 8170.01, Online Information Management and Electronic Messaging	Active
Data	Data Rights Management	DODI 8230.07	DOD Instruction 8230.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense	Active
Data	Data Rights Management	DSP0004 v2.7.0	Common Information Model (CIM) Infrastructure, Version 2.7.0, 2012-04-22	Mandated
Data	Data Loss Prevention	IATA-STD-021-CDS-V1.0	Information Sharing Cross Domain Solution (CDS) Standard, 15 January 2017	Active
Data	Encryption	FIPS Pub 140-3	Security Requirements for Cryptographic Modules	Emerging

Visibility & Analytics	Artificial Intelligence, Machine Learning	Executive Order 13859	Maintaining American Leadership in Artificial Intelligence	Active
Visibility & Analytics	Security Information Event Management (SIEM)	NIST SP 1500-4r2	NIST Big Data Interoperability Framework: Volume 4, Security and Privacy Version 3	Active
Visibility & Analytics	Security Information and Event Management (SIEM), Discovery and Baselining	NIST SP 800-160 Volume I	Systems Security Engineering (SSE) Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, November 2016 (Including updates as of 03-21-2018)	Active
Visibility & Analytics	Security Information and Event Management (SIEM), Discovery and Baselining	NIST SP 800-160 Volume 2	Developing Cyber Resilient Systems: A Systems Security Engineering Approach November 2019	Active
Visibility & Analytics	Discovery and Baselining	NIST SP 800-18 Rev. 1	Guide for Developing Security Plans for Federal Information Systems	Active
Visibility & Analytics	Security Information and Event Management (SIEM)	NIST SP 800-60 Vol. 1 Rev. 1	Guide for Mapping Types of Information and Information Systems to Security Categories	Active
Visibility & Analytics	Security Information and Event Management (SIEM)	NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	Active
Visibility & Analytics	Discovery and Baselining	FIPS Pub 199	Standards for Security Categorization of Federal Information and Information Systems, February 2004	Mandated
Visibility & Analytics	Security Information and Event	NIST SP 800-115	Technical Guide to Information Security Testing and Assessment	Active

	Management (SIEM)			
Automation & Orchestration	Security, Orchestration, Automation and Response (SOAR)	IATA-STD-019-CCM-V1.0	Cyber Configuration Management Standard 15 January 2017	Active
Automation & Orchestration	API Standard	OGF GFD-P-R.221	Open Grid Forum (OGF) - Grid Final Document (GFD) - Open Cloud Computing Interface (OCCI) 221 - Core, September 19, 2016	Mandated

4 PATTERNS

4.1 Capability Dependencies (CV-4)

View Definition: The CV-4 describes the dependencies between planned capabilities. It also defines logical groupings of capabilities.

View Purpose/Intended Usage: The Zero Trust RA CV-4 Version 1.0 provides a means of analyzing the dependencies between capabilities. The groupings of capabilities are logical, and to guide enterprise management. In particular, the dependencies and groupings may suggest specific interactions between acquisition projects to achieve the overall capability. The intended use is to identify capability dependencies and capability management.

View Structure: The Zero Trust RA CV-4 Version 1.0 is structured as a graphical representation of the capability's dependencies and relationships.

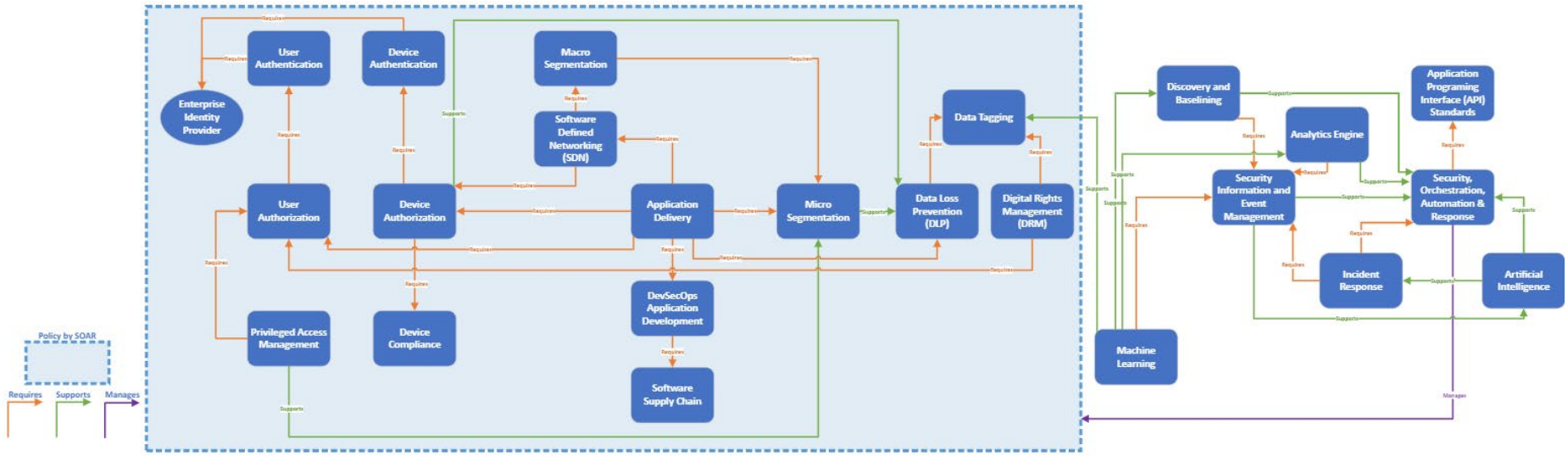

Figure 5: Capability Dependencies (CV-4)

4.2 Capabilities to Operational Activities Mapping (CV-6)

View Definition: The CV-6 describes the mapping between capabilities required and the activities that enable those capabilities.

View Purpose/Intended Usage: The Zero Trust RA CV-6 Version 1.0 provides a bridge between capability analyzed using CVs and operational activities analyzed using OVs. Specifically, it identifies how operational activities can be performed using various available capability elements. The capability to activity mappings may include both situations where activities fully satisfy the desired capability and those where the activity only partially meets the capability requirement.

View Structure: The table below is formatted in a way to show relationship between the Zero Trust pillars (column title - “Capabilities”), how the capability itself is defined (column title – “Definition”), as well as the activities the primary capability relates to. The hierarchy top level are the capabilities. The activities provided in the last column (column title – “CV-6 Operational Activities (required/optional)”) below are defined within this document in the vocabulary section. In order to fully understand the mapping between a capability and activity, the definitions of the below operational activities were thoroughly read and understood, then placed with the capability of best fit. The definitions in the table and the AV-2 are not Zero Trust-created content and therefore do not mesh perfectly with our defined capabilities.

Table 3: Capability to Operational Activities Model (CV-6)

Capabilities	Definition	CV-6 Operational Activities (required/optional)
User Authentication	The ability to verify the identity of a user, often as a prerequisite to allowing access to a system’s resources.	A1.1.2.9.2 Develop Identity Management and Authentication (IdM&A) Policy A2 Protect and Secure the IE A2.1 Enable Global Authentication and Access Control A2.1.1 Provide Identity Management and Authentication A2.1.1.1.1 Register Identity A2.1.1.1.2 Maintain Identity A2.1.1.3 Authenticate Entity A2.1.1.3.1 Provide Authentication Mechanisms A2.1.1.3.2 Validate Credential Authenticity A2.1.1.3.3 Verify Identity A2.1.2.1.1 Identify Standard Attributes A2.1.3 Provide Federation A2.1.5 Manage Digital Rules

User Authorization	The ability to grant or deny device access to data, assets, applications, or services after a prerequisite check.	A1.1.2.8 Develop Configuration Management Policy A1.1.2.9.3 Develop Access Control PolicyA2 Protect and Secure the IE A2.1 Enable Global Authentication and Access Control A2.1.1 Provide Identity Management and Authentication A2.1.1.2.1.1 Issue Credential A2.1.1.2.1.2 Maintain Credential A2.1.2 Provide Access Control A2.1.2.1 Provide Adaptive Access Framework A2.1.2.1.2 Enable Access Controls A2.1.2.2 Manage Access Process A2.1.3 Provide Federation A2.1.4 Monitor Authentication and Access Control A2.1.5 Manage Digital Rules A5.3.4 Assess Training Performance
Privileged Access Management	The ability to secure, control, and manage privileged access on critical assets and applications.	A1.1.2.8 Develop Configuration Management Policy A1.1.2.9.3 Develop Access Control PolicyA2 Protect and Secure the IE A2.1 Enable Global Authentication and Access Control A2.1.1 Provide Identity Management and Authentication A2.1.1.1.1 Register Identity A2.1.1.1.2 Maintain Identity A2.1.1.1.3 Expose Identity Information A2.1.1.2 Provide Credentialing Mechanisms A2.1.1.2.1.1 Issue Credential A2.1.1.3.3 Verify Identity A2.1.2 Provide Access Control A2.1.2.1 Provide Adaptive Access Framework A2.1.2.1.2 Enable Access Controls A2.1.2.2 Manage Access Process A2.1.2.2.1 Manage Trust Negotiation A2.1.2.2.2 Manage Access Privileges A2.1.4 Monitor Authentication and Access Control A2.1.5 Manage Digital Rules

		A2.3 Safeguard the IE A3.2.1.3.1 Provide Security Control Mechanisms for CI A3.2.1.3.1.1 Provide Privilege Controls for CI Resources A4.2.1.3.4 Facilitate Assured Access to IE Situational Awareness Information A4.2.1.3.4.1 Manage Access to IE Situational Awareness Information A4.2.4.3 Provide Critical Infrastructure Protection (CIP)
Device Authentication	The ability to verify the identity of a process or device, often as a prerequisite to allowing access to a system's resources.	A1.1.2.8 Develop Configuration Management Policy A1.1.2.9.3 Develop Access Control Policy A2 Protect and Secure the IE A2.1 Enable Global Authentication and Access Control A2.1.1 Provide Identity Management and Authentication A2.1.1.1.1 Register Identity A2.1.1.1.2 Maintain Identity A2.1.1.2 Provide Credentialing Mechanisms A2.1.1.3 Authenticate Entity A2.1.1.3.1 Provide Authentication Mechanisms A2.1.1.3.2 Validate Credential Authenticity A2.1.1.3.3 Verify Identity A2.1.2.1 Provide Adaptive Access Framework A2.1.2.1.1 Identify Standard Attributes A2.1.3 Provide Federation A2.1.5 Manage Digital Rules
Device Authorization	The ability to grant or deny user access to data, assets, applications, or services after a prerequisite check.	A1.1.2.8 Develop Configuration Management Policy A1.1.2.9.3 Develop Access Control PolicyA2 Protect and Secure the IE A2.1 Enable Global Authentication and Access Control A2.1.1 Provide Identity Management and Authentication A2.1.1.2.1.1 Issue Credential A2.1.1.2.1.2 Maintain Credential A2.1.2 Provide Access Control

		A2.1.2.1 Provide Adaptive Access Framework A2.1.2.1.2 Enable Access Controls A2.1.2.2 Manage Access Process A2.1.3 Provide Federation A2.1.4 Monitor Authentication and Access Control A2.1.5 Manage Digital Rules A4.2.1.3.4 Facilitate Assured Access to IE Situational Awareness Information A4.2.1.3.4.1 Manage Access to IE Situational Awareness Information
Device Compliance	The ability to validate associated policies on endpoints to include mobile devices, laptops, desktop PCs, servers, and hardware within data centers.	A1.1.2.8 Develop Configuration Management Policy A1.1.2.9.3 Develop Access Control Policy A2 Protect and Secure the IE A2.1.1 Provide Identity Management and Authentication A2.1.1.3.3 Verify Identity A2.1.2.1.1 Identify Standard Attributes A2.1.2.1.2 Enable Access Controls A2.1.4 Monitor Authentication and Access Control A2.1.5 Manage Digital Rules A2.3 Safeguard the IE A2.3.3 Provide IT Platform Protection A2.3.5 Manage Information Assurance & Vulnerability Assessment (IAVA) Compliance A2.6.1 Manage Computer Network Defense (CND) and Cybersecurity Services A3.2.1.3 Provide Computing Infrastructure Controls A3.2.1.3.1 Provide Security Control Mechanisms for CI A3.2.1.3.1.2 Provide Hardware and Operating System Security Configuration Controls A4.2.3.6 Perform Patch Management A4.2.4.1 Provide Security Monitoring, Vulnerability Analysis, and Threat Identification
Software-Defined	The ability for software to provision and manage network configurations	A1.1.2.1.1 Administer NetOps Policy A1.1.3.4 Develop Computing Infrastructure Standards

Networking (SDN)	on programmable infrastructure such as routers, switches, and firewalls.	A2.1.3 Provide Federation A2.1.2.1.2 Enable Access Controls A2.1.2.2.2 Manage Access Privileges A2.3.2 Manage Network Resources to Defend IE A2.3.3 Provide IT Platform Protection A2.6.2 Provide Policy-Based Management of Cybersecurity Components of IE A3.2.1 Provide Computing Infrastructure A3.2.1.1.5 Test and Accredit Computing Infrastructure Solution A3.2.1.2 Establish Computing Infrastructure Environment A3.2.1.2.1 Provide Self-Managing Computing Infrastructure Operations A3.2.1.2.1.2 Enable Automated NetOps Information Reporting in Computing Infrastructure A3.2.1.2.6 Provide Grid Computing Environment A3.2.1.2.9.3 Provide Trusted Computing A3.2.1.3 Provide Computing Infrastructure Controls A3.2.1.3.1 Provide Security Control Mechanisms for CI A3.2.1.3.2 Provide Optimization / Performance Controls A3.3 Evolve IE A3.3.1.1 Enhance Computing Infrastructure with New Technology A4.2.3.4 Provide Configuration Control A4.2.4 Conduct Network Defense A4.2.5.1 Prioritize Information Resources
Macro Segmentation	The ability to segment traffic on the network through the use of broad categories. These categories can be defined by items such as location, network type, branch, organization and segmentation are typically achieved	A2 Protect and Secure the IE A2.3 Safeguard the IE A2.1.3 Provide Federation A2.2.4 Implement End-to-End Security Accreditation A2.3 Safeguard the IE A2.3.1 Protect Network and Enclave Boundaries A2.3.1.1 Provide Technical Protection Standards A2.3.2 Manage Network Resources to Defend IE A2.3.4.2.1 Manage Security Strategy for Data-in-Transit over IPv6

	through the application of additional hardware, SDN or VLANs.	A2.3.4.2.2 Protect Data-in-Transit Between NIPRNet and Internet A2.3.4.2.5 Protect Data-in-Transit during Coalition Information Sharing A3.2.1.3 Provide Computing Infrastructure Controls A4.2.4 Conduct Network Defense
Software-Defined Compute (SDC)	The ability for software to provision and manage compute configurations on programmable infrastructure such as physical and virtual servers.	A3.2.1.1.5 Test and Accredit Computing Infrastructure Solution A3.2.1.1.2 Install Computing Infrastructure Solution A3.2.1.2.1.2 Enable Automated NetOps Information Reporting in Computing Infrastructure A3.2.1.2.2 Provide Hardware Environment A3.2.1.2.5 Provide High Productivity Computing Environment A3.2.1.2.6 Provide Grid Computing Environment A3.2.1.2.7 Provide Computing Infrastructure Service A3.2.1.2.7.1 Provide Shared Computing A3.2.1.2.9.3 Provide Trusted Computing A3.2.1.3 Provide Computing Infrastructure Controls A3.2.1.3.1 Provide Security Control Mechanisms for CI A3.2.1.3.2 Provide Optimization / Performance Controls A3.3 Evolve IE A3.3.1.1 Enhance Computing Infrastructure with New Technology A3.3.1.1.3 Assess Changes to Computing Infrastructure A4.2.3.1.2 Allocate Computing Infrastructure Resources A4.2.3.1.2.1 Allocate Computing Resources A4.2.3.1.2.1.1 Allocate Shared Computing Resources A4.2.3.1.2.1.2 Allocate Processing Resources

		A4.2.3.1.2.1.3 Allocate Operations Across Hardware Resources A4.2.5.1 Prioritize Information Resources
DevSecOps (DSO)	The ability to develop software in concert with the operations and security teams to maximize the protection, quality integrity of applications while shortening the development life cycle.	A1.1.2.8 Develop Configuration Management Policy A1.1.3 Establish IE Standards A1.1.3.2 Develop Cybersecurity Standards A1.1.3.3 Develop Communications Standards A1.1.3.4 Develop Computing Infrastructure Standards A1.1.3.5 Develop Data/Service Standards A1.1.3.6 Develop Metadata Standards A1.1.3.7 Develop Procedural/working Pipeline A3.1.1.3.1 Provide Service Oriented Architecture Foundation (SOAF) Services A4.2.3.4 Provide Configuration Control A4.2.3.6 Perform Patch Management
Software Supply Chain	The ability to validate the security on a binary, library, or source code used to build an application.	A2.8 Manage Mission Assurance A2.8.1 Evaluate Software Assurance A2.8.2 Evaluate Hardware Assurance A2.8.3 Evaluate System Assurance A2.8.4 Evaluate Supplier Assurance A3.1.2 Provide End User Services and Applications A3.2.1.2.4 Provide System Software Environment A4.2.3.4 Provide Configuration Control
Application Delivery	The ability to control resource authorization on applications and services typically implemented via an identity-aware proxy.	A2.3 Safeguard the IE A2.1.2.1.2 Enable Access Controls A2.3.2 Manage Network Resources to Defend IE A2.3.4.2.1 Manage Security Strategy for Data-in-Transit over IPv6 A3.1 Provide Information and Services from the Edge A3.1.1.2 Enable Data and Service Separation from Applications A3.1.2 Provide End User Services and Applications A3.1.2.1 Provide Mission Oriented Applications

		A3.1.2.2 Publish Mission-Oriented Services A4.2.4 Conduct Network Defense
Micro Segmentation	The ability to divide or isolate logical segments on a network at the individual workload or process level. Security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.	A2 Protect and Secure the IE A2.1.2 Provide Access Control A2.3 Safeguard the IE A2.3.1 Protect Network and Enclave Boundaries A2.3.1.1 Provide Technical Protection Standards A2.3.2 Manage Network Resources to Defend IE A2.3.4.2.1 Manage Security Strategy for Data-in-Transit over IPv6 A2.3.4.2.3 Protect Data-in-Transit Across System High Boundaries A2.3.4.2.4 Integrate Data-in-Transit Protection Across Architecture Components A2.3.4.2.5 Protect Data-in-Transit during Coalition Information Sharing A4.2.4 Conduct Network Defense
Software-Defined Storage (SDS)	The ability for software to provision and manage storage configurations on programmable infrastructure such as physical and virtual network attached storage, storage area networks, and hyperconverged platforms.	A1.1.3.5 Develop Data/Service Standards A2.3.4.1 Standardize Data-at-Rest Protection A3.2.1.2.1 Provide Self-Managing Computing Infrastructure Operations A3.2.1.2.2 Provide Hardware Environment A3.2.1.2.3 Provide Storage Environment A3.2.1.2.7 Provide Computing Infrastructure Service A3.2.1.2.7.2 Provide Computing Infrastructure Storage Services A4.2.3.1.2.2 Allocate Storage Resources A4.2.5.1 Prioritize Information Resources
Data Tagging	The ability to assign metadata on a file for use in policy to allow or	A1.1 Provide Enterprise-wide Guidance A1.1.3 Establish IE Standards A1.1.3.6 Develop Metadata Standards

	deny access. Access control can be implemented in a granular fashion based on the specific attributes and tags associated to data, users, and devices.	A2.3.4 This activity defines standards and enforces protection properties for protecting data objects. A2.7 Tag Data Objects with cybersecurity Metadata A2.7.1 Bind Cybersecurity Metadata Tags to Data Objects A2.7.2 Develop Cybersecurity Metadata Tagging Standards
Data Loss Prevention (DLP)	The ability to detect and prevent potential data breaches and ex-filtration transmissions. This is accomplished through monitoring, analysis and control of data while in use, in motion, and at rest.	A1 Manage and Oversee IE A1.1.2.4 Develop Quality of Protection (QoP) Policy A2 Protect and Secure the IE A2.3 Safeguard the IE A2.3.4 Enable Data Protection A2.3.4.1 Standardize Data-at-Rest Protection A2.3.4.2 Standardize Data-in-Transit Protection A2.3.4.2.2 Protect Data-in-Transit Between NIPRNet and Internet A2.3.4.2.3 Protect Data-in-Transit Across System High Boundaries A2.3.4.2.4 Integrate Data-in-Transit Protection Across Architecture Components A2.3.4.2.5 Protect Data-in-Transit during Coalition Information Sharing A3.1 Provide Information and Services from the Edge A3.1.3.1.2 Manage Integrity A3.1.3.1.3 Manage Authenticity A3.2.1.2.9.1 Enable Cybersecurity for Shared Storage and Media Functions A3.2.1.3 Provide Computing Infrastructure Controls A3.2.1.3.1 Provide Security Control Mechanisms for CI
Data Rights Management (DRM)	The ability to align access controls to encryption on a file that prevents unauthorized users or devices from	A2 Protect and Secure the IE A2.1.2 Provide Access Control A2.1.2.1.2 Enable Access Controls A2.3 Safeguard the IE A2.3.4 Enable Data Protection A2.3.4.1 Standardize Data-at-Rest Protection

	modifying, accessing or distributing, data.	A2.3.4.2 Standardize Data-in-Transit Protection A2.3.4.2.2 Protect Data-in-Transit Between NIPRNet and Internet A2.3.4.2.4 Integrate Data-in-Transit Protection Across Architecture Components A3.1.3.1.2 Manage Integrity A3.1.3.1.3 Manage Authenticity A3.2.1.3 Provide Computing Infrastructure Controls
Discovery and Baselining	The ability to identify characteristics of networks, environments, applications, devices to determine normal operating parameters. This capability allows for the establishment of a baseline for use in policy evaluations.	A2.1.4.1 Define Threat Level A2.1.4.2 Perform Audit A2.1.4.3 Identify Threats
Security Information and Event Management (SIEM)	The ability to collect and analyze security events on all aspects of the network, environment, device and application to support threat detection, compliance, and incident management.	A1.1.1.3 Enable IE Audit A1.1.2.1.2 Monitor NetOps Policy A2.1.2 Provide Access Control A2.1.4 Monitor Authentication and Access Control A2.1.4.1 Define Threat Level A2.1.4.3 Monitor Threat Landscape A2.3 Safeguard the IE A2.3.3 Provide IT Platform Protection A3.2.1.2.1.2 Enable Automated NetOps Information Reporting in Computing Infrastructure A3.2.1.2.7.5 Provide Operation Oversight Services A3.2.1.2.7.6 Assess Computing Infrastructure Requirements and Performance A3.2.1.5.1.2 Register Computing Infrastructure Metadata A4.2 Exercise Operational Control of IE Through NetOps A4.2.1 Manage IE Situational Awareness A4.2.1.1 Produce IE Situational Awareness

		Information A4.2.1.1.1 Process IE Situational Awareness Data A4.2.1.1.2 Create Tailorable Visualizations A4.2.1.3 Report IE Situational Awareness A4.2.1.3.1 Publish IE Situational Awareness Information A4.2.1.3.3 Advertise IE Situational Awareness Information A4.2.1.2 Collect Situational Awareness Data A4.2.4.1 Provide Security Monitoring, Vulnerability Analysis, and Threat Identification A4.2.4.2 Perform Threat / Incident Management
Machine Learning	The ability to study data on security events regarding all aspects of the network, environment, device and application to improve the security, performance, and execution of future policy and risk scoring decisions.	A3.2.1.2.1 Provide Self-Managing Computing Infrastructure Operations A3.2.1.2.1.1 Automate Computing Infrastructure Operations A3.2.1.2.1.3 Enable Dynamic, Virtual Processing in Computing Infrastructure A3.2.1.2.1.4 Provide Autonomous CI Environment A3.2.1.5.1 Provide Computing Infrastructure Metadata
Application Programming Interface (API) Standard	The ability to provide a standard method of communication between disparate technologies to allow for automated activities. These standards are critical to the automation of security policy and executing dynamic access controls.	A1 Manage and Oversee IE A1.1 Provide Enterprise-wide Guidance A1.1.3 Establish IE Standards A1.1.3.1 Develop NetOps Standards A1.1.3.2 Develop Cybersecurity Standards A1.1.3.3 Develop Communications Standards A1.1.3.4 Develop Computing Infrastructure Standards A1.1.3.5 Develop Data/Service Standards A1.1.3.6 Develop Metadata Standards
Incident Response	The ability to respond to a security event or issue on the environment, device, application or data. Automation of incident response is	A1.1.2 Develop IE Functional Policy A1.1.2.1 Develop NetOps Policy A2 Protect and Secure the IE A2.1.2.1 Provide Adaptive Access Framework A2.1.4.1 Define Threat Level A2.1.4.3 Identify Threats

	enabled by workflows integrated into SOAR, SIEM, and infrastructure.	A2.3.3 Provide IT Platform Protection A2.6.1 Manage Computer Network Defense (CND) and Cybersecurity Services A2.8 Manage Mission Assurance A2.8.1 Evaluate Software Assurance A2.8.2 Evaluate Hardware Assurance A2.8.3 Evaluate System Assurance A2.8.4 Evaluate Supplier Assurance A4.2.2 Respond to IE Situation A4.2.4 Conduct Network Defense A4.2.4.2 Perform Threat/ Incident Management
Security Orchestration, Automation & Response (SOAR)	The ability to automate detection, response and remediation of security incidents. The SOAR capability will integrate with the SIEM for analysis of security events and execute automated workflows in response to threats.	A1.1.2.1.1 Administer NetOps Policy A1.1.2.1.3 Enforce NetOps Policy A1.1.2.8 Develop Configuration Management Policy A2 Protect and Secure the IE A2.1.2 Provide Access Control A2.1.2.1 Provide Adaptive Access Framework A2.1.2.2.2 Manage Access Privileges A2.1.4.1 Define Threat Level A2.1.5 Manage Digital Rules A2.3 Safeguard the IE A2.3.3 Provide IT Platform Protection A2.3.3.1 Assess Vulnerability of Potential IT Platforms A2.3.5 Manage Information Assurance & Vulnerability Assessment (IAVA) Compliance A2.6 Provide Assured Control of IE A2.6.1 Manage Computer Network Defense (CND) and Cybersecurity Services A2.6.2 Provide Policy-Based Management of Cybersecurity Components of IE A2.6.2.1 Manage Technology and Infrastructure for Cybersecurity Policy Management A3.2.1.2.1 Provide Self-Managing Computing Infrastructure Operations A3.2.1.2.1.1 Automate Computing Infrastructure Operations A3.2.1.2.1.4 Provide Autonomous CI Environment A3.2.1.2.9.2 Enable Secure Interoperability

		A3.2.1.3 Provide Infrastructure Controls A3.2.1.3.1 Provide Security Control Mechanisms for CI A3.2.1.3.1.1 Provide Privilege Controls for CI Resources A3.2.1.3.1.2 Provide Hardware and Operating System Security Configuration Controls A4 Control and Operate the IE A4.2 Exercise Operational Control of IE Through NetOps A4.2.4 Conduct Network Defense A4.2.4.1 Provide Security Monitoring, Vulnerability Analysis, and Threat Identification A4.2.3.1.2 Allocate Computing Infrastructure Resources A4.2.3.1.2.1 Allocate Computing Resources A4.2.3.1.2.1.1 Allocate Shared Computing Resources A4.2.3.1.2.1.2 Allocate Processing Resources A4.2.3.1.2.1.3 Allocate Operations Across Hardware Resources A4.2.3.1.2.2 Allocate Storage Resources A4.2.3.1.2.3 Allocate Network Interfaces A4.2.3.4 Provide Configuration Control A4.2.4.2 Perform Threat / Incident Management
Artificial Intelligence	The ability of machines to perform tasks that normally require human intelligence – for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or acting – whether digitally or as the smart software	A3.2.1.2.1 Provide Self-Managing Computing Infrastructure Operations

	behind autonomous physical systems.[10]	
Analytics	The ability to provide analysis of data and statistics to create individualized user and device profiles. Analytics will be used for the discovery, interpretation, and communication patterns to convert analyzed data into usable data patterns towards effective decision making and confidence scoring.	A1.1.3.6 Develop Metadata Standards A2.1.4 Monitor Authentication and Access Control A2.1.4.1 Define Threat Level A2.1.4.2 Perform Audit A2.1.4.3 Identify Threats A2.1.5 Manage Digital Rules A2.3 Safeguard the IE A2.3.3 Provide IT Platform Protection A2.3.3.1 Assess Vulnerability of Potential IT Platforms A2.7 Tag Data Objects with Cybersecurity Metadata A2.7.1 Bind Cybersecurity Metadata Tags to Data Objects A2.7.2 Develop Cybersecurity Metadata Tagging Standards A3.1.3.1 Manage Satisfaction of Information and Services Requirements A4.2.3.7 Manage IE Performance A4.2.3.7.1 Develop and Apply IE Performance Metrics A4.2.3.7.2 Assess Performance of IE Resources A4.2.3.8 Measure IE Effectiveness A4.2.3.8.1 Measure Operational Effectiveness of NetOps A4.2.3.8.2 Measure Strategic Effectiveness of IE

10 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY, 2018.

4.3 Capabilities to Services Mapping (CV-7)

View Definition: The CV-7 describes the mapping between the capabilities required and the services that enable those capabilities. It is important to ensure that the services match the required capability.

View Purpose/Intended Usage: The Zero Trust CV-7 identifies how services can be performed using various available capability elements. The capability to service mappings may include both situations where a service fully satisfies the desired capability and those where the service only partially meets the capability requirement.

View Structure: The Zero Trust CV-7 Version 1.0 is structured as a table. CV-7 Services definitions can be found in Appendix H of this document.

Zero Trust Narrative/Summary: The tables below are formatted in a way to show relationship between the Zero Trust pillars (column title - “Capabilities”), how the capability itself is defined (column title – “Definition”), as well as the services the primary capability relates to. The hierarchy top level are the capabilities. The services provided in the last column (column title – “CV-7 Services (required/optional)”) below are defined within this document in Appendix F. In order to fully understand the mapping between a capability and service, the definitions of the below operational activities were thoroughly read and understood, then placed with the capability of best fit. The definitions in the table and the AV-2 are not Zero Trust-created content and therefore do not mesh perfectly with our defined capabilities.

Table 4: Capability to Services Mapping (CV-7)

Capabilities	Definition	CV-7 Services (required/optional)
User Authentication	The ability to verify the identity of a user, often as a prerequisite to allowing access to a system’s resources.	S1.2.1 Access Control Services S1.2.2.1 Identity Management Services S1.2.2.2 Attribute Management Services S1.2.2.3 Credential Management Services S1.2.2.4 Authentication Management Services S1.3.8 Audit Services S3.2.1 Digital Access Policy Management Services
User Authorization	The ability to grant or deny user access to data, assets, applications, or services after a prerequisite check.	S1.2.1 Access Control Services S1.2.2.1 Identity Management Services S1.2.2.3 Credential Management Services S1.2.2.4 Authentication Management Services S1.2.3 Directory Management Services

		S1.3.8 Audit Services S3.2.1 Digital Access Policy Management Services S1.2.2.2 Attribute Management Services
Privileged Access Management	The ability to secure, control, and manage privileged access on critical assets and applications.	S1.2.1 Access Control Services S1.2.2.1 Identity Management Services S1.2.2.2 Attribute Management Services S1.2.2.3 Credential Management Services S1.2.2.4 Authentication Management Services S1.3.8 Audit Services S3.2.1 Digital Access Policy Management Services
Device Authentication	The ability to verify the identity of a process or device, often as a prerequisite to allowing access to a system's resources.	S1.2.1 Access Control Services S1.2.2.1 Identity Management Services S1.2.2.3 Credential Management Services S1.2.2.4 Authentication Management Services S1.2.1 Access Control Services S1.3.8 Audit Services S1.2.3 Directory Management Services S3.2.1 Digital Access Policy Management Services S1.2.2.2 Attribute Management Services
Device Authorization	The ability to grant or deny user access to data, assets, applications, or services after a prerequisite check.	S1.1.7 End User Device Services S1.2.1 Access Control Services S1.2.2.1 Identity Management Services S1.2.2.3 Credential Management Services S1.2.2.4 Authentication Management Services S1.2.1 Access Control Services S1.3.8 Audit Services S3.2.1 Digital Access Policy Management Services S1.2.2.2 Attribute Management Services
Device Compliance	The ability to validate associated policies on endpoints to include mobile devices, laptops, desktop	S1.3.8 Audit Services S2.2.2 Information Assurance Management Service S3.3 Monitoring and Compliance Services

	PCs, servers, and hardware within data centers.	
Software Defined Networking (SDN)	The ability for software to provision and manage network configurations on programmable infrastructure such as routers, switches, and firewalls.	S1.1 Connect Services S1.1.2 IP Based Networking Services S1.1.5 Wired Communication Services S1.1.6 Computing and Data Storage Services S1.3.2.2 Cross Domain Services S1.3.5 Custom Application Services S1.3.6 Cloud Computing Services S1.3.6.1 Software as a Service S1.3.6.2 Infrastructure as a Service S1.3.6.3 Platform as a Service S1.3.8 Audit Services
Macro Segmentation	The ability to segment traffic on the network using broad categories. These categories can be defined by items such as location, network type, branch, organization and segmentation are typically achieved through the application of additional hardware, SDN or VLANs.	S1.1.2.4 Ad Hoc Network Services S1.1.6 Computing and Data Storage Services S1.3.6.2 Infrastructure as a Service
Software Defined Compute (SDC)	The ability for software to provision and manage compute configurations on programmable infrastructure such as physical and virtual servers.	S1.1.6 Computing and Data Storage Service S1.1.6.1 Storage on Demand Services S1.1.6.2 Computing on Demand Services
DevSecOps	Development Security and Operations (DevSecOps) is a set of software development practices that combines software development (Dev), security (Sec), and information technology operations (Ops) to secure the outcome and shorten the development lifecycle. Software features,	S2.1.1 Change Management Services S2.1.2 Virtual Test Platform Services S2.1.3 Common Development Platform Services S2.2 Defend Services S3.3 Monitoring and Compliance Services

	patches, and fixes occur more frequently and in an automated fashion. Security is applied at all phases of the software lifecycle.	
Software Supply Chain	The ability to validate the security on a binary, library, or source code used to build an application.	S2.1.1 Change Management Services S2.1.2 Virtual Test Platform Services S2.1.3 Common Development Platform Services S2.2 Defend Services
Application Delivery	The ability to control resource authorization on applications and services typically implemented via an identity-aware proxy.	S1.2.1 Access Control Services S1.3.1.2 Content Delivery Service S1.3.2.2 Cross Domain Services S1.3.5 Custom Application Services S2.1 Operate Services S2.2 Defend Services
Micro Segmentation	The ability to divide or isolate logical segments on a network at the individual workload or process level. Security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.	S1.1.2.4 Ad Hoc Network Services S1.1.6 Computing and Data Storage Services S1.3.6.2 Infrastructure as a Service
Software Defined Storage (SDS)	Data storage is the collective methods and technologies that capture and retain digital information on electromagnetic, optical, or silicon-based storage media.	S1.1.6.1 Storage on Demand Services S2.2.1 Security Metadata Management Services
Data Tagging	The ability to assign metadata on a file for use in policy to allow or deny access. Access control can be implemented in a granular fashion based on the specific attributes and	S1.3.1.1 Content Discovery Services S2.2.1 Security Metadata Management Services

	tags associated to data, users and devices.	
Data Loss Prevention (DLP)	The ability to detect potential data breaches and ex-filtration transmissions. This is accomplished through monitoring, analysis and control of data while in use, in motion, and at rest.	S1.3.2.1 Information Sharing Services S1.3.2.2 Cross Domain Services S3.3 Monitoring and Compliance Services S2 Operate and Defend Services S2.2 Defend Services S2.2.3 Cryptography Management Services
Data Rights Management (DRM)	The ability to align access controls to prevent unauthorized users or devices from modifying, accessing, or distributing data.	S1.3.2.1 Information Sharing Services S1.3.2.2 Cross Domain Services S3.3 Monitoring and Compliance Services S2 Operate and Defend Services S2.2 Defend Services S2.2.3 Cryptography Management Service S3.2.1 Digital Access Policy Management Services
Discovery and Baselining	The ability to identify characteristics of networks, environments, applications, and devices to determine normal operating parameters. This capability allows for the establishment of a baseline for use in policy evaluations, defined prior to suggesting any architectural changes	S2.1.1 Change Management Services S3.2 Standards and Policy Services S3.3 Monitoring and Compliance Services
Security Information and Event Management (SIEM)	The ability to collect and analyze security events on all aspects of the network, environment, device, and application to support threat detection, compliance, and incident management.	S1.3.8 Audit Services S2.1 Operate Services S2.2 Defend Services S3.3 Monitoring and Compliance Services
Machine Learning	The ability to study data on security events regarding all aspects of the network, environment, device, and	S3.2 Standards and Policy Services

	application to improve the security, performance, and execution of future policy and risk scoring decisions.	
Application Programming Interface (API) Standard	The ability to provide a standard method of communication between disparate technologies to allow for automated activities. These standards are critical to the automation of security policy and executing dynamic access controls.	S2.1.3 Common Development Platform Services
Incident Response	The ability to respond to a security event or issue on the environment, device, application, or data. Automation of incident response is enabled by workflows integrated into SOAR, SIEM, and infrastructure.	S2.1 Operate Services S2.2 Defend Services S2.2.3 Cryptography Management Services
Security Orchestration, Automation & Response (SOAR)	The ability to automate detection, response, and remediation of security incidents. The SOAR capability will integrate with the SIEM for analysis of security events and execute automated workflows in response to threats.	S3 Govern Services S2 Operate and Defend Services S2.2 Defend Services S2.1.1 Change Management Services S2.2.2 Information Assurance Management Services S3.2.1 Digital Access Policy Management Services
Artificial Intelligence	The ability of machines to perform tasks that normally require human intelligence – for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or acting – whether digitally or as the	S1.3.7 Language Translation Services S3 Govern Services S3.2 Standards and Policy Services S3.2.1 Digital Access Policy Management Services

	smart software behind autonomous physical systems.[11]	
Analytics	The ability to provide analysis of data and statistics to create individualized user and device profiles. Analytics will be used for the discovery, interpretation, and communication patterns to convert analyzed data into usable data patterns towards effective decision making and confidence scoring.	S1.2.2.2 Attribute Management Services S1.3.8 Audit Services S3.1 Processes and Models Services S2.2.1 Security Metadata Management Services S2.2.2 Information Assurance Management Services

11 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY, 2018.

4.4 Operational Resource Flow Description (OV-2)

View Definition: A DODAF Operational Resource Flow (OV-2) applies the context of the operational Zero Trust Architecture capabilities to a community of anticipated users.

View Purpose/Intended Usage: The Zero Trust RA OV-2 Version 1.0 is to define capability requirements within an operational context.

View Structure: The Zero Trust RA OV-2 Version 1.0 is structured as a graphic. Many of the key capabilities have already been covered in the OV-1 narrative and overview documentation.

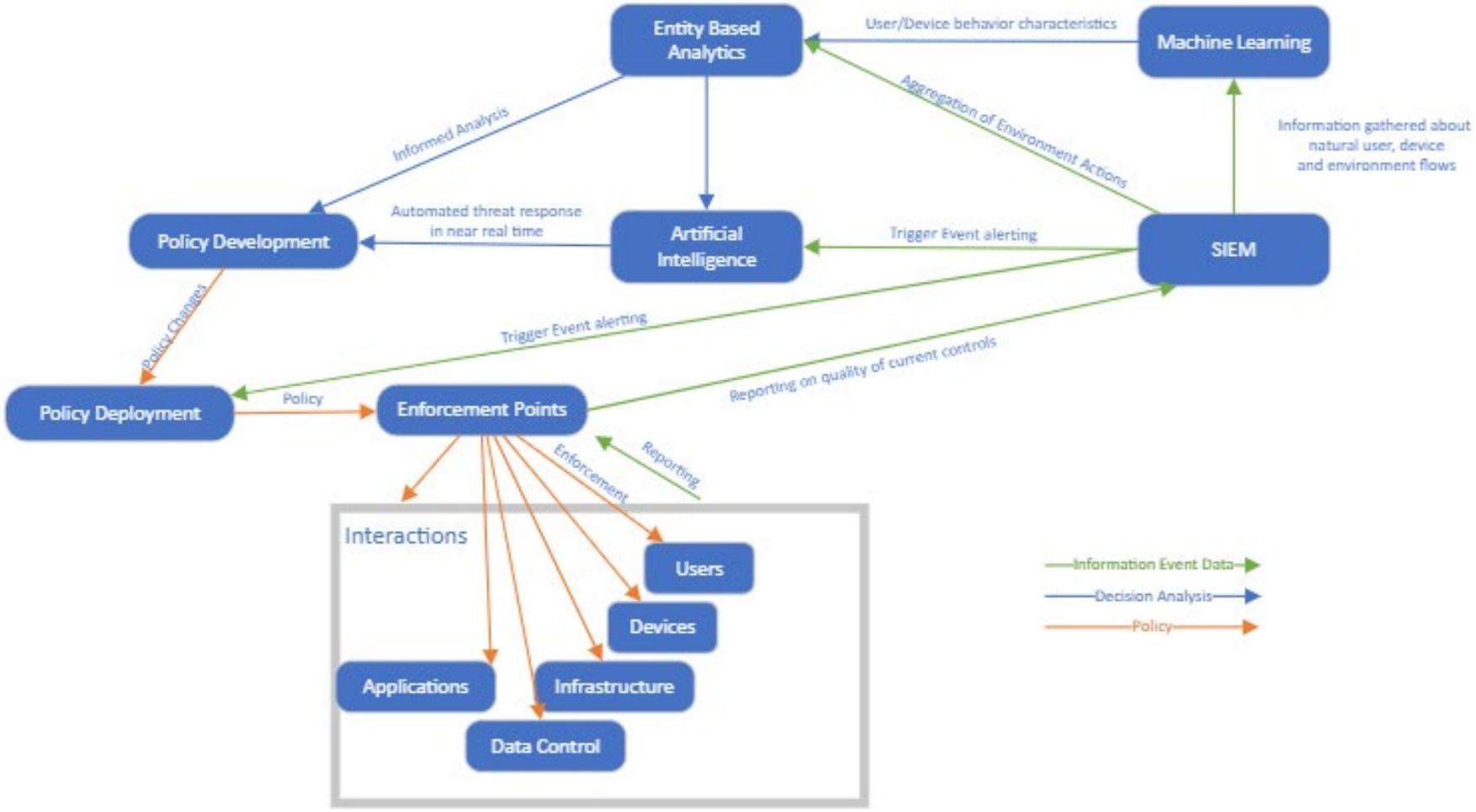

Figure 6: Operational Resource Flow Description – Policy (OV-2)

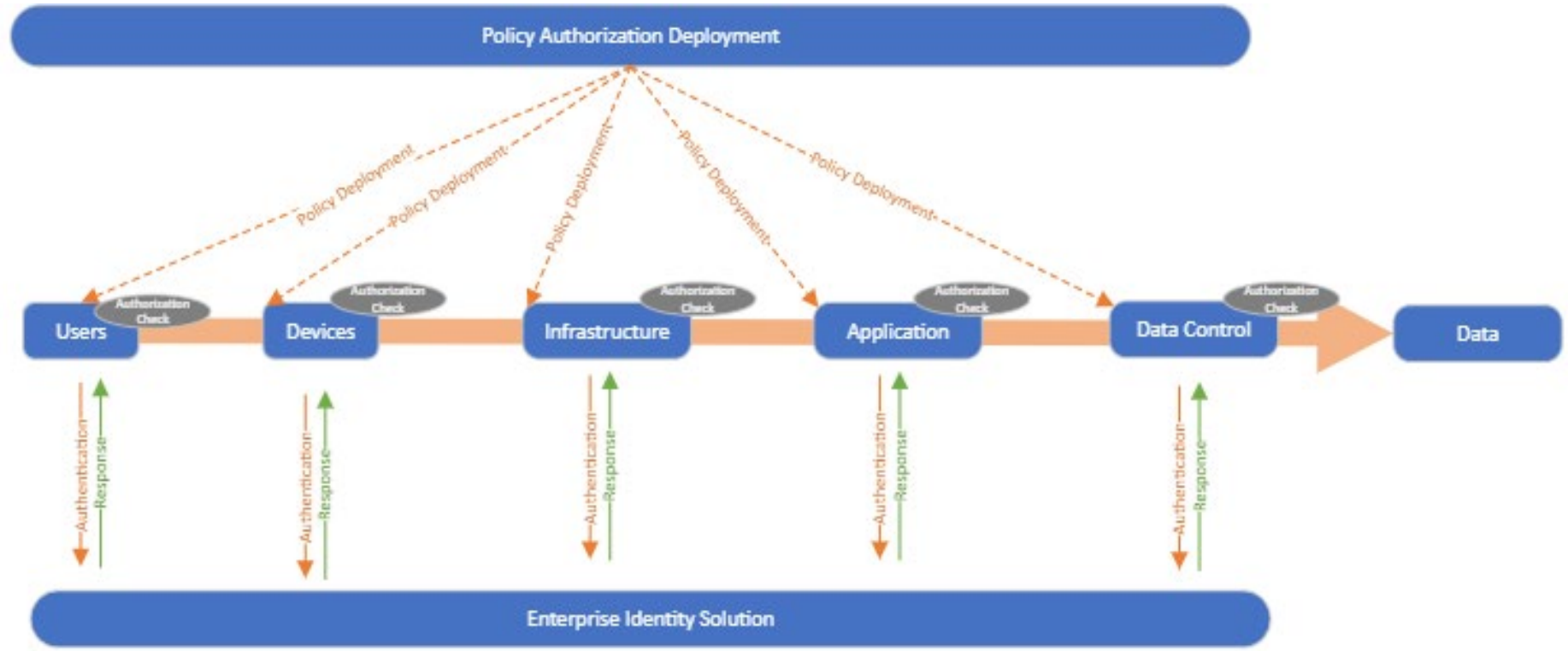

Figure 7: Operational Resource Flow Description – Authentication (OV-2)

4.5 Operational Activity Model (OV-5b)

View Definition: A DODAF Operational Activity Model (OV-5b) describes the operations that are normally conducted in the course of achieving a mission or goal.

View Purpose/Intended Usage: The Zero Trust OV-5b Version 1.0 is used to describe Zero Trust operational activities and workflows, requirements, task analysis, operational planning, and provides an analysis of information flows.

View Structure: The Zero Trust OV-5b is structured as multiple diagrams constructed by secured encrypted resource flows. Diagrams have been broken out based on example scenario capabilities within the Zero Trust pillars. As Zero Trust encompasses every facet of an organizations network and infrastructure, these diagrams are not exhaustive of every scenario or variation. Additionally, not every capability is shown for each scenario or required for each implementation. Below each diagram is a breakdown of potential operational activities.

View Narrative: The Zero Trust OV-5b has an overarching Logging, Analytics and Automation section. This section is shown on multiple diagrams and requires some explanation. This section ingests security and the relevant data required to derive policy development decisions. These decisions are then deployed to enforcement points or administration nodes. This process can involve analysis of an entity's actions and how it might compare to an established baseline. Abnormal behavior can be identified and evaluated. Policy changes can then be targeted. The exact deployed policy will be dependent on the technology in use. A user may have all the right attributes and roles, but analytics may flag a user as suspect due to activity that user has been preforming over time. Derived policy may add a user to a role or specific rule permission that will restrict the user's network, application or data access.

4.5.1 Authentication Request Simplified

- CAC inserted into reader and Cert provided goes to the identity agent for validation or another multifactor authentication.
- Identity Agent authenticates to Enterprise IDP to verify identity validity.
- The certificate is then checked with OCSP for validity.
- If the OCSP and Enterprise IDP checks are good, the user can proceed to login.
- If the OCSP check fails, then the user is denied access
- If the Enterprise IDP checks fail, then the user is denied access, highly restricted in their access, or sent to a honey pot
- All actions are logged to the SIEM, analyzed through the Analytics Engine, and deployed via the SOAR to provide real time policy access decisions.

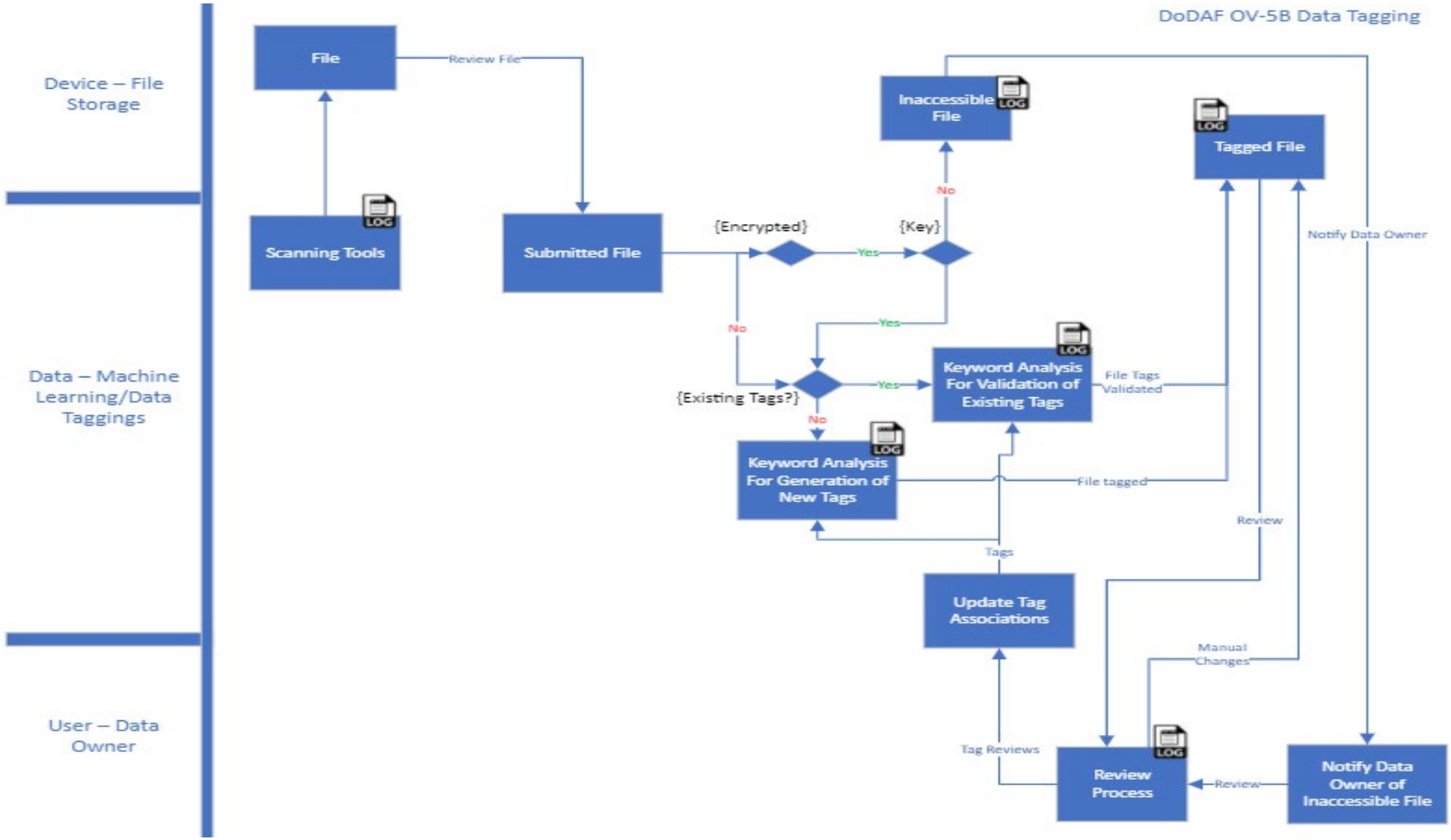

Figure 8: Operational Activity Model – Authentication Request (OV-5b)

4.5.2 Device Compliance

- Device Compliance Check is initiated with the local security agent gathering the device's current configuration.
- The compliance agent sends the device's current configuration to the Patch Environment where it is checked against current acceptable Baseline Configurations.
- If any of the checks return anything different than the acceptable baseline configuration, it is immediately remedied and then checked again.
- If it is unable to be remedied, the Policy Enforcement Point has the ability to allow it on the network or remove it from the network based on policy.
- After all checks are completed and the baseline configuration is in an acceptable state, the policy enforcement point can allow or remove the device based on policy.
- All actions are logged to the SIEM, analyzed through the Analytics Engine, and deployed via the SOAR to provide real time policy access decisions.

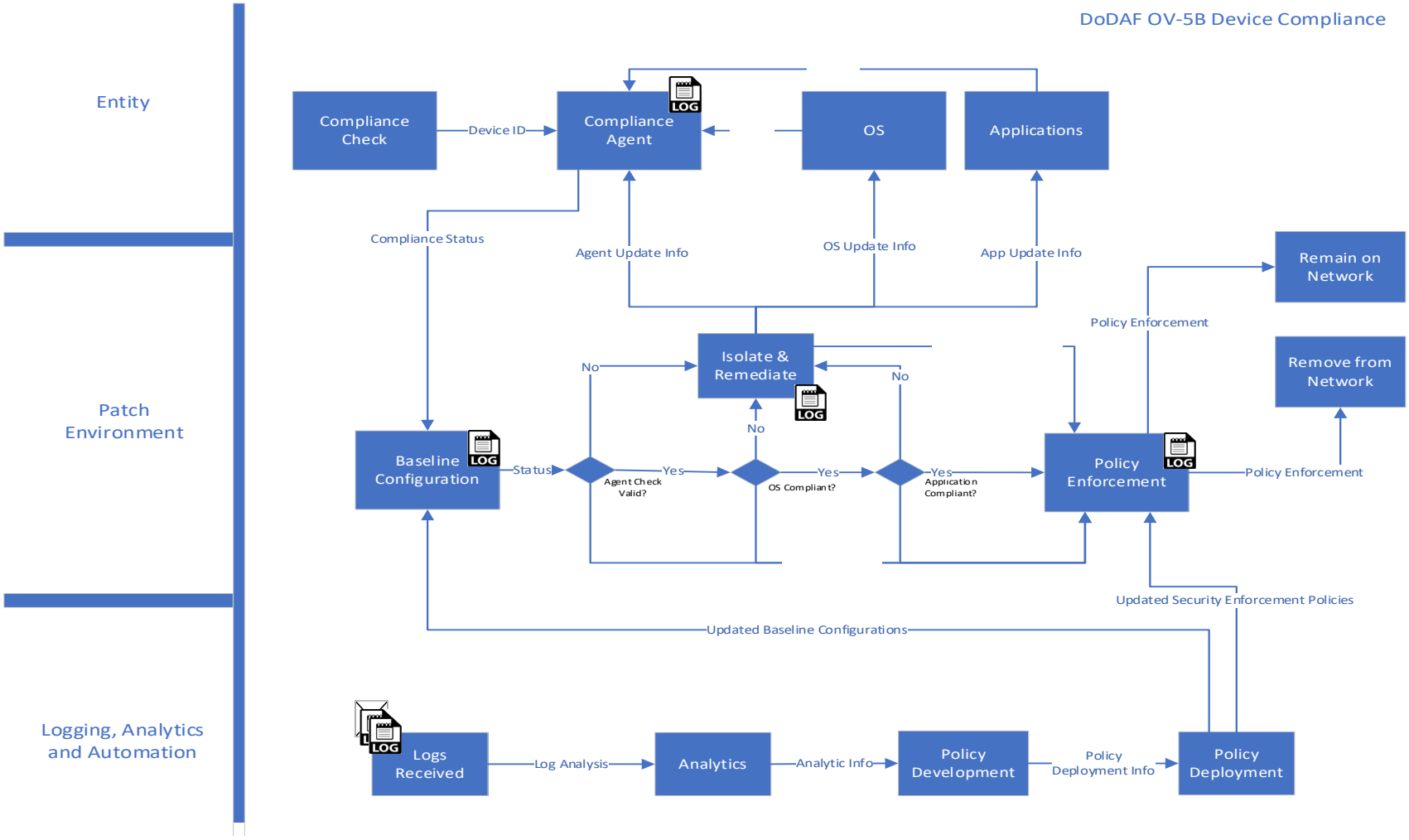

Figure 9: Operational Activity Model – Device Compliance (OV-5b)

4.5.3 User Analytics

- Historical User Behavioral Data and Current Users Actions are sent to Analytics Engine to be analyzed.
- User's historical and current actions/behaviors are compared against global baselines or unusual activity indicators that houses all acceptable trends. These baselines and unusual activity indicators can be derived from internal analytics metrics or security vendor feeds.
- The analysis is then given a Score based on the confidence it has on the user's behavior.
- The Confidence Score is then attached to the user as they traverse the network and continuous monitoring is happening in the background.
- Continuous monitoring and continuous analysis are happening in the background.
- As the users traverses the network and works, their access is based on the score they have received based on their behavior.
- If a user's actions negatively affect their score to below the allowed threshold, the users attempt to access a resource can be denied.
- If the action and behavior do not appear malicious, the user can be informed that their behavior and score do not meet the threshold.
- If the actions and behavior appear to be malicious, different handling procedures will be put in place depending on the actions, behavior, and resources accessed.
- All actions are logged to the SIEM, analyzed through the Analytics Engine, and deployed via the SOAR to provide real time policy access decisions.

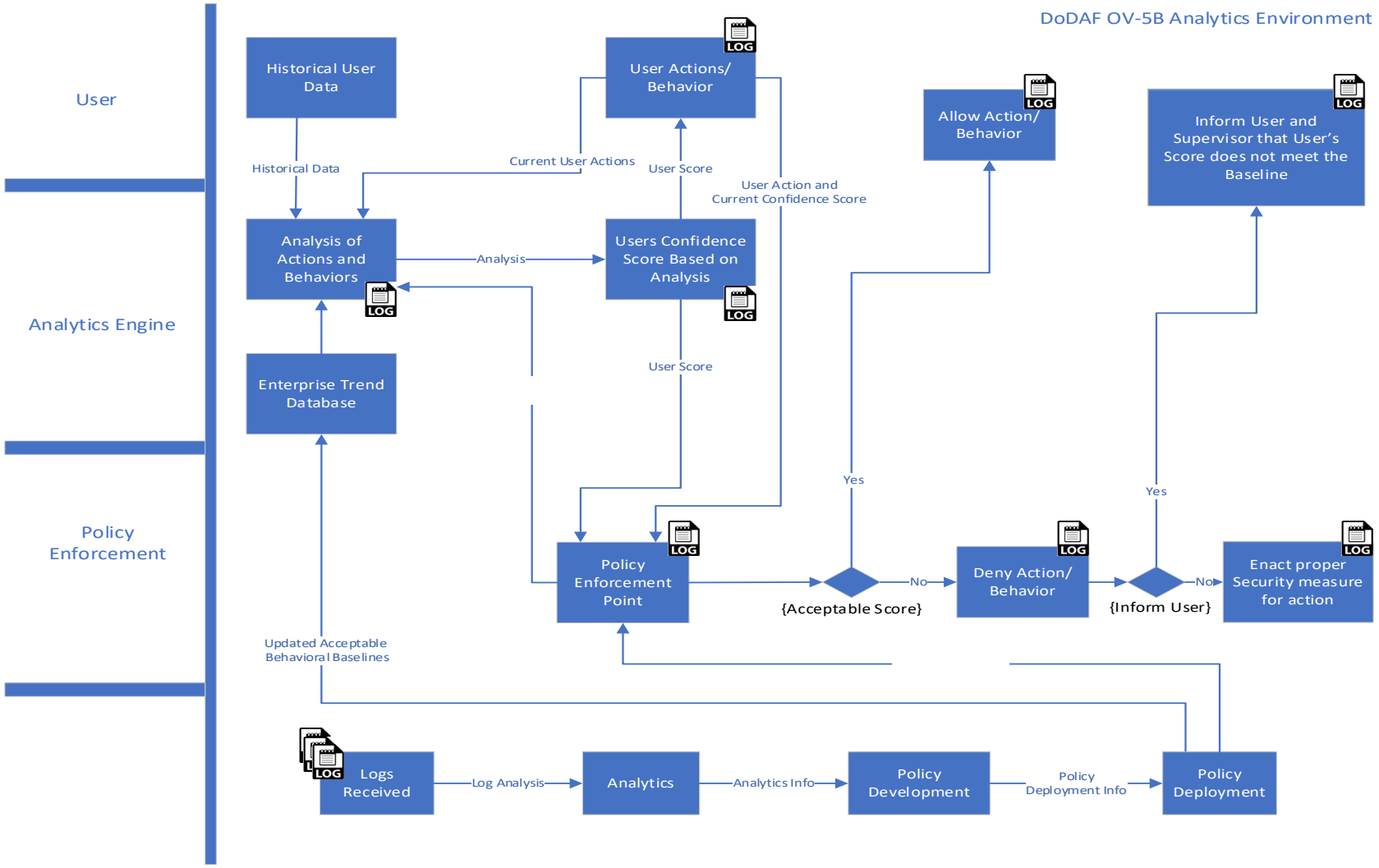

Figure 10: Operational Activity Model – Analytics (OV-5b)

4.5.4 Data Rights Management (DRM)

- User attempts to open an encrypted file
- DRM on the Endpoint checks for a cached key to open encrypted file
    - If a cached key is present, they key is checked with the Key Store to verify it's still valid.
    - If Key is valid, the document is opened with applied permissions and features.
    - If the key is invalid, a new request is initiated.
- If DRM has no cached key, a new request is initiated.
- Access request is sent to the DRM manager for access evaluation.
- If they DRM manager determines that the User does not meet the requirements to access the file, it will deny the user access and the user is notified.
- If the user is determined to be in good standing, the request is sent to the Key Store.
- The Key Store generates a new, temp key, based on the user's policy and the key is then deployed with the user's accessible permissions and features.
- The file is then opened with the provided permissions and features.
- All actions are logged to the SIEM, analyzed through the Analytics Engine, and deployed via the SOAR to provide real time policy access decisions.

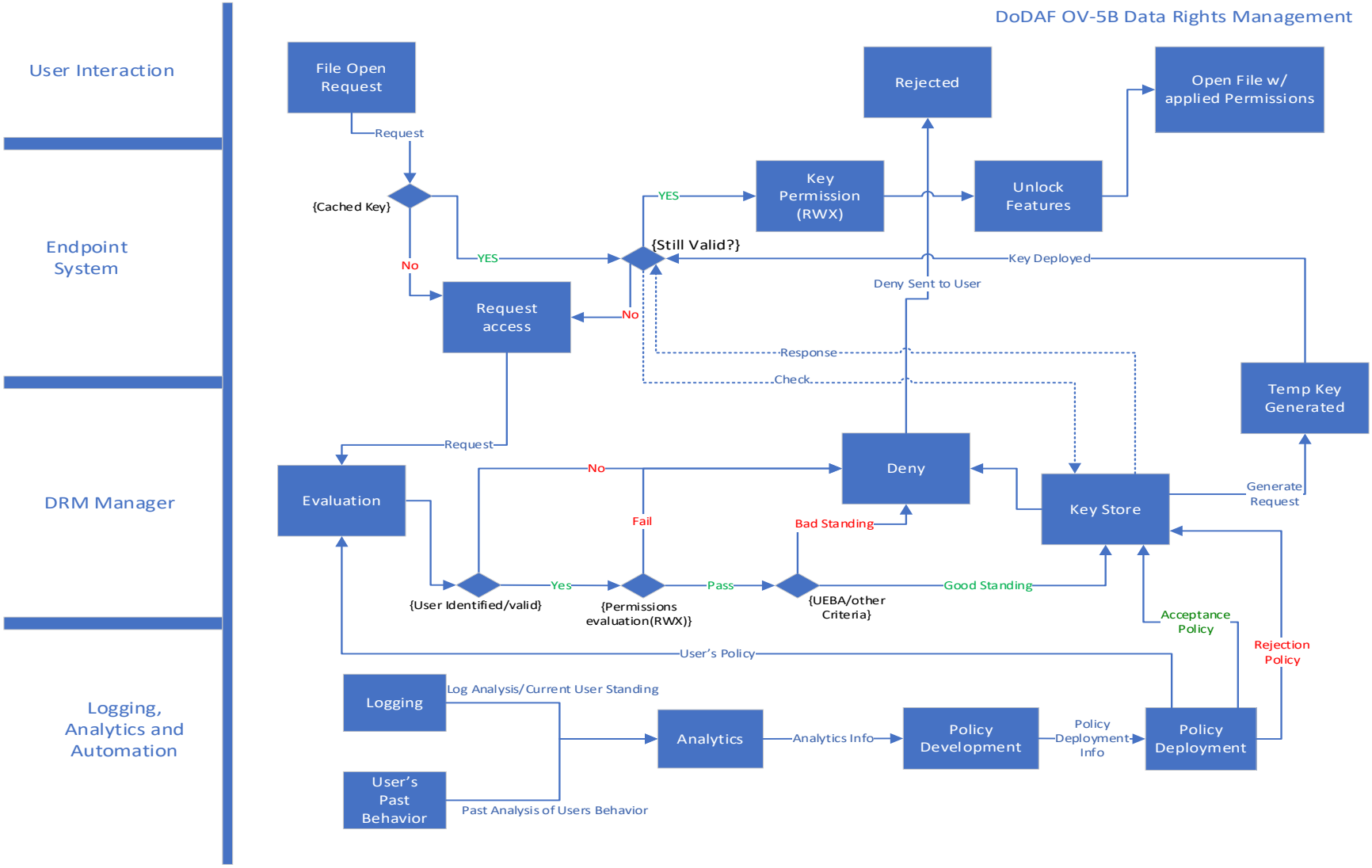

Figure 11: Operational Activity Model – Data Rights Management (OV-5b)

4.5.5 Macro Segmentation

- Entity requests access to network resource.
- Proxy/Enforcement Point checks Device’s attributes, behavior, and other data for proper policy enforcement.
- If the Proxy/Enforcement Point finds the device not in compliance or accessing a resource it shouldn’t be, access to the resource is denied.
- If the Proxy/Enforcement Point finds the device complies and has acceptable attributes have been determined, access to the Resource is granted.
- All actions are logged to the SIEM, analyzed through the Analytics Engine, and deployed via the SOAR to provide real time policy access decisions

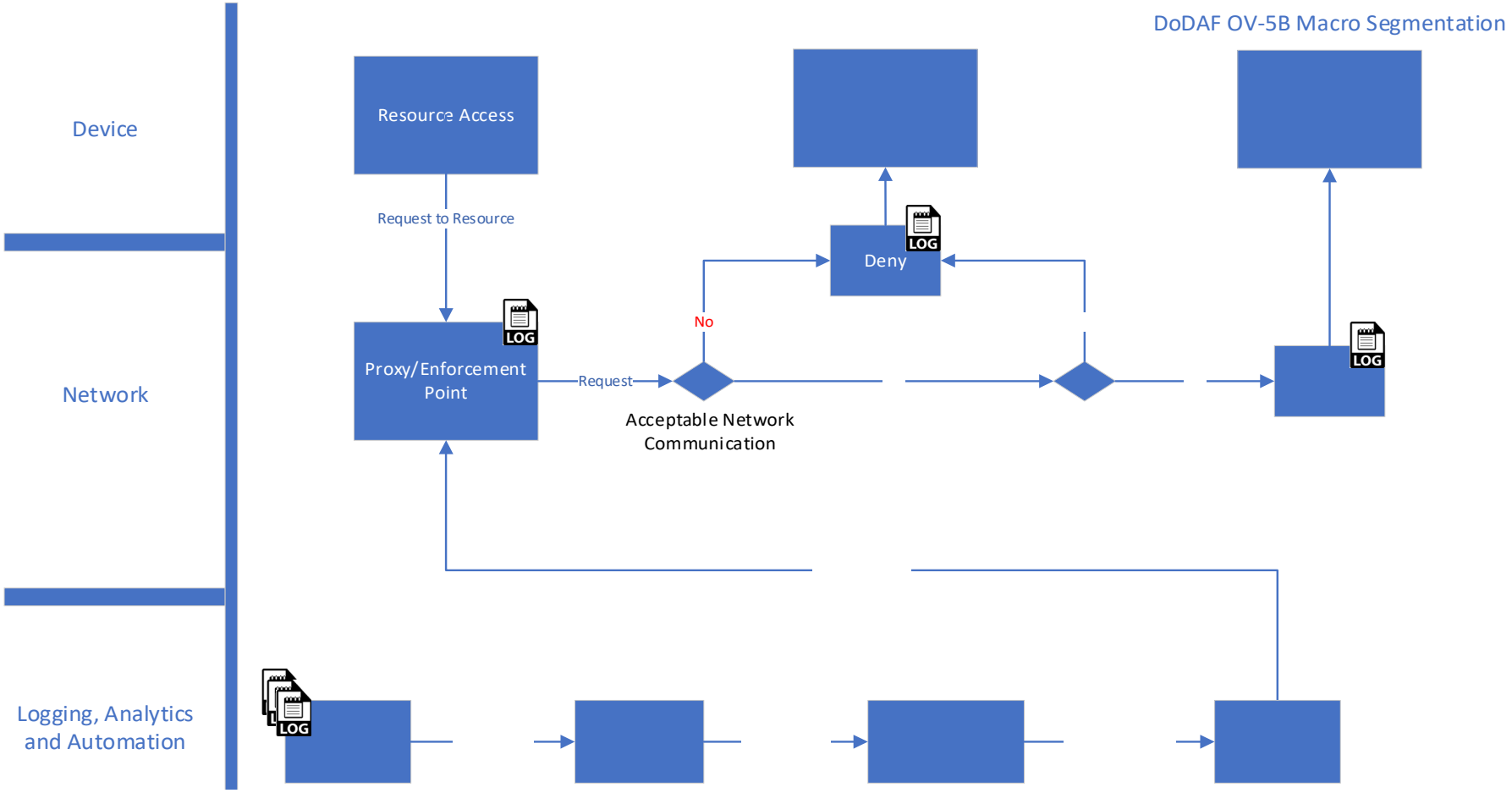

Figure 12: Operational Activity Model – Macro Segmentation (OV-5b)

4.5.6 Micro Segmentation

- A database Query will initiate a Request to the Resource from the Application Server
- If the Originating Process Communication is Acceptable, then move to next policy element. If not, then Log details and Deny Access
- If the Owner of originating process authenticated for task, then move to next policy element. If not, then Log details and Deny Access
- If the Proper Protocols are in use, then move on to next policy element. If any element policy check is invalid, deny access and log query.
- If it is from an approved location, then Allow the Traffic from the Network. If any element policy check is invalid, then deny access and log query.
- Repeat the above process for the Database Server. If all element policy checks passed proceed to the return query through the network. If any element policy check is invalid, then deny access and log query.
- If all element policy checks are valid on the return query through the network, then move onto the return query to the application server. If any element policy check is invalid, then deny access and log query.
- If all element policy checks are valid on the return query through the application server then query return shall be accepted. If any element policy check is invalid, then deny access and log query.

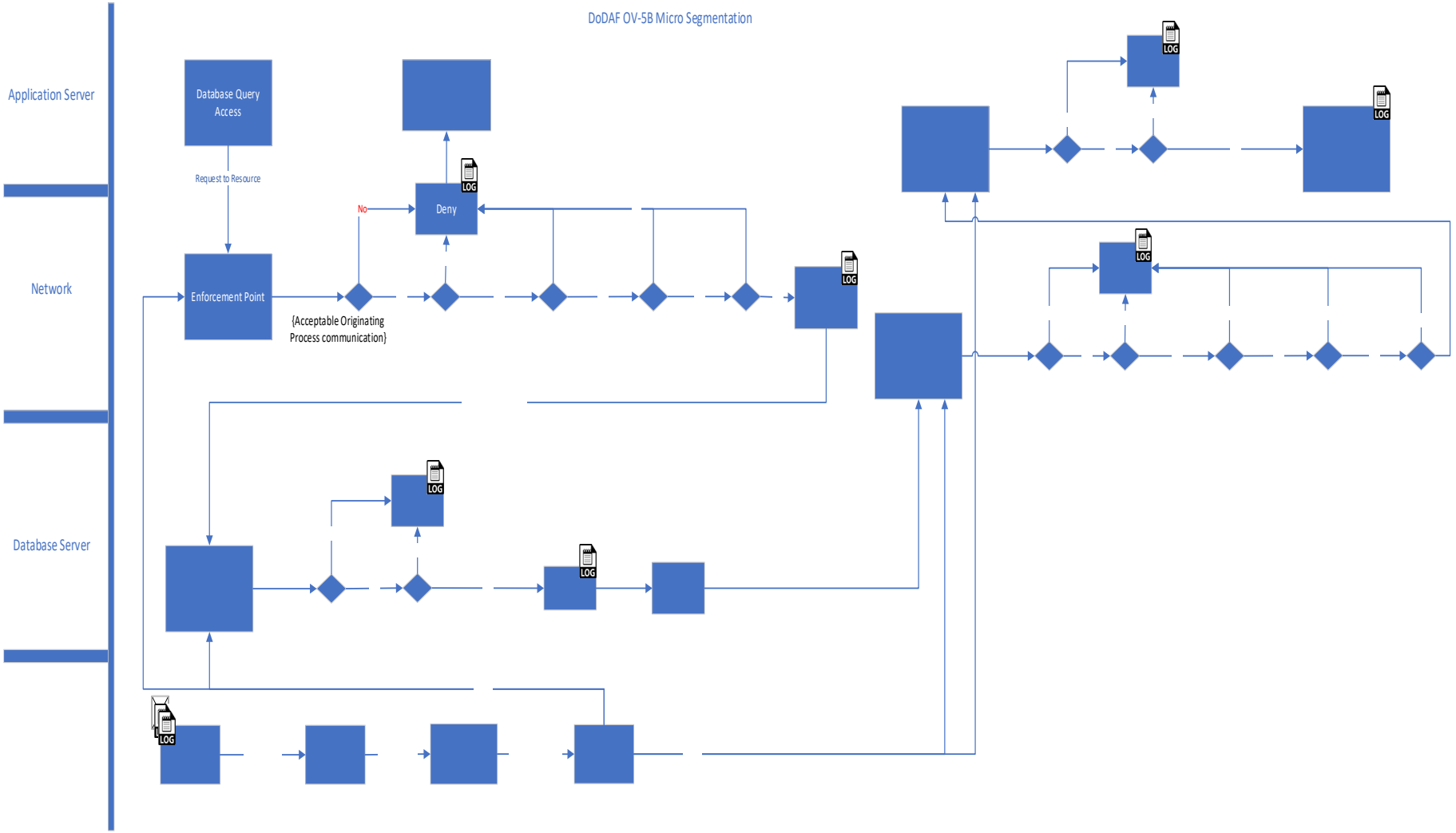

Figure 13: Operational Activity Model – Micro Segmentation (OV-5b)

4.5.7 Privileged Access

- User requests Elevated Resource Access with their own credentials.
- Enforcement Point validates the user's credentials, permissions, and behavior for authentication.
- The Enforcement Point will deny access if the User does not meet requirements.
- If the Enforcement Point deems the user in good standing, the user is Authenticated. The proxy opens a session with a request for Elevated Credentials from the Credential Vault to be applied to the session.
- The Credential Vault identifies the correct level of access required for the elevated session and applies the associated credentials with the correct level of access.
- The user is granted session access from the Proxy.
- User's session can be monitored in real time and will be logged.
- Once the user logs out of the session, the Proxy ends the session and notifies the Credential Vault.
- The Credential Vault destroys the elevated credentials.
- All actions are logged to the SIEM, analyzed through the Analytics Engine, and deployed via the SOAR to provide real time policy access decisions.

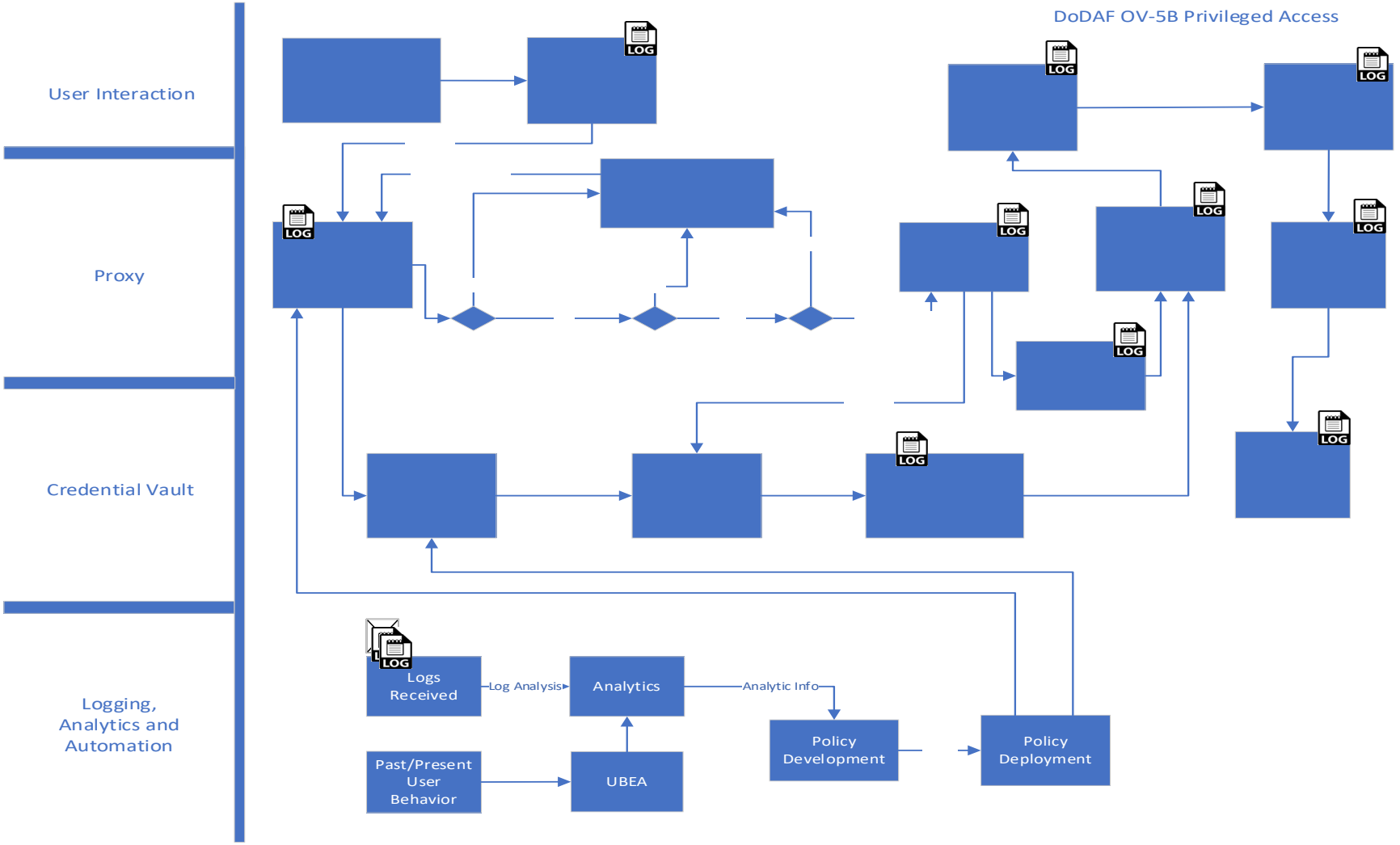

Figure 14: Operational Activity Model – Privileged Access (OV-5b)

4.5.8 Application Delivery

- User will first request access to the Web Application
- The device and user identity will be checked and then logged
- When logs are received, they will go through the process of Log Analysis -> Analytics -> Analytics Info -> Policy Development -> Policy Development Info -> Policy Deployment
- Once Policy Deployment is set it will send it through to the Segmentation Policy, User Policy Enforcement, and finally the UEBA Policy.
- They will then go through a segmentation policy check. If successful will go to the next policy check and if denied the access will be terminated for that session
- The next check shall be a User Policy enforcement. If successful will go to the next policy check and if denied the access will be terminated for that session
- The next check is the UEBA policy and if successful they will then gain access. If the policy check is denied the access will be terminated for that session

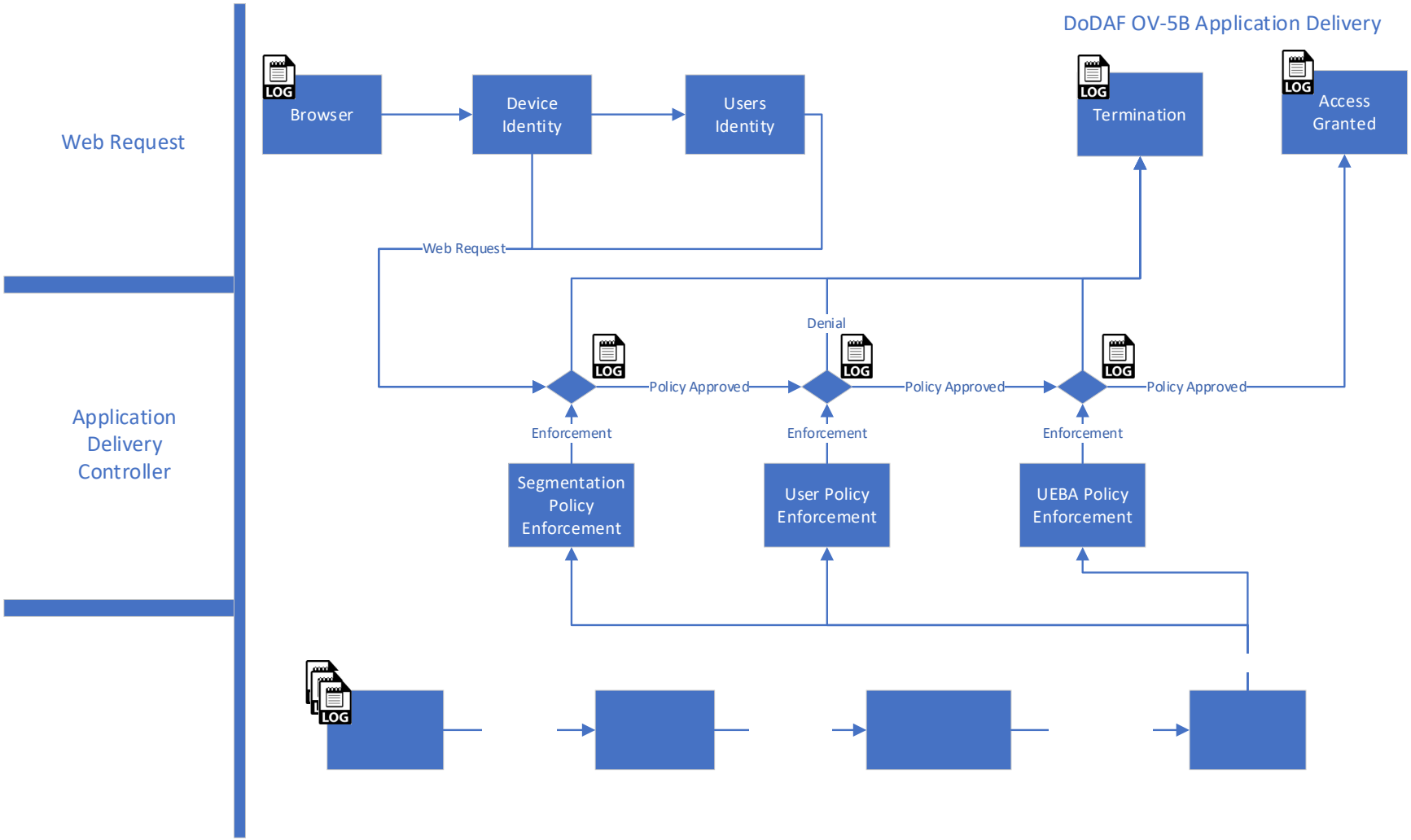

Figure 15: Operational Activity Model – Application Delivery (OV-5b)

5 VOCABULARY (AV-2)

Vocabulary provides context dependent ontology of semantic classification and meaning of the acronyms, terms and definitions of architecture elements used within the subject area. It enables a common understanding of terms and consistency of definitions used across the subject area. It includes acronyms, a taxonomy of terms, and definitions that are used in the Reference Architecture and relevant to solution architectures.

5.1 Glossary of Terms

Table 5: Integrated Dictionary (AV-2)

Term	Definition
Automatic Account Provisioning (AAP)	AAP is an access management system. It supports manual, dynamic, and hybrid entitlement provisioning and de-provisioning.
Assets	Examples of assets described in this ZT RA are SCADA controls, point-of-sale terminals, manufacturing assets and IoT devices
Attack Surface	The attack surface is the sum of the different points where an unauthorized user can (try to) enter data to or extract data from an environment. Keeping the attack surface as small as possible is a basic security measure.
Attribute	Characteristics of the subject, object, or environment conditions. Attributes contain information given by a name-value pair.
Attribute Based Access Control (ABAC)	An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.
Authorization	The process of granting or denying access to a network resource.
Confidence Levels	A formula that is used to determine the level of access based on the confidence of a tuple.

	(Note: We avoid “trust scores” because the term undermines the mindset shift required to eliminate the concept of “trust” with Zero Trust principles.)
Continuous Multi Factor Authentication (CMFA)	Continuous, or adaptive, authentication offers a better alternative for monitoring user activity, with user confirmation based on behavioral biometrics.
Credential Service Provider (CSP)	A CSP is a trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use.
Data Centric	An environment where data is the primary and permanent asset separated from systems/applications making data available to a broad range of tools and analytics within and across security domains of enrichment and discovery (ref. IC Data Management Lexicon, January 2020)
Device Attestation	A process that confirms or authenticates validation and verification of devices and/or associated policy data. Device attributes and contents (e.g. files, registry keys) may be used to validate the device.
Device/Asset Inventory (Service)	Contains information on devices (physical and virtual) and their associated hosts. It can continuously collect, processes, and publishes changes about the state of known devices.
Endpoint	Endpoints are often defined as end-user devices, such as mobile devices, laptops, and desktop PCs; although hardware such as servers in a data centers are also considered endpoints. This can be any device that transmits a packet. Devices such as zero clients, virtualized systems, and infrastructure equipment (i.e. routers and switches) are considered endpoints

Enterprise Mobility Management (EMM)	A comprehensive, hardware-agnostic method of remotely managing devices, including their configuration and the enterprise content generated on them, through Mobile Device Management (MDM) and Mobile Application Management (MAM). EMM is all-encompassing; it can control access to corporate apps, internal websites and even the data silos associated with them.
Federated Identity	In a federated identity scenario, the subscriber does not authenticate directly to the RP. Instead, the federation protocol defines a mechanism for an IdP to generate an assertion for the identifier associated with a subscriber, usually in response to a request from the RP.
Federation	A process that allows for the conveyance of authentication and subscriber attribute information across networked systems. In a federation scenario, the verifier or CSP is referred to as an identity provider, or IdP. The relying party, or RP, is the party that receives and uses the information provided by the IdP
Granular Access Control	Granular access control is the explicit defining of who can have access to what part of a network, or system resource, and what they can do with that access in policy.
Identity	Identity is an attribute or set of attributes that uniquely describe a subject within a given context.
Identity Provider (IdP)	The party that manages the subscriber's primary authentication credentials and issues assertions derived from those credentials. Is used in conjunction with a CSP for added security.
Joint Information Environment (JIE)	The JIE is a single, joint, secure, and agile command in order to combine the DOD's many networks into a command and shared global network in order to increase operational efficiency, enhance network

	security, and save money by reducing infrastructure and staffing.
Just Enough Administration (JEA)	Just Enough Administration allows one to grant an arbitrary subset of administrative privileges to a user. In practice, this allows one to grant only the privileges that are required to perform a particular action or duty. As a result, administrators performing any duty would be limited to only the rights and privileges that are required to do them, ensuring that abuse of admin credentials minimizes the potential damage that can occur.
Just in Time (JIT)	Just in Time Administration allows a timed expiration of group membership. In practice, this allows administrative rights to be given at the time of need for as long as an action or duty needs them. As a result, access to administrative privileges becomes limited and abuse must be timed for when those privileges are given.
Least Privilege	Also referred to as the Principle of Least Privilege, states that a subject/entity should be given only those privileges needed for it to complete its task.
Macro-segmentation	Similar in concept to physical network segmentation, macro-segmentation can be achieved through the application of additional hardware or VLANs.
Master User Record (MUR)	MUR is an access accountability system that supports access review. Supports identification of insider and external threats, and will enable financial management segregation of duties auditability across DoD Component organizations.
Microperimeter	A Microperimeter creates a point of control that ensures only known allowed traffic and legitimate applications have access to the protect surface. A Microperimeter should be

	placed as close to the protect surface as possible.
Micro-segmentation	Micro-segmentation is the practice of dividing (isolating) the network into small logical segments by enabling granular access control, whereby users, applications, workloads and devices are segmented based on logical, not physical, attributes. This also provides an advantage over traditional perimeter security, as the smaller segments present a reduced attack surface (for malicious actors). In a Zero Trust Architecture, security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.
Mission Owners	A mission owner is the person solely responsible for owning the mission of a program. They are accountable for designing an effective and efficient process, using the right resources to run the mission, and delivering quality outcomes as required.
Mobile Application Management (MAM)	Locks down enterprise applications and the data associated with them -- not the devices themselves. In short, MAM allows a company to control access to business applications and the content associated with them without controlling the entire physical device.
Mobile Device Management (MDM)	Allows IT to remotely enroll an employee or corporate-issued cell phone, tablet or other device and then track it, manage it and secure it through a profile specific to that employee and their tasks. It also allows IT to enforce device security, which can include locking out a device and wiping data if it's lost or an employee leaves a company.
Multi-Factor Authentication (MFA)	Authentication using two or more different factors to achieve authentication. Factors

	include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Next Gen-Firewall	Next-generation firewalls (NGFWs) offer a single virtual or physical appliance that combines traditional stateful firewall capabilities (OSI Layers 2 and 3), and other network device filtering functions, such as an application firewall using in-line deep packet inspection, intrusion prevention functionality, and advanced malware analysis features into a single solution that spans the entire stack (up to Layer 7). Within a Zero Trust architecture this can be used as a segmentation gateway to logically separate groups of users, devices and applications.
Non-Person Entity (NPE)	An entity with a digital identity that acts in cyberspace but is not a human actor. This can include an autonomous service or application, hardware devices (e.g. IOTs), and software applications (e.g. Bots).
Policy	The representation of rules or relationships that makes it possible to determine if a requested access should be allowed, given the values of the attributes and possibly environment conditions. Security policies that are automated and orchestrated consistently (within a Zero Trust Architecture) across Endpoints, LAN/WAN/Wi-Fi networks, Cloud, Software as a Service, etc.
Policy Decision Point (PDP)	A system entity that makes authorization decisions for itself or for other system entities that request such decisions. It examines requests to access resources and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the particular requester who issued the request under consideration.

Policy Enforcement Point (PEP)	A system entity enforces policy decisions in response to a request from a subject requesting access to a protected object. When a user tries to access a file or other resource on a computer network or server, the PEP will describe the user's attributes to the Policy Decision Point (PDP), request a security decision, and enforce that decision.
Policy Information Policy (PIP)	The system entity that acts as a source of attribute values (when requested by the PDP).
Privileged Access Management (PAM)	Privileged Access Management (PAM) refers to a class of solutions that help secure, control, manage and monitor privileged access to critical assets.
Privileged Access Workstation (PAW)	A workstation that has been specifically designated only for certain administrative tasks. Extraneous applications are removed to lower the attack surface. Because the PAW has heightened administrative accesses, it is necessary to ensure that the PAW has been properly configured and secured.
Protect Surface	A protect surface is based upon at least one of the below four items (remembered by the acronym DAAS): Data: What data needs to be protected? Applications: Which applications consume sensitive information? Assets: Which assets are most sensitive? Services: Which services, such as DNS, DHCP, and Active Directory, can be exploited to disrupt normal IT operations?
Role Based Access Control (RBAC)	Role-based access control is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on

	organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user.
(Network) Segmentation	A security technique used for protection of data center resources; this can be physical and/or logical (virtualized network). *Physical segmentation* of a data center network is enabled using physical devices such as the Top of the Rack (ToR) switches, aggregate switches, core switches and routers as well as the physical Network Interface Cards (NICs) in each of the hosts. *Logical network segmentation*, on the other hand, requires the deployment of (is only relevant in the context of) a logical or virtual network on top of the physical network in the data center. Depending on the use case, segmentation can be accomplished using the following techniques, a DMZ (based on virtual switches and physical NICs); VLANs for protecting virtualized infrastructures; or an overlay-based approach in a cloud data center.
Segmentation Gateway	A term used by industry to define boundaries that effectively compartmentalize different segments of the infrastructure, allowing administrators to protect critical intellectual property from unauthorized applications or users, reduce the exposure of vulnerable

	systems, and prevent the lateral movement of malware.
Strong Identity	The pairing of an authenticated user and device.
Software Defined Networking (SDN)/SDN Architecture	Software-Defined Networking is an API-driven orchestration of the IT network infrastructure used to enable orchestration of network routing within an IT network. SDN enables dynamic, programmatically network configuration in order to improve network performance and monitoring; making it more like cloud computing than traditional network management. The focus of SDN is traffic efficiency—not security and authorization. A well-run SDN system delivers reliable, efficient, and adaptive network bandwidth to an enterprise.
Tuple	A set of attributes to make access decisions (e.g. device, identity, location, and time of day).
Unified Endpoint Management (UEM)	A class of software tools that provide a single management interface for mobile, PC and other devices. It is an evolution of, and replacement for, mobile device management (MDM) and enterprise mobility management (EMM) and client management tools.

5.2 Activities Definitions

Table 6: Activities Definitions (AV-2)

Activity Name	Activity Definition
A0 Provide the DOD Information Enterprise (IE)	This activity allows the IE to function as one unified DOD Enterprise, creating an information advantage for our people and mission partners by providing: a rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise; and an available and protected network infrastructure that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.

A1 Manage and Oversee IE	This activity governs the development and implementation of the IE. It establishes and uses those structures and processes required to provide effective, high-level management and oversight of IE components and operations. It implements strategies, policies, and standards providing the direction necessary for the IE to meet applicable laws, regulations, and policies (LRP), while at the same time delivering the capabilities necessary to fully enable net-centric warfighting, business, and intelligence operations for successful mission accomplishment.
A1.1 Provide Enterprise-wide Guidance	This activity develops, maintains, and enforces the policy and provides the oversight required for the development, deployment, and overall management of solutions, common operational strategies, business processes, standards, policies, laws, and culture for the IE. It is the responsibility of the DOD CIO, CJCS, DISA, and other stakeholders to provide an enterprise-wide policy management solution for the generation, deconfliction, and distribution of IE policies at any level in the enterprise hierarchy. These policies provide the authority to govern and the guidance to achieve an IE end state consisting of a consolidated and secure computing environment that delivers Information Technology (IT) capabilities to meet warfighter, business, and intelligence requirements of the DOD.
A1.1.1 Develop IE Vision and Strategy	This activity provides a set of overarching principles, rules, and strategic requirements describing the desired end state of the IE and how it is to be governed to enable net-centric operations and conform to a specified set of baseline or foundation operational requirements.
A1.1.1.1 Define IE Interoperability	This activity establishes principles, rules, and strategy describing required interoperability for IE assets, in accordance with approved operational requirements and applicable Joint Capabilities Integration and Development System (JCIDS) documents and compliant with the operational, capabilities, services, and technical viewpoints of the DOD Enterprise Architecture (EA).
A1.1.1.2 Determine Common Infrastructure Architecture Requirements	This activity establishes the requirements for a common, or enterprise-level, communications and computing infrastructure architecture for DOD, able to provide a full range of information services at all major security classifications and information handling caveats consistent with NSTISSP No. 11.
A1.1.1.3 Enable IE Audit	This activity makes the details of IE plans, architectures, designs, hardware, software, and supporting organizational resources available and accessible in order to conduct the level of audit review required to ensure appropriate security and effective management of engineering, operations, maintenance, and sustainment of the IE.
A1.1.1.4 Develop IE Evolution Strategy	This activity establishes a strategy for the continual architecting, planning, and engineering of flexible, agile, and integrated capabilities within the IE and its rapid evolution through judicious application of commercial technologies and standards.

A1.1.1.5 Develop Precedence-Based Services Strategy	This activity supports the development of policies designating precedence-based, assured services for all Command and Control (C2) applications traffic with multiple levels of differentiation and support of Commander's Intent.
A1.1.1.6 Develop IE Acquisition Strategy	This activity establishes a strategy for IT acquisition describing how IE resources are to be planned, resourced, acquired, and implemented in accordance with the 5000 series of DOD Issuances.
A1.1.1.7 Develop Joint Training Strategy	This activity establishes a common IE training strategy for commanders at all echelons to use in improving joint readiness by fully educating the user on topics related to the IE.
A1.1.2 Develop IE Functional Policy	This activity establishes and enforces policies required to implement, direct, and enable NetOps, communications, information sharing, services, and information assurance functions in the IE in order to enable seamless integration mechanisms that support joint IT capabilities. Such policies are established and enforced by both the DOD CIO and the Chairman of the Joint Chiefs of Staff (CJCS).
A1.1.2.1 Develop NetOps Policy	This activity administers, monitors, and enforces policy governing Network Operations (NetOps) processes, procedures, structures, and concepts for ensuring the availability, configuration, security, and performance of IE resources during operations. It focuses on policies managing NetOps enablement of the sharing of IE resources and coordination of NetOps actions across the enterprise.
A1.1.2.1.1 Administer NetOps Policy	This activity deploys and maintains NetOps policies, standards, governance, and guidelines addressing traditional systems and network management (Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management (FCAPS)) and information and infrastructure protection. It enables the ability of NetOps to control the maneuvering of information across the terrestrial, space, and airborne wireless environments through Enterprise Management, Network Defense, and Configuration Management.
A1.1.2.1.2 Monitor NetOps Policy	This activity reviews and analyzes the application and practice of NetOps policies, standards, governance, and guidelines.
A1.1.2.1.3 Enforce NetOps Policy	This activity applies NetOps policies during operations to achieve the desired effects of Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery.
A1.1.2.2 Develop NetOps Command and Control (C2) Policy	This activity establishes and enforces policy and a command structure for the exercise of authority and direction by a properly designated NetOps commander over assigned and attached forces to attain information superiority by way of unity of effort in command, control, and management of the IE.

A1.1.2.3 Develop Quality of Service (QoS) Policy	This activity establishes and enforces policy directing a certain level of performance for data flow across the IE, implementation of resource reservation control mechanisms, guaranteed Data-in-Transit availability, and transfer rate and resource allocation. Such policies also establish network performance metrics and Service Level Agreements (SLA). The focus is on determining appropriate traffic engineering parameters comparable to Quality of Protection (QoP) in network security and software measurements.
A1.1.2.4 Develop Quality of Protection (QoP) Policy	This activity establishes and enforces policy ensuring Data-in-Transit protection and establishing security metrics and Program Level Agreements (PLA) that are appropriately addressed across architecture components. The focus is on determining appropriate protection parameters and establishing progress towards quality of protection in security comparable to QoS in networking and software measurements.
A1.1.2.5 Develop Communications Policy	This activity establishes and enforces policy assigning responsibilities and providing guidance for the planning, coordination, and production of joint communications.
A1.1.2.6 Develop Joint Spectrum Data Plan	This activity establishes a spectrum data plan to enable all users to work together by exchanging vital spectrum information from the beginning of the joint planning process and ensuring that scarce spectrum resources are used effectively and efficiently.
A1.1.2.7 Develop Information Sharing Policy	This activity establishes and enforces policy providing guidance for information sharing in a net-centric environment through collaborative forums (i.e., communities of interest or COIs), establishing a set of activities that members of COIs and associated leadership can use to implement key policies of DODD 8320.02, and directing the sharing of information across security domains.
A1.1.2.8 Develop Configuration Management Policy	This activity establishes and enforces policy providing an enterprise-wide configuration management solution for the assured implementation, update, and management of network/platform configurations, software patches/upgrades, and hardware upgrades. Such policy also directs that all deployed Cybersecurity devices and mechanisms incorporate approved features, functions, capabilities, and settings necessary to support their intended mission. This includes security critical versions, patches, interface standards, lifecycle configuration, mode and option settings, and crypto algorithms.
A1.1.2.9 Develop Cybersecurity Policy	This activity establishes and enforces policies that protect information and information systems by ensuring secured availability, integrity, authentication, confidentiality, and non-repudiation.

A1.1.2.9.1 Develop Cybersecurity Assessment & Accreditation (A&A) Policy	This activity establishes and enforces policy providing oversight for a DOD-wide A&A program responsible for identifying, implementing, validating, certifying, and managing cybersecurity personnel, capabilities, and services and authorizing the operation of information systems throughout the IE. It also enables initiatives to develop a A&A process, controls baseline, and mechanisms that are common across all Federal departments, Agencies, and Communities of Interest and promotes participation in the development, promulgation, implementation, and governance of guidelines and milestones for migration to Unified A&A standards and processes.
A1.1.2.9.2 Develop Identity Management and Authentication (IdM&A) Policy	This activity establishes and enforces policy providing for common identity management and authentication processes across DOD in accordance with Federal guidance and direction and addressing trust negotiation between DOD components and mission partners for providing assured IE access to all authorized entities.
A1.1.2.9.3 Develop Access Control Policy	This activity establishes and enforces a common access policy defining what access subjects may have to classes of objects, how access decisions will be handled in tactical and non-tactical domains, and mechanisms by which exceptions to policy can be made in response to operational needs.
A1.1.3 Establish IE Standards	This activity provides and enforces a common set of standards for the IE, enabling the consolidation, interoperability, and security of a joint infrastructure and development of joint IT capabilities supporting warfighter, business, and intelligence mission requirements. Enterprise-level standards support both internal and external users by providing a common platform for integration across the IE and with mission partners.
A1.1.3.1 Develop NetOps Standards	This activity defines common NetOps standards for the enterprise to ensure integration across components. Once defined, these standards are shared with the community and enforced. These standards include, but are not limited to, QoS and QoP.
A1.1.3.2 Develop Cybersecurity Standards	This activity defines common information assurance standards for the enterprise to ensure integration across components. Once defined, these standards are shared with the community and enforced. These standards include, but are not limited to, defense messaging, cryptographic key algorithms, and Public Key Infrastructure (PKI).
A1.1.3.3 Develop Communications Standards	This activity defines common communications standards for the enterprise to ensure integration across components. Once defined, these standards are shared with the community and enforced. These standards include, but are not limited to, wireless security, communication protocols, and ports.
A1.1.3.4 Develop Computing Infrastructure Standards	This activity defines common computing standards for the enterprise to ensure integration across components. Once defined, these standards are shared with the community and enforced. These standards include, but are not limited to,

	programming languages, server architectures, and operating system components.
A1.1.3.5 Develop Data/Service Standards	This activity defines common data and services standards for the enterprise to ensure integration across components. Once defined, these standards are shared with the community and enforced. These standards include, but are not limited to, messaging specifications, metadata exchange specifications, and security specifications.
A1.1.3.6 Develop Metadata Standards	This activity defines metadata standards and cataloging techniques to share information across the enterprise in an understandable manner.
A1.2 Implement Joint/Enterprise Level Governance of the IE	This activity establishes and uses required structures, mechanisms, processes and procedures to effectively govern the development and operation of the IE. It provides clear legal authority for such governance by defining accountable commander requirements and processes to meet mission objectives.
A2 Protect and Secure the IE	This activity guard's critical data, capabilities, the IT infrastructure, and data exchanges within the IE, while providing authentication and non-repudiation of information and transactions to enable assurance and trust. It controls user access to data and services, determines vulnerabilities and attempts to prevent the exploitation of these vulnerabilities from both external and internal threats, and monitors IE activity, recognizing and assessing security-related incidents and then providing appropriate responses.
A2.1 Enable Global Authentication and Access Control	This activity ensures secure, adaptive, and rapid access across trusted and authenticated domains for all authorized entities requesting interaction with IE resources from any location, at any time, using common and portable identity attributes. Authorized entities include personnel, such as members of the DOD, IC, United States Government (USG) agencies, and coalition partners, and elements of the infrastructure, such as servers, unmanned aerial vehicles (UAVs), and handheld devices. The activity further ensures authentication processes are performed with an appropriate level of assurance, privileges are properly managed as subjects and objects join and leave the federation, interoperability is enhanced across components, and mission and business benefit are derived from the efforts.
A2.1.1 Provide Identity Management and Authentication	This activity provides joint identity management, universal credentialing, and secure authentication services to the warfighter, business, and intelligence operator, ensuring timely access to critical information and services. It oversees identity management initiatives within the Department and ensures DOD transition to two-factor authentication mechanisms is carried out in a way that

	enhances interoperability among Service and Agency authentication systems.
A2.1.1.1 Manage Identity Life Cycle	This activity identifies and oversees the identity life-cycle for DOD entities. It manages identities in both tactical and non-tactical environments and across classification levels. It also manages the identity life-cycle for non-DOD users of DOD IE components, to include other federal agency employees, coalition personnel, first responders, and unanticipated users.
A2.1.1.1.1 Register Identity	This activity vets' identities, correlates identifying attributes, records initial identifying attribute values, records initial identity metadata, and assigns a unique identifier to each identity.
A2.1.1.1.2 Maintain Identity	This activity updates identifying attribute values, correlates altered identifying attributes, vet's identity updates, updates identity metadata, and archives identities.
A2.1.1.1.3 Expose Identity Information	This activity makes identity information (i.e., identifying attributes and metadata) from the domain of origin visible, available, and accessible to authorized users.
A2.1.1.2 Provide Credentialing Mechanisms	This activity provides the tools, controls, and processes required to issue, revoke, and store credentials, whether physical or electronic.
A2.1.1.2.1 Manage Credential	This activity manages comprehensive credentials providing an enterprise-wide source of data about user identities and attributes, to include implementing a comprehensive credential registry.
A2.1.1.2.1.1 Issue Credential	This activity includes validation of credential requests, generation of a credential using validated attributes, and secure delivery of a credential to the proper entity.
A2.1.1.2.1.2 Maintain Credential	This activity performs maintenance for an issued credential, including tracking of credential status (e.g., revocation and expiration) and re-issuance of credentials when authorized by policy (e.g., recovery of lost or locked passwords or recovery of a key encryption certificate). It also provides a real-time mechanism for suspending / terminating credentials for those entities under suspicion or identified as cybersecurity threats.
A2.1.1.2.1.3 Expose Credential Information	This activity responds to queries for credential information (e.g., status, strength) and exposes the requested credential attributes to properly authorized users.
A2.1.1.2.2 Manage Credential Repository	This activity manages a joint / common repository for storing attributes associated with requested, issued, and revoked credentials.
A2.1.1.3 Authenticate Entity	This activity identifies, tests, and certifies authentication mechanisms; validates the authenticity of credentials; and verifies

	identities to establish non-repudiation and control information dissemination.
A2.1.1.3.1 Provide Authentication Mechanisms	This activity provides the tools, controls, and processes required to exploit credential attributes.
A2.1.1.3.2 Validate Credential Authenticity	This activity ensures a presented credential is valid and meets all security requirements based on the operating environment.
A2.1.1.3.3 Verify Identity	This activity ensures the entity presenting the credential is the identity associated with the credential.
A2.1.2 Provide Access Control	This activity uses a joint control mechanism to grant authorized entities access to required information, services, and applications on the IE from any location. It uses predefined attributes and rules to provide safe, secure, and rapid access to data and applications required to execute daily operations across the IE.
A2.1.2.1 Provide Adaptive Access Framework	This activity develops and manages the policy, standards, and mechanisms required to govern access to DOD information and IT systems. It implements procedures for handling access decisions in both the tactical and non-tactical domains and defines mechanisms by which exceptions to access policy are made in response to operational needs.
A2.1.2.1.1 Identify Standard Attributes	This activity defines a standard attribute model for DOD people, services, and property to enable attribute-based access control. This includes defining a common set of agreed upon attributes as defined by COIs and establishing and publishing a standardized format for each agreed upon attribute.
A2.1.2.1.2 Enable Access Controls	This activity provides configuration controls to manage and administer the level of access granted to IE resources. It supports the configuration of hardware resources, operating systems, shared applications, and data so access for users, groups of users, other applications, and other computing components is controlled through ABAC by leveraging applicable digital rules.
A2.1.2.2 Manage Access Process	This activity exposes the attributes associated with an authenticated entity requesting access to the GIG and leverages those attributes, the attributes of the requested service or data, and the governing digital rules to establish privileges to GIG resources.
A2.1.2.2.1 Manage Trust Negotiation	This activity allows trust to be established between two previously unrelated entities by means of an iterative exchange of credentials. As credentials are processed and validated, greater levels of access are granted according to predefined digital rules.
A2.1.2.2.2 Manage Access Privileges	This activity manages privileges derived from entity attributes and established digital policy to establish attribute-based access control to IE resources. It oversees the creation of processes by which privileges are managed, to include their creation, assignment, modification, delegation, revocation, and elimination. It also develops and maintains an attribute management infrastructure for the Department.

A2.1.3 Provide Federation	This activity manages DOD's Cybersecurity federation with multiple entities both within and external to DOD, enabling secure operation and information exchange across a wide range of policies, standards, architectures, registries, and attributes. It provides the environment which enables portability of identity and credential information across autonomous domains without the need for redundancy. As part of this activity identity and credential managers associated with the federation participate in governance, comply with federation requirements, and submit to audits.
A2.1.3.1 Manage DOD's Participation in Federation	This activity manages and maintains DOD's alignment with other Federation partners, including other Federal Departments and Agencies, state and local governments, coalition partners, first responders, and non-governmental organizations (NGOs).
A2.1.3.2 Synchronize and Deconflict DOD Cybersecurity Attributes	This activity coordinates and aligns DOD identity, authentication, and subject/object attributes with Federation partners.
A2.1.3.3 Manage Federation Rules	This activity develops guidance and manages processes and mechanisms enabling the implementation of DOD federation policy, within DOD, as well as with other non-DOD federation partners.
A2.1.4 Monitor Authentication and Access Control	This activity enables threat management and trend analysis of authentication and access requests, providing a cybersecurity mechanism for highlighting potential breaches or vulnerabilities associated with unauthorized attempts to authenticate, excessive use of access privileges, or other suspicious activities.
A2.1.4.1 Define Threat Level	This activity establishes an incident threshold associated with authentication and access requests for use in identifying threats. This threshold is based on frequency, geography, information sensitivity, and other suspicious patterns.
A2.1.4.2 Perform Audit	This activity provides real-time tracking and analysis of authentication and access requests across the IE.
A2.1.4.3 Identify Threats	This activity identifies authentication and access incidents which meet or exceed established threat profiles.
A2.1.5 Manage Digital Rules	This activity maintains the digital rules used for authentication and access control processes. These rules define the relationships between IE components to ensure that all authentication and access control related policies (i.e. Quality of Protection (QoP), Access Control, etc.) are followed.

A2.2 Enable Cross Domain Security	This activity involves the DOD CIO providing oversight and guidance for the development and deployment of solutions and services facilitating the sharing of information across disparate security domains. It implements methods for managing the transition from today's information-sharing paradigm, focused on interconnecting physical networks separated by classification, to a more Net-Centric paradigm, allowing information sharing based on classification and role-based access. Special attention given to development of enterprise-wide Cross-Domain Solutions (CDS) and services permitting collaboration with first responders, NGOs, state and local governments, as well as coalition information sharing.
A2.2.1 Enable Cross Domain Information Discovery	This activity provides the capabilities required to perform information and service search and discovery across domains with different security policies.
A2.2.2 Enable Cross Domain Information Exchange and Service Invocation	This activity provides the capabilities required for the exchange of information and invocation of service capabilities across domains with different security policies.
A2.2.3 Manage CDS Initiatives	This activity provides oversight, direction, and guidance to the development and deployment of new and enhanced Cross Domain Solution (CDS) capabilities.
A2.2.3.1 Participate in Unified Cross Domain Management Office (UCDMO)	This activity provides for DOD involvement in the UCDMO, which is responsible for centralized coordination and oversight of all cross-domain activities and investments for the DOD and Intelligence Community (IC).
A2.2.3.2 Deliver Cross Domain Solutions as Enterprise Services	This activity implements enterprise-wide cross domain solutions as services that can be accessed by any authorized user.

A2.2.4 Implement End-to-End Security Accreditation	This activity oversees and guides DOD transition to enterprise-wide accreditation and security accountability.
A2.3 Safeguard the IE	This activity provides key protection processes, procedures, and management. It safeguards the IE by implementing protection of network and enclave boundaries, managing network resources, providing IT platform protection, protecting data at rest and in transit, and overseeing Information Assurance & Vulnerability Assessment (IAVA) compliance.
A2.3.1 Protect Network and Enclave Boundaries	This activity provides CIO guidance and standards for protecting the IE and the boundaries of enclaves within the IE. The CIO will develop standards on how individual components are put together to secure those boundaries. The concepts of cybersecurity and CND are key to ensuring information and information systems in the IE are protected and defended from adversaries.
A2.3.1.1 Provide Technical Protection Standards	This activity develops and promulgates ports and protocols standards and tools required to limit the vulnerability of networks within the IE and to assure secure compatibility between systems operating in the IE.
A2.3.1.2 Issue Enclave Protection Policy	This activity develops and communicates guidance and standards for protecting the boundaries of enclaves within the Information Enterprise.
A2.3.2 Manage Network Resources to Defend IE	This activity involves the DOD CIO providing guidance and direction for the management of network resources, computing, communications, and services, as well as information availability and accessibility, to protect the IE from internal and external threats. Highly Available Enterprise (HAE) and Assured Mission Management (AMM) core capabilities are integral parts of this activity. HAE provides for high assurance networking, robust networking services, and flexible resource management. AMM provides Course of Action policy and configuration management automation to assist in dynamically managing network resources.

A2.3.3 Provide IT Platform Protection	This activity involves the DOD CIO providing guidance and direction regarding the ability to protect individual IT components essential to ensuring the security of the GIG (as need arises). This direction is based on assessments of the vulnerability to exploitation and attack of potential IT platforms and establishes processes and standards for acquiring and using the least vulnerable of such platforms.
A2.3.3.1 Assess Vulnerability of Potential IT Platforms	This activity evaluates the degree to which potential IT platforms can be trusted to operate securely in the IE.
A2.3.3.2 Support National Vulnerability Evaluation and Acquisition Requirements Development	This activity enables DOD's participation in the development of common National requirements, standards, and processes for evaluating the vulnerability of IT platforms and use of evaluated products in the IE.
A2.3.4 Enable Data Protection	This activity defines standards and enforces protection properties for protecting data objects while stored electronically and in transit between end systems. The activity involves the DOD CIO's involvement in providing direction and guidance describing how data resources are to be protected while in transit between end systems. Protection includes prevention of direct disclosure (confidentiality), indirect disclosure through traffic analysis and covert channel exploitation, and data modification (integrity). Key components of the activity include issuing and administering relevant policies and standards and ensuring that anticipated future needs are addressed in an overall evolution strategy.
A2.3.4.1 Standardize Data-at-Rest Protection	This activity defines standards and enforces properties for protecting data objects while 'at rest' (e.g., stored on electronic media such as hard disk drives, storage area networks (SANS), cartridges or other backup media, CDs/DVDs, thumb drives, personal digital assistants (PDAs), cell phones, or other removable storage media).

A2.3.4.2 Standardize Data-in-Transit Protection	This activity oversees and manages the security strategy for data moving between various processing and storage nodes within the IE. It maintains visibility of issues relating to specific Data-in-Transit needs, manages associated initiatives and programs to address these needs, and ensures compliance through the funding process.
A2.3.4.2.1 Manage Security Strategy for Data-in-Transit over IPv6	This activity develops and enforces a strategy for protecting data-in-transit associated with the implementation of IPv6 across DOD.
A2.3.4.2.2 Protect Data-in-Transit Between NIPRNet and Internet	This activity oversees the safeguarding of data transferred between the NIPRNet and the Internet.
A2.3.4.2.3 Protect Data-in-Transit Across System High Boundaries	This activity establishes and manages a security model providing data-in-transit protection across system high system and enclave boundaries.
A2.3.4.2.4 Integrate Data-in-Transit Protection Across Architecture Components	This activity oversees the incorporation of Data-in-Transit protection mechanisms and concepts into DOD architecture descriptions.
A2.3.4.2.5 Protect Data-in-Transit during Coalition Information Sharing	This activity manages the protection of data-in-transit during the sharing of information with coalition forces, including in Federated Coalition environments.
A2.3.5 Manage Information Assurance & Vulnerability Assessment (IAVA) Compliance	This activity enforces organizational compliance with IAVA regulations and policy, as stated within the Defense Critical Infrastructure Program (DCIP). It ensures implementation of IAVA-compliant security solutions delivering complete vulnerability management, to include asset discovery and inventory, network and agent-based assessments of software and configuration vulnerabilities, automated remediation and ongoing policy compliance audits - all from a single, seamlessly integrated solution with enterprise reporting.

A2.4 Manage IE Assessment and Accreditation (A&A) Program	This activity provides oversight for a DOD-wide Assessment and Accreditation (A&A) program responsible for identifying, implementing, validating, certifying, and managing cybersecurity capabilities and services and authorizing the operation of information systems.
A2.4.1 Govern Enterprise-wide A&A	This activity ensures proper execution of standard certification processes and accreditation decisions across the IE.
A2.4.2 Provide Automated A&A Services	This activity provides common and interoperable automated A&A services that implement policy and standards, manage A&A data as an enterprise asset, and support Federal Information Security Management Act (FISMA) and other performance reporting.
A2.5 Provide Cybersecurity Workforce	This activity provides guidance, standards, and tools promoting the development of a cybersecurity workforce with a common understanding of DOD cybersecurity concepts, principles, and applications.
A2.5.1 Identify DOD Cybersecurity Positions	This activity defines a DOD-wide cybersecurity personnel structure, associated skill sets, and qualification standards.
A2.5.2 Manage Cybersecurity Personnel Lifecycle	This activity oversees and monitors events in the lifecycle of the cybersecurity workforce.
A2.5.3 Oversee DOD Cybersecurity Training and Education	This activity oversees and monitors training and education for the cybersecurity workforce. This activity also guides and oversees the development of cybersecurity educational material and training and awareness aids, as well as the services and mechanisms for their dissemination.
A2.5.4 Implement Cybersecurity Orientation and Awareness	This activity establishes and monitors minimum requirements for cybersecurity orientation and awareness for IE users.
A2.6 Provide Assured Control of IE	This activity governs and manages cybersecurity services and resources in defense of IE.
A2.6.1 Manage Computer Network Defense (CND) and Cybersecurity Services	This activity governs services performing CND and cybersecurity functions for the IE.
A2.6.2 Provide Policy-Based Management of Cybersecurity Components of IE	This activity executes policy-based management for the assured implementation and automated update of network/platform configurations, software patches, and hardware upgrades to cybersecurity-enabled components of the IE.
A2.6.2.1 Manage Technology and Infrastructure for Cybersecurity Policy Management	This activity guides and oversees DOD technology initiatives and infrastructure developments focused on development and governance of machine-executable policy and automated lifecycle processes for cybersecurity elements of the IE.
A2.6.2.2 Implement Architecture for Cybersecurity Policy Management	This activity provides the principles and conceptual framework underlying the development and implementation of human-readable and machine executable policies for cybersecurity-enabled components of the IE.

A2.6.2.3 Provide Operational Management of Cybersecurity	This activity implements an enterprise-wide process for the day-to-day operational management of Cybersecurity components of the IE.
A2.7 Tag Data Objects with Cybersecurity Metadata	This activity defines standards and deploys tools and services to enable cybersecurity-relevant metadata tags to be permanently and incorruptibly associated with data objects in the IE.
A2.7.1 Bind Cybersecurity Metadata Tags to Data Objects	This activity develops and deploys a cryptographic binding tool/service to bind data objects to associated cybersecurity metadata tags.
A2.7.2 Develop Cybersecurity Metadata Tagging Standards	This activity manages the development and use of DOD Discovery Metadata Standard (DDMS)-compliant, enterprise-wide, net-centric standards for cybersecurity metadata tags.
A2.8 Manage Mission Assurance	This activity manages processes and procedures coordinating and deconflicting cybersecurity system configuration and resource changes, mission priority changes, and cyber-attack responses to maintain prioritized mission operations and secure IE availability.
A2.8.1 Evaluate Software Assurance	This activity provides guidance and establishes processes and procedures for assessing cybersecurity risk associated with software products used by DOD.
A2.8.2 Evaluate Hardware Assurance	This activity provides guidance and establishes processes and procedures for assessing cybersecurity risk associated with hardware products used by DOD.
A2.8.3 Evaluate System Assurance	This activity provides guidance and establishes processes and procedures for evaluating cybersecurity risk associated with any system made up of components from numerous suppliers.
A2.8.4 Evaluate Supplier Assurance	This activity provides guidance and establishes processes and procedures for assessing cybersecurity risk associated with product suppliers and vendors used by DOD.
A2.9 Manage Globalization Risks	This activity provides oversight and guidance in all areas where DOD information superiority could be adversely impacted by the globalization of information technology and services. Globalization drives change. The immense economic transition that comes with globalization has brought an unprecedented prosperity to the world. ... Opponents will look to the immense global economic machine created for commerce to find new ways to attack. Creating policies that can maintain economic opportunity while managing new risks is one of the most complex challenges that governments face today. [Foreign Influence on Software - Risks and Recourse, CSIS, March 2007]

A3 Provide IE Infrastructure	This activity provides the service-oriented environment and supplies the enterprise-level communications and computing capabilities required to enable net-centric operations and the Enterprise-wide services needed by all users. It provides basic IT elements/components which are foundational to the DOD IE and which enable it to fully support assured information sharing across the Enterprise and with mission partners.
A3.1 Provide Information and Services from the Edge	This activity provides the warfighter and enabling business and intelligence elements with trusted, timely, and assured access to data and services required to fully gain an information advantage in enabling mission accomplishment.
A3.1.1 Provide Enterprise Services	This activity manages service orientation and provides services, including hardware and software, usable across the enterprise and required to meet the needs of the warfighter and enabling business and intelligence elements. Services provided by this activity include, but are not limited to, enterprise directory, discovery, and collaboration services. The activity also provides foundational, back-end services transparent to the user, such as registration, mediation, orchestration and data translation.
A3.1.1.1 Provide Services Infrastructure	This activity provides the support required to manage and operate Enterprise Services across the IE. It includes managing and operating the: (1) federation of services, (2) institutionalization of services, (3) service interfaces, (4) service delivery, and (5) service execution.
A3.1.1.2 Enable Data and Service Separation from Applications	This activity makes data and services accessible and available to the unanticipated user by separating them from the underlying hardware and software applications that deliver them.
A3.1.1.3 Provide Core Services	This activity includes all the tasks necessary to deliver the core services provided by the enterprise. Such tasks include providing functionality that the end user directly uses and back end services necessary for the operation of user services but of which the end user may not be aware. This activity also includes the proper design of a service so that data is provided as a service and services are exposed from existing applications.
A3.1.1.3.1 Provide Service Oriented Architecture Foundation (SOAF) Services	This activity delivers back end services necessary for proper operation of a service-oriented IE. The user is normally unaware of these services or their actions. The SOAF is a loosely-coupled set of services that provide some of the foundational infrastructure for building service-oriented applications.
A3.1.1.3.2 Provide Enterprise Directory Services	This activity maintains a common enterprise directory, leveraging existing enterprise directories across the IE, and makes the content available to all authorized entities.
A3.1.1.3.2.1 Manage Enterprise Directory	This activity supervises the implementation of a comprehensive directory that provides an enterprise-wide source of user information.

A3.1.1.3.2.1.1 Provide Directory Federation	This activity provides the environment which enables the portability of directory information across autonomous domains without the need for redundancy. Directory managers associated with the federation participate in governance, comply with federation requirements, and submit to audits.
A3.1.1.3.2.1.2 Maintain Entity Attributes	This activity maintains in the enterprise directory those attributes associated with an enterprise entity including, but not limited to, classification level, rank, mission, location, nationality, and organization. These attributes are leveraged when defining access privileges.
A3.1.1.3.2.2 Publish Enterprise Directory	This activity exposes the information maintained within the enterprise directory and provides authorized entities the ability to query attribute and other information.
A3.1.1.3.2.2.1 Provide Access to Enterprise Directory	This activity permits authorized entities to locate and use the enterprise directory.
A3.1.1.3.2.2.2 Expose Entity Attributes	This activity responds to queries for attribute and other information maintained in the enterprise directory and exposes the requested data to authorized users.
A3.1.1.3.3 Provide Discovery Services	This activity enables users, to include unanticipated users, to locate and access data, services, and IT resources across the IE.
A3.1.1.3.3.1 Provide Registration Services	This activity maintains registries that make data, services, and other IT resources visible and accessible to users across the IE.
A3.1.1.3.3.2 Provide Search Services	This activity uses available data, service, and IT resource registries and catalogs to search for specific IE components the user desires.
A3.1.1.4 Provide Collaboration Services	This activity includes all the tasks necessary to deliver the services that allow users to interact with one another in the IE. Such tasks include providing messaging services, awareness services, and other collaboration services that foster teamwork, cooperation, and group efforts.
A3.1.1.4.1 Provide Other Collaboration Services	This activity provides portals, shared work spaces, and other similar collaborative environments.
A3.1.1.4.2 Provide Messaging Services	This activity provides services enabling users, both human and machine, to communicate with one another via electronic messages.
A3.1.1.4.3 Provide Awareness Services	This activity delivers services enabling collaboration by allowing users to know and understand the activities, location, and interactions of others involved in the collaboration session. Such services facilitate collaboration by showing information about presence (is anyone in the virtual workspace?), the identity of those present, their actual location(s), their actions, etc.
A3.1.2 Provide End User Services and Applications	This activity provides the mission-unique services and applications required by the warfighter and enabling business and intelligence elements to achieve operational success. In supporting a net-

	centric environment, this activity also ensures the separation of data and services from new and existing end-user applications.
A3.1.2.1 Provide Mission Oriented Applications	This activity develops and delivers mission-specific services and applications required to support warfighting, business, and intelligence functions.
A3.1.2.2 Publish Mission-Oriented Services	This activity advertises the functionality of mission-specific applications and services to all authorized users across the IE, to include external mission partners.
A3.1.3 Enable User Trust and Utility of IE	This activity designs and develops information and services with the warfighter, business, and intelligence user as the primary focus. This includes ensuring the user is provided with the best possible information and services when they are needed, guaranteeing the integrity of the information and services, and supporting the unanticipated user.
A3.1.3.1 Manage Satisfaction of Information and Services Requirements	This activity manages the user experience of the IE, so warfighter, business, and intelligence needs and requirements are satisfied, and feedback received is used to enhance IE functionality.
A3.1.3.1.1 Manage Availability	This activity enables availability of required data and services, so user have access whenever and wherever needed. This activity establishes trust in the robustness of operational data based on user perception of the completeness of available information.
A3.1.3.1.2 Manage Integrity	This activity oversees the protection of data from unauthorized modification or destruction, and the coordination and validation of services maintaining this level of data integrity. This activity manages the integrity of data and services across DOD, as well as with external DOD partners.
A3.1.3.1.3 Manage Authenticity	This activity manages the process by which the origin of information is verified to be sufficiently vetted, accurate, and genuine, to be worthy of user trust. This activity includes the tasks necessary to manage the pedigree of data and services across DOD, as well as with external DOD partners.
A3.1.3.2 Optimize Information and Services from the Edge	This activity provides the warfighter, business, and intelligence user with optimized access to information and services based on location, bandwidth availability, data and service requirements, mission criticality, and other measures at the commander's disposal to optimize the network in his or her battlespace.
A3.1.3.2.1 Manage Communities of Interest (COIs)	This activity oversees COIs established to promote net-centric information sharing. As members of such COIs, users participate in information sharing and collaboration. For each mission, this activity involves: (1) identifying a COI with a similar mission, (2) establishing a COI for the mission if none currently exists with a similar mission, (3) managing the COI in accordance with the

	mission, and (4) participating in the COI to ensure mission success.
A3.1.3.2.2 Provide Common End User Interfaces	This activity manages the development of common end user interfaces facilitating dissemination of information in a manner most beneficial to the warfighter and enabling business and intelligence elements and provision of flexible and agile services to assist in accomplishment of a mission objective.
A3.1.3.2.2.1 Provide Data to Meet End User Needs	This activity uses common interfaces to deliver information, so it is useful and meaningful to the end user.
A3.1.3.2.2.2 Provide Flexible and Agile Services	This activity uses common interfaces in delivering flexible and agile services that are useful and meaningful to the end user.
A3.1.3.2.3 Ensure Supportability of Multiple User Types	This activity enables multiple types of user, to include the unanticipated user, to successfully use information and services in the IE and manages optimization schemes and prioritization rules to allow for unexpected user demands.
A3.2 Provide Joint Infrastructure	This activity enables the implementation of a consolidated, reliable, and seamless infrastructure with computing, connectivity, and communications capabilities across the globe to all IE users. This infrastructure supports the sharing of information from the tactical edge throughout an interconnected IE. It also employs logical means to ensure that an approved level of security separation is always in place.

A3.2.1 Provide Computing Infrastructure	This activity provides the necessary computing infrastructure and related services to allow the DOD to operate according to net-centric principles. It ensures that adequate processing, storage, and related infrastructure services are in place to dynamically respond to computing needs and balance loading across the infrastructure. The activity evolves a unified computing infrastructure from existing Service infrastructures, enabling the consolidation of resources, allowing for seamless information sharing capabilities, and strengthening IT system delivery and integration. All computing infrastructure components are acquired, installed, configured, and evaluated in accordance with national and DOD policy and guidance.
A3.2.1.1 Implement Joint Computing Infrastructure	This activity acquires, installs, integrates, deploys, tests, and accredits computing infrastructure solutions. It evolves the current computing infrastructure to achieve an operational capability ensuring the joint warfighting force has the best IT capabilities, within resource constraints, to enable mission accomplishment and achieve net-centric information sharing goals.
A3.2.1.1.1 Acquire Computing Infrastructure Solution	This activity obtains computing infrastructure solutions. It uses aspects of the DOD decision process to implement the phased acquisition of computing infrastructure-based capabilities. The activity follows established policies and procedures for the Joint Capabilities Integration and Development System (JCIDS) and Business Capability Lifecyle (BCL) and is initiated by identification of a capability need requiring a materiel solution. The solution acquired by this activity is then installed, integrated, deployed, and tested to support its operation for the lifecycle of the solution.
A3.2.1.1.2 Install Computing Infrastructure Solution	This activity conducts the physical installation of an acquired computing infrastructure solution.

A3.2.1.1.3 Integrate Computing Infrastructure Solution	This activity integrates a computing infrastructure solution with other systems in the IE, as required. Integration is greatly facilitated by net-centric engineering of computing infrastructure interfaces.
A3.2.1.1.4 Deploy Computing Infrastructure Solution	This activity configures a computing infrastructure solution, so it attains an operational state at a given physical location.
A3.2.1.1.5 Test and Authorize Computing Infrastructure Solution	This activity manages testing throughout the development and implementation of the computing infrastructure solution and establishes infrastructure testing parameters for Joint Interoperability Test Command (JITC). Testing will include initial concept testing, interoperability testing, unit/module testing, end-to-end system testing, and operational testing. Benchmark testing using representative sets of programs and data designed to evaluate the performance of computer hardware, operating systems, and storage in a given configuration is applied extensively in this activity. The activity also enables the authorization of the solution for operation.
A3.2.1.2 Establish Computing Infrastructure Environment	This activity realizes the various components of the joint computing infrastructure (hardware, system software, data storage, service centers, etc.) to enable net-centric operations.
A3.2.1.2.1 Provide Self-Managing Computing Infrastructure Operations	This activity enables computing infrastructure resources to operate so they are self-managing with a minimum of human awareness or involvement. The activity documents and encourages the use of utilities and self-correcting automated procedures to manage recurring computing and storage functions. The objective is to increase the efficiency, effectiveness, robustness, and productivity of the entire computing infrastructure and its operation.
A3.2.1.2.1.1 Automate Computing Infrastructure Operations	This activity automates CI operations so they can be self-managed with a minimum of human awareness or involvement.

A3.2.1.2.1.2 Enable Automated NetOps Information Reporting in Computing Infrastructure	This activity provides the automated capability for CI resources to collect, process, and report information on their condition and situation as required to enable Network Operations (NetOps) and IE command and control.
A3.2.1.2.1.3 Enable Dynamic, Virtual Processing in Computing Infrastructure	This activity provides an automated capability for dynamically orchestrating and configuring computing infrastructure resources to enable net-centric, virtual data processing across the IE for all component computing, cross-component computing, and authorized users.
A3.2.1.2.1.4 Provide Autonomous CI Environment	This activity enables CI resources to operate with minimal manual administration by use of autonomous processes and machine "learning" that continually integrates best practices and knowledge gained during operations.
A3.2.1.2.2 Provide Hardware Environment	This activity supplies the hardware components that are part of the CI, to include those associated with processor nodes, storage, graphics cards/processors, grid hardware interface components, server architectures, storage area network architectures, and on-the-wire processor devices. The resulting hardware environment is capable of continually evolving in response to operationally (mission) defined capabilities and requirements.
A3.2.1.2.3 Provide Storage Environment	This activity provides storage functions, storage security (access restrictions, data-at-rest encryption), platforms, and architectures for shared space (e.g., storage area networks), and common storage solutions approved by senior managers, CIOs, and Decision Approval Authorities at DOD components and computing centers, e.g., the Defense Enterprise Computing Center (DECC). Shared space is addressed as a mix of persistent (i.e., archived) storage and non-persistent (i.e., cached) storage.
A3.2.1.2.4 Provide System Software Environment	This activity implements all system software including, but not limited to, operating systems, runtime services, resource allocation, and utilities needed to operate the CI.

A3.2.1.2.5 Provide High Productivity Computing Environment	This activity implements, in the computing infrastructure, high productivity computing systems with computational efficiency, reduced development time, interoperability, portability and robustness for improved reliability.
A3.2.1.2.6 Provide Grid Computing Environment	This activity implements a grid computing infrastructure with standards-based, interoperable solutions to enable a distributed, net-centric DOD computing environment. This grid computing environment enables the sharing of computing and information resources across the enterprise in a secure, highly efficient manner, while allowing the distributed DOD computing environment to operate as a uniform service.
A3.2.1.2.7 Provide Computing Infrastructure Services	This activity provides fundamental computing infrastructure capabilities as services, including platform services, operating system and runtime services, shared computing services, and storage services.
A3.2.1.2.7.1 Provide Shared Computing	This activity enables a set of computing infrastructure services that provide the ability to share computing resources.
A3.2.1.2.7.2 Provide Computing Infrastructure Storage Services	This activity enables a set of computing infrastructure services that provide shared data storage.
A3.2.1.2.7.3 Provide Operating System (OS) Services	This activity enables a set of computing infrastructure services that provide operating systems for the IE.
A3.2.1.2.7.4 Provide Runtime Services	This activity enables a set of computing infrastructure services that provide runtime operations.
A3.2.1.2.7.5 Provide Operation Oversight Services	This activity provides services that oversee CI operations and collect and report operations data for review and assessment.

A3.2.1.2.7.6 Assess Computing Infrastructure Requirements and Performance	This activity collects and processes user requirements and CI performance to enable quality of service and service level agreement (SLA) assessments for use in adjusting the operation of the computing infrastructure.
A3.2.1.2.7.7 Provide Application Migration Support	This activity enables the support required to move services and applications between computing infrastructure platforms.
A3.2.1.2.8 Provide COCOM Aligned Service Centers	This activity implements DOD network service centers that are regionally-based and COCOM-aligned. These regional service centers are designed to improve operational control of the networks by each COCOM while optimizing data transport and use. The activity implements industry best practices and standards to enhance security and service availability for each regional service center.
A3.2.1.2.9 Provide Cybersecurity for Computing Infrastructure	This activity applies Information Assurance rules, processes, procedures, and mechanisms to the Computing Infrastructure to achieve confidentiality and integrity.
A3.2.1.2.9.1 Enable Cybersecurity for Shared Storage and Media Functions	This activity enforces policy decisions and enforcement parameters for accessing shared storage and media functions in the Computing Infrastructure.
A3.2.1.2.9.2 Enable Secure Interoperability	This activity applies cybersecurity rules, processes, procedures, and mechanisms to the Computing Infrastructure to enable secure interoperability in facilitating collaboration and information sharing.
A3.2.1.2.9.3 Provide Trusted Computing	This activity applies cybersecurity rules, processes, procedures, and mechanisms to the Computing Infrastructure to consistently enable assured computing.
A3.2.1.3 Provide Computing Infrastructure Controls	This activity enables control mechanisms to manage and administer the computing infrastructure environment.

A3.2.1.3.1 Provide Security Control Mechanisms for CI	This activity implements configuration controls to manage and administer user and machine access, privileges, security mechanisms and performance for the computing infrastructure environment.
A3.2.1.3.1.1 Provide Privilege Controls for CI Resources	This activity implements configuration controls to manage and administer user access privileges for computing infrastructure environment resources.
A3.2.1.3.1.2 Provide Hardware and Operating System Security Configuration Controls	This activity implements configuration controls to minimize vulnerabilities that could be exploited by adversaries in computing infrastructure hardware and operating system resources.
A3.2.1.3.2 Provide Optimization / Performance Controls	This activity provides the controls required to reconfigure computing infrastructure resources in order to maximize overall performance of the computing infrastructure.
A3.2.1.3.3 Parameterize CI Resources	This activity establishes numerical parameters for computing infrastructure resources used in measuring the objective performance of their use.
A3.2.1.4 Maintain Computing Infrastructure	This activity sustains the computing infrastructure, so predictable faults do not occur.
A3.2.1.5 Provide Information on Computing Infrastructure Resources	This activity implements metadata for locating computing infrastructure resources and associated information on those resources needed by a user to determine their availability and access requirements.
A3.2.1.5.1 Provide Computing Infrastructure Metadata	This activity develops metadata describing resources within the computing infrastructure. This metadata includes information on resource functionality, capacity, and location.

A3.2.1.5.1.1 Develop Computing Infrastructure Ontology	This activity establishes the semantic and syntactic structure for computing infrastructure metadata required to locate and use computing infrastructure resources.
A3.2.1.5.1.2 Register Computing Infrastructure Metadata	This activity places metadata describing computing infrastructure resources into a searchable registry.
A3.2.1.5.1.3 Provide Computing Infrastructure Functionality Information	This activity makes information describing the functionality of computing infrastructure resources visible and accessible to authorized users, including unanticipated users.
A3.2.1.5.1.4 Provide Computing Infrastructure Capacity Information	This activity makes information describing the capacity of computing infrastructure resources visible and accessible to authorized users, including unanticipated users.
A3.2.1.5.1.5 Provide Computing Infrastructure Asset Location Information	This activity makes information describing the location of computing infrastructure resources visible and accessible to authorized users, including unanticipated users.
A3.2.1.5.2 Provide Computing Infrastructure Availability and Access Information	This activity exposes information on the availability of and access requirements for computing infrastructure resources.
A3.2.1.5.2.1 Provide Computing Infrastructure Availability Information	This activity informs operational users and Network Operations (NetOps) of the availability of a given computing infrastructure resource.
A3.2.1.5.2.2 Provide Computing Infrastructure Access Information	This activity informs operational users about how to access a given computing infrastructure resource.

A3.2.2 Provide Communications Infrastructure	This activity implements and manages an evolvable transport infrastructure containing adequate bandwidth and access capabilities to meet warfighter, business, and intelligence needs. The activity provides transport functions enabling an end-to-end, seamless net-centric communications capability across all IE assets. It also provides overarching interoperability across the IE and with mission partners, physical connectivity across the globe, and the enablement of Quality of Service (QoS) and secure data transport.
A3.2.2.1 Procure Interoperable Transport Components	This activity manages the procurement of IE communications transport components, so they have standard interfaces and protocols and meet appropriate DOD standards able to provide interoperability between those components and with the components of appropriate external networks (e.g., those of external mission partners).
A3.2.2.2 Standardize Extensions to Other Network Infrastructures	This activity provides an environment where all users, both internal to DOD and external mission partners, can join physical and logical transport systems so that joint and combined/partnered missions can be accomplished in an efficient manner. This activity establishes a pre-determined path for design and implementation of connectivity from DOD networks and systems to non-DOD mission partners, coalition forces, and state and local governments, as required.
A3.2.2.3 Provide Global Connectivity	This activity implements transport infrastructure to enable network connectivity across the globe in response to changing mission priorities and based on commander's intent. It includes the implementation of wired and wireless transport protocol to ensure distributed network connectivity.
A3.2.2.3.1 Provide Wide Area Network (WAN) Connectivity	This activity implements transport infrastructure, including wired and wireless transport, enabling wide area network connectivity to meet the requirements of large fixed sites and enterprise users across the IE.

A3.2.2.3.2 Provide Local Area Network (LAN) Connectivity	This activity implements transport infrastructure, including wired and wireless transport, enabling local area network connectivity to meet the requirements of regionally deployed users and temporary sites across the IE.
A3.2.2.3.3 Provide Ad Hoc Connectivity	This activity implements agile, on-demand network connectivity resources, including wired and wireless transport, needed to support the connectivity requirements of mobile platforms and tactical users (afloat, sub-surface, airborne, in space, and on the ground) across the IE.
A3.2.2.4 Provide Communication Support Mechanisms	This activity implements service prioritization, Quality of Service (QoS), and cybersecurity means to enable high quality and secure transport and availability between IE communications resources.
A3.2.2.4.1 Provide Quality of Service (QoS) Mechanisms	This activity implements communications infrastructure mechanisms ensuring optimal network traffic flow in high-performance computing environments, while at the same time providing service optimization for lower bandwidth requirements at the tactical edge.
A3.2.2.4.1.1 Support Service Level Agreements	This activity manages acquisition standards providing for performance configurability of all IE communication infrastructure components.
A3.2.2.4.1.2 Facilitate Continuity of Communications Service	This activity manages acquisition standards providing an equipment quality sufficient enough to support Reliability, Maintainability, Availability (RMA), redundancy, alternate power, and diminished capacity support (configurability) to provide the highest availability of connectivity and service access across the IE.
A3.2.2.4.1.2.1 Implement Reliability, Maintainability, and Availability (RMA) Standards	This activity provides interoperability standards for reliability, maintainability, and availability to direct the acquisition of the communications infrastructure.

A3.2.2.4.1.2.2 Enable System Redundancy	This activity provides for the collaboration of architectural designs, so they incorporate systemic redundancy in the communications infrastructure to minimize the possibility of extensive transport outages.
A3.2.2.4.1.3 Follow Precedence Policies	This activity provides a transport infrastructure enabling Precedence and Preemption (P&P) based configurations.
A3.2.2.4.2 Enable Security Mechanisms	This activity provides a means by which network assets and/or users are segregated by COI's set up to protect the network infrastructure from a group or groups of users who may represent an internal threat and from entities representing external threats.
A3.3 Evolve IE	This activity manages incremental adjustments to the IE in accordance with DOD plans in order to meet changing operational and environmental requirements and incorporate technology advances.
A3.3.1 Evolve Computing Infrastructure	This activity manages incremental adjustments to the computing infrastructure in accordance with DOD plans in order to meet changing operational and environmental requirements and incorporate technology advances.
A3.3.1.1 Enhance Computing Infrastructure with New Technology	This activity assesses projected advances in technology and performs research and development to determine the feasibility of incorporating new technology solutions into the computing infrastructure to improve capability and pro-actively address changing requirements and environments across the DOD enterprise.
A3.3.1.1.1 Develop Technology Forecast	This activity projects advancements in technology for use in assessing the feasibility of incorporating such advancements into the computing infrastructure.

A3.3.1.1.2 Conduct Research and Development	This activity performs research and development to determine and recommend potential changes to computing infrastructure to incorporate changes in technology and address evolving DOD needs.
A3.3.1.1.3 Assess Changes to Computing Infrastructure	This activity evaluates technology forecasts and the results of research and development efforts to determine their applicability to the computing infrastructure in meeting evolving DOD requirements.
A3.3.1.2 Develop Transition Plans for Computing Infrastructure	This activity builds transition plans to implement new technology solutions meeting evolving computing infrastructure requirements.
A3.3.2 Evolve Communications Infrastructure	This activity facilitates the incorporation of present and future technology upgrades and innovations with an acceptable maturity level into the communications infrastructure while identifying and reusing existing or replacing obsolete systems. It manages the monitoring and testing of new Commercial Off-the-Shelf (COTS) products to support legacy communications systems while improving and evolving the transport infrastructure.
A3.3.3 Evolve Network Operations (NetOps) Capabilities	This activity adapts and evolves NetOps capabilities in time-phased increments that are consistent with defined IE capability increments enabling a structured and consistent transition to net-centric operations.

A4 Control and Operate the IE	This activity provides integrated Network Operations (NetOps) – Enterprise Management, Content Management, and Network Defense – enabling information and service access and use by any IE user across network and security domains. It monitors the status and health and directs the operation of IE resources in support of successful accomplishment of joint warfighting, business, and intelligence missions. The activity enables the coordination and cooperation (at all levels and across all DOD components) of supporting commanders with a single commander tasked with responsibility for operation and defense of the IE. This activity controls the IE to enable the continuous ability to easily access, manipulate, and share any information, from any location at any time. It enforces policies and establishes and implements priorities necessary to operate and defend the IE. It implements common processes and standards governing the operations, monitoring, and defense of IE resources.
A4.1 Establish Commander's Intent for NetOps	This activity determines the Commander's Intent for Network Operations (NetOps), to include objectives, priorities, roles and responsibilities, and rules and constraints to be met, based on the operational situation and mission needs. It then develops an overarching strategy for operating and defending the IE and its information to achieve this intent, as a prelude to NetOps planning. The activity develops, promulgates, and monitors the Commander's Intent for NetOps and provides the leadership and broad direction required for effective operation and defense of the IE as a unified and agile information enterprise supporting all assigned missions.

A4.1.1 Develop Commander's Intent for NetOps	This activity assesses user requirements and the operational situation to establish an overall intent for NetOps to use in guiding and directing the availability, delivery, and protection of the IE to achieve that intent.
A4.1.2 Communicate Commander's Intent for NetOps	This activity advertises the Commander's Intent for NetOps to all operators across DOD and external mission partners, as applicable.
A4.1.3 Monitor Accomplishment of Commander's Intent for NetOps	This activity establishes metrics and measures and uses them to determine how well the operation of the IE is meeting the Commander's Intent. The objectives, priorities, roles and responsibilities, rules and constraints of NetOps must be in accordance with the Commander's Intent to encourage a unified and agile IE.
A4.2 Exercise Operational Control of IE Through NetOps	This activity develops and uses an operational framework, consisting of essential tasks, Situational Awareness (SA), and command and control (C2), to operate and defend the IE and enable information superiority for warfighter, business, and intelligence elements. The essential tasks performed are Enterprise Management, Network Defense, and Content Management. Exercising NetOps responsibilities inherent in these essential tasks produces the desired effects of: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery in support of the overall goal of providing the right information to the edge. This activity also develops, selects, coordinates, and directs responses to deal with immediate events, including natural disaster recovery, effecting the IE situation in support of Commander's Intent.

A4.2.1 Manage IE Situational Awareness	This activity oversees the development and use of information providing situational awareness of IE resources. It provides authorized users, operators, and commanders at all levels with accurate and timely information enabling a shared understanding of the health and mission readiness of the overall IE.
A4.2.1.1 Produce IE Situational Awareness Information	This activity processes, analyzes, and displays data describing the current situation of IE resources to provide authorized users with accurate information on the health and mission readiness of the IE and its operational status and performance.
A4.2.1.1.1 Process IE Situational Awareness Data	This activity performs initial analysis of collected situational awareness data as a first step towards establishing the health and mission readiness of IE resources.
A4.2.1.1.2 Create Tailorable Visualizations	This activity develops a user definable operational picture (UDOP) of the IE situation based on processed IE Situational Awareness data.
A4.2.1.2 Collect Situational Awareness Data	This activity uses automated and autonomous means to collect data from individual IE resources for use in determining the overall situation, status, health, and readiness of the IE.
A4.2.1.3 Report IE Situational Awareness	This activity makes IE Situational Awareness information available and known to all authorized users, to include unanticipated users. Users are made aware of the current health and mission readiness of the IE and its resources to enable the timely and accurate distribution of operationally significant information across the DOD enterprise.
A4.2.1.3.1 Publish IE Situational Awareness Information	The activity provides the tools, standards, and procedures required to make IE Situational Awareness information available and accessible across DOD.
A4.2.1.3.2 Subscribe to IE Situational Awareness Information	This activity provides the ability for authorized users to register to receive specific IE Situational Awareness information as soon as it becomes available.

A4.2.1.3.3 Advertise IE Situational Awareness Information	This activity makes IE Situational Awareness information visible to and discoverable by all authorized users, to include unanticipated users.
A4.2.1.3.4 Facilitate Assured Access to IE Situational Awareness Information	This activity controls access to information regarding the health and readiness of the GIG, providing authorized users with the ability to obtain such information without the need to know its exact location; its format; a specific query language to find the information; or the details of ownership, access controls, and protocols.
A4.2.1.3.4.1 Manage Access to IE Situational Awareness Information	This activity enforces access control policy to enable authorized users to obtain IE situational awareness information. The activity: (1) retrieves and validates input needed to make an authorization decision, (2) evaluates these inputs with respect to the appropriate access policy and makes an authorization decision regarding the information asset requester, and (3) distributes the resulting authorization decision.
A4.2.1.3.4.2 Create/Maintain Shared Space for IE Situational Awareness Information	This activity provides the shared data and information storage required to enable the visibility, accessibility, and sharing of NetOps information within the DOD and with DOD mission partners, as appropriate.
A4.2.2 Respond to IE Situation	This activity provides an executed response to a given event or situation occurring in the IE. The response will be one agreed to by the appropriate Combatant Command(s)/Military Service(s)/Agency(is) (CC/S/As), and will support the needs of the appropriate warfighter, business and intelligence elements, US Cyber Command (USCYBERCOM), and the DOD NetOps community. The executed response will conform to appropriate technical and operational standards related to the event or situation.

A4.2.2.1 Develop Response to IE Situation	This activity reviews and analyzes IE situational awareness information and establishes recommended responses to an event or situation occurring in the IE. NetOps is responsible for overall management, control, and technical direction for all designated responses to IE events/situations.
A4.2.2.2 Select Response to IE Situation	This activity picks the appropriate response to an IE event or situation from those previously developed through a collaboration process involving DOD components and partners and supporting the needs of warfighter, business, and intelligence operations, USCYBERCOM, and the overall NetOps community.
A4.2.2.3 Coordinate Response to IE Situation	This activity synchronizes the selected response to an IE event or situation across the relevant DOD CC/S/As and mission partners to enable the needs of warfighter, business, and intelligence operations, USCYBERCOM, and the overall NetOps community.
A4.2.2.4 Execute Response to IE Situation	This activity carries out the response to an IE event or situation agreed to by the relevant CC/S/As, while supporting the needs of the mission areas, USCYBERCOM, and the overall NetOps community.
A4.2.3 Conduct Enterprise Management of IE	This activity monitors, controls, and operates the functional capabilities and operational processes required to manage the availability, allocation, and performance of IE resources across the DOD enterprise. Enterprise management includes the performance of Enterprise Service Management, Applications Management, Computing Infrastructure Management, Network Management, Satellite Communications Management, and Electromagnetic Spectrum Management.
A4.2.3.1 Allocate IE Resources	This activity analyzes past and present IE performance data, plans for IE resource needs, and dynamically assigns resources (both physical and logical) to meet the requirements of IE users.

A4.2.3.1.1 Allocate Communications Infrastructure Resources	This activity analyzes past and present communications infrastructure performance data, plans for communications resource needs, and dynamically assigns communications resources (both physical and logical) to meet the requirements of IE users.
A4.2.3.1.1.1 Plan Communications Resource Allocation	This activity develops plans, based on historical data, describing how transport infrastructure elements are to be allocated to enable operations.
A4.2.3.1.1.2 Support Surge Loading	This activity allocates, based on historical data, enough bandwidth (i.e., communications capacity) to support critical surges in requirements resulting from added users, changes in missions/operations, or the addition of new services.
A4.2.3.1.1.3 Support Multiple Military Operations	This activity provides enough provisional bandwidth (i.e., communications capacity), based on historical data, to support new theater operations, addition of mission elements, or new deployments.
A4.2.3.1.1.4 Support Day-to-Day Operations	This activity maintains sufficient bandwidth (i.e., communications capacity) to end-points, based on historical data, to support ordinary daily operations.
A4.2.3.1.1.5 Allocate Electromagnetic Spectrum	This activity assigns a Radio Frequency (RF) for mission support based on electromagnetic communication and interoperability needs, and frequency availability (by location)
A4.2.3.1.1.5.1 Optimize Spectrum Use	This activity employs technological means to determine and implement the best use of available and compatible electromagnetic frequencies based on mission requirements and location with use of policy and regulatory guidance.
A4.2.3.1.1.5.2 Enable RF Communications with Mission Partners	This activity coordinates spectrum uses with external partners, enabling their systems to have RF connectivity to access IE resources.

A4.2.3.1.1.6 Manage Satellite Communications (SATCOM)	This activity performs the day-to-day operational management of all apportioned and non-apportioned Satellite Communications (SATCOM) resources. It provides appropriate support when disruption of service occurs; reports on global SATCOM system status; maintains global Situational Awareness of SATCOM assets, to include those supporting each Combatant Command's (COCOM's) current and planned operations, as well as Space, Control, and Terminal Segment asset and operational configuration management; manages resolution of radio coordinates resolution of radio frequency interference; performs satellite anomaly resolution and management; and manages and resolves SATCOM interference within the IE.
A4.2.3.1.2 Allocate Computing Infrastructure Resources	This activity adjusts the assignment of computing infrastructure resources to support changing workloads while ensuring agreed to performance levels are met.
A4.2.3.1.2.1 Allocate Computing Resources	This activity adjusts available computing resources to support changing workloads while ensuring agreed to performance levels are met.
A4.2.3.1.2.1.1 Allocate Shared Computing Resources	This activity adjusts shared computing resources in the IE to support changing workloads while ensuring agreed to performance levels are met.
A4.2.3.1.2.1.2 Allocate Processing Resources	This activity adjusts available processing resources to support changing workloads while ensuring agreed to performance levels are met.
A4.2.3.1.2.1.3 Allocate Operations Across Hardware Resources	This activity spreads operations across the computing infrastructure to ensure agreed to performance levels are met.
A4.2.3.1.2.2 Allocate Storage Resources	This activity adjusts data storage across the computing infrastructure to ensure agreed to performance levels can be met.
A4.2.3.1.2.3 Allocate Network Interfaces	This activity adjusts network interfaces across the computing infrastructure to ensure agreed to performance levels can be met.

A4.2.3.1.2.4 Allocate Physical Facilities	This activity adjusts physical facilities across the computing infrastructure to ensure agreed to performance levels can be met.
A4.2.3.2 Perform System Administration	This activity conducts day-to-day operations and maintenance of the IE. This includes, but is not limited to, performing routine audits of systems and software, conducting backups, and maintaining a help desk.
A4.2.3.3 Provide Change Management	This activity puts the proper procedures and methods in place for efficient management of IT infrastructure changes across the IE. This includes implementing an effective Continuity of Operations Plan (COOP) to ensure network outages resulting from natural or man-made disasters are minimized.
A4.2.3.4 Provide Configuration Control	This activity manages and administers individual configuration items across the IE. It provides enterprise-wide solutions for the assured implementation, update, and management of network/platform configurations, software patches, and hardware upgrades of IE components. It ensures all deployed devices and mechanisms incorporate approved features, functions, capabilities, and settings necessary to support their intended mission. This includes security critical versions, patches, interface standards, lifecycle configuration, mode and option settings, and cryptologic algorithms, where appropriate.
A4.2.3.5 Perform Tech Refresh	This activity provides technical updates to IE components as these updates become available to ensure the IE is up-to-date with current technological standards.
A4.2.3.6 Perform Patch Management	This activity executes processes and oversight to deploy patches throughout the IE in order to effectively fix glitches, update systems and policies, and improve Computer Network Defense (CND).

A4.2.3.7 Manage IE Performance	This activity provides mechanisms required to measure and administer the performance of users and resources in the IE. It applies a variety of mechanisms to achieve varying levels of service quality. Such mechanisms may focus on data availability, priorities of service (e.g., processing node cycles devoted to a particular operating system or application call), or on the processing of storage fetches and puts.
A4.2.3.7.1 Develop and Apply IE Performance Metrics	This activity implements metrics for use in assessing, managing, and administering the performance of users and resources in the IE.
A4.2.3.7.2 Assess Performance of IE Resources	This activity uses developed metrics to evaluate the performance of users and resources in the IE and compare this performance to service level agreements (SLAs).
A4.2.3.8 Measure IE Effectiveness	This activity determines, evaluates, and generates reports on the effectiveness of the IE in terms of operational mission support and its ability to meet the Commander's Intent for NetOps.
A4.2.3.8.1 Measure Operational Effectiveness of NetOps	This activity determines, in coordination with the overall NetOps Community, the effectiveness of NetOps in operating and defending the IE to deliver information superiority.
A4.2.3.8.2 Measure Strategic Effectiveness of IE	This activity determines the strategic effectiveness of the IE based on goals and objectives described by USCYBERCOM for NetOps and evaluates how well the IE provides net-centric capabilities across strategic, operational, and tactical boundaries in enabling DOD's full spectrum of warfighting, business, and intelligence missions.
A4.2.4 Conduct Network Defense	This activity enables the functional capabilities and operational processes required to protect and defend the IE, to include the conduct of Computer Network Defense (CND), associated Response Actions, and Critical Infrastructure Protection.

A4.2.4.1 Provide Security Monitoring, Vulnerability Analysis, and Threat Identification	This activity establishes and executes security monitoring protocols, conducts system vulnerability assessments, provides proactive threat identification and analysis, and implements Information Assurance Vulnerability Alert (IAVA) policy fortifying IE computing infrastructure and protecting IE resources.
A4.2.4.2 Perform Threat/ Incident Management	This activity monitors and detects security events, conducts timely and effective assessment of risks, streamlines existing assurance processes, encourages the use of best practice solutions and test methods on a computer or computer network, and executes proper responses to any events that increase vulnerabilities and invite new threats across the unified IE.
A4.2.4.3 Provide Critical Infrastructure Protection (CIP)	This activity implements a DOD risk management program that seeks to ensure the availability of networked assets critical to DOD missions. CC/S/As and field activities coordinate their CND activities and implement procedures IAW DODI O-8530.2, Joint Concept of Operations (CONOPS) for the GIG NetOps and DOD-wide operational direction and guidance issued by CDRUSSTRATCOM. Sub-activities include the identification, assessment, and security enhancement of assets essential for executing the National Military Strategy.
A4.2.4.4 Issue Information Assurance & Vulnerability Assessment (IAVA) Task Orders	This activity develops and executes task orders invoking compliance with IAVA security protocols.

A4.2.5 Perform Content Management	This activity provides the functional capabilities and operational processes necessary to monitor, manage, and facilitate the visibility and accessibility of information (which includes data and knowledge) within and across the IE. It also optimizes the use of information distribution capabilities to enable timely and accurate sharing of information across the IE.
A4.2.5.1 Prioritize Information Resources	This activity prioritizes processing, communications, and storage resources for use in allocating these resources to optimize information sharing performance in response to changing operational demands. This activity also pro-actively determines information exchange resource needs for use in dynamically adjusting infrastructure to address rapidly changing operational requirements. It establishes longer range requirements for planned growth of the IE to enable logical, phased expansion and extension in improving information superiority for IE users.
A4.2.5.2 Optimize Information Infrastructure Use	This activity directs the allocation of processing, communications, and storage in order to optimize information sharing performance in response to changing user demands and operational needs.
A4.2.5.3 Monitor Information Delivery	This activity tracks and evaluates the use of the IE information distribution infrastructure to ensure timely and accurate information delivery.
A4.3 Plan IE NetOps	This activity generates NetOps requirements from operational mission needs, then develops, coordinates, and implements operational plans for NetOps.
A4.3.1 Determine NetOps Requirements	This activity traces and decomposes NetOps requirements from operational mission needs.

A4.3.2 Develop NetOps Plans	This activity plans and rapidly re-plans for NetOps operations, including the managing of end-to-end configurations and allocation of IE resources. It provides time lines and Joint Tactics Techniques and Procedures (JTTPs) for NetOps to be able to anticipate changing situations and proactively respond as necessary.
A4.3.3 Coordinate NetOps Plans	This activity coordinates NetOps plans with stake holders within supported and supporting organizations to ensure the operations, defense, and employment of the planned capabilities will support planned missions in a coherent manner.
A4.3.4 Implement NetOps Plans	This activity executes NetOps operations in accordance with established plans and conducts re-planning in preparation for unanticipated changes in missions and the IE situation.
A5 Use the IE	This activity enables an authorized user to access the IE and use its functionality to easily discover information, services, and applications, regardless of location, and to assess and critique information, services, and applications based on specific needs in order to improve IE capabilities and service. In support of operations, the activity also enables the user to collaborate with others and share information produced.
A5.1 Locate and Use Information, Services and Applications	This activity enables a user to discover, request, verify, use, and rate information, services, and applications across the IE.
A5.1.1 Discover Information, Services, or Applications	This activity enables users to find information, services, and applications either reactively (through means such as "Google-like" searches, etc.) or proactively (through means such as Rich Site Summary (RSS) feeds, smart-push capabilities, etc.). Discovery is not dependent on knowing beforehand of the existence of such information, services, and applications.

A5.1.1.1 Reactively Discover Information, Services, and Applications	This activity provides the means for users to discover information, services, and applications using reactive methods, such as "Google-like" searches.
A5.1.1.2 Proactively Discover Information, Services, and Applications	This activity allows users to discover information, services, and applications through proactive means such as Rich Site Summary (RSS) feeds, smart-push capabilities, etc.
A5.1.2 Establish Authenticity of Discovered Information, Services, or Applications	This activity uses authentication processes, procedures, and services to determine if the discovered information, services, or applications are genuine. This requires authentication of the information, services, or applications through an authentication service which: (1) validates the authentication request of a requested service, (2) verifies the credentials of the requested service, and (3) makes an authentication decision for the requested service.
A5.1.3 Assess Utility of Discovered Information, Services, or Applications	This activity enables an IE user (warfighter, business, or intelligence) to assess and provide feedback on the information, services, or applications he or she uses, providing input from the tactical edge to influence the improvement of IE information and services.
A5.2 Share Information	This activity enables IE users (warfighter, business, intelligence) to share information (which includes data and knowledge) through metadata tagging and posting of information and collaborate with peers via both structured and ad-hoc user groups.
A5.2.1 Post Information	This activity enables an authorized user, or a service acting on the user's behalf, to (1) make an information asset visible, accessible, and available on the IE, and (2) make the information asset discoverable and understandable by making metadata on the information asset visible, accessible, and available on the IE.

A5.2.2 Collaborate	This activity provides a collaborative environment to increase the IE user's information advantage through information sharing and social networking. Collaboration can take place within structured Communities of Interest (COIs) and/or ad-hoc user groups.
A5.2.2.1 Participate in Real-Time Collaboration	This activity enables a user to collaborate with others via real-time, synchronous collaboration tools. These tools include, but are not limited to, instant messaging, tele-conferencing, and video chat.
A5.2.2.2 Participate in Non-Real-Time Collaboration	This activity enables a user to collaborate with others via non-real-time, asynchronous collaboration tools. These tools include, but are not limited to, email, wikis, blogs, and forums.
A5.3 Maintain IE Proficiency	This activity provides the means to measure user proficiency with the IE and conduct joint training to maintain and/or improve that proficiency. The activity provides guidance to the combatant commander on IE requirements in the Joint Training System when implementing CJCS policy for developing Joint Mission Essential Task List (JMETL) and Agency Mission Essential Task List (AMETL) planning and when conducting joint training and assessing command readiness with regard to joint capabilities.
A5.3.1 Identify Mission Capability Requirements for IE Proficiency	This activity determines the required functions (Phase 1-Requirements) of all echelons involved with accomplishing the mission regarding IE use. The JMETL, which defines the command's mission capability requirements, will then include the appropriate IE proficiency tasks.

A5.3.2 Develop Common Training Plan for IE Proficiency	This activity establishes a standard training plan and process for maintaining IE proficiency. This standard training plan will then be used in the production of Joint Training Plans (JTP) and Agency Training Plans (ATP) (Phase 2-Plans) which are based on IE capability requirements identified in the JMETL and AMETL and provide commander's guidance and a comprehensive Plan of Action (POA) to link common IE assessment derived training requirements with training events to accomplish training audience objectives.
A5.3.3 Execute Common Training Plan for IE Proficiency	This activity conducts the events (Phase 3-Execution) planned in the JTP/ATP's and evaluates the training audience performance in the events relative to specified training objectives for IE proficiency.
A5.3.4 Assess Training Performance	This activity (Phase 4- Assessment) determines how well an organization or entity can meet the appropriate standard for IE proficiency, how well each user is trained on IE use, and whether a user can use the IE to enable the missions the command is trained to accomplish. This assessment serves as the basis for planning additional or remedial training.

5.3 Services Definitions

Table 7: Services Definition (AV-2)

Service Name	Service Definition
S0 DOD Information Enterprise Services	Service provided to the DOD that execute sets of required functionalities around the provisioning of information resources, assets, and processes, and that enables the execution of Defense IE Capabilities.
S1 Connect, Access, and Share Services	The set of services that provides the functionality for user to find, access, provide, share, process and manage information and other services.
S1.1 Connect Services	The set of services that provides the functionality required for computing and communications infrastructure.
S1.1.1 Commercial Satellite Communication Services	This service provides telecommunications through the use of communications satellites to receive signals from antennae on the Earth's surface, or from other satellites, amplify the signals, and beam them back to Earth.

S1.1.2 IP Based Networking Services	This service group provides for the seamless transmission of information (voice, video, or data) by using the set of communication protocols used for the Internet and other similar networks.
S1.1.2.1 Video over IP Services	This service provides for the execution of video teleconferencing over broadband Internet connections. This also includes Video over Secure Internet Protocol.
S1.1.2.2 Voice over IP Services	This service provides for the execution of voice calls over broadband Internet connections. This also includes Voice over Secure Internet Protocol (VoSIP).
S1.1.2.3 VPN Services	This service provides remote offices or traveling users access to a central organizational network through a public telecommunication infrastructure, such as the Internet.
S1.1.2.4 Ad Hoc Network Services	This service provides the ability to deploy and install ad hoc networks in support of mission needs, regardless of geographical location.
S1.1.3 Video Teleconferencing Services	This service provides the capability to operate (schedule, facilitate) and maintain common-user VTC Studios to include interface access for VTC and secure telephone equipment. These services also include design and installation advice and technical support.
S1.1.4 Wireless Communication Services	This service provides communications via radio frequency, microwave, infrared (IR), or other methods that transfer information without the use of wires.
S1.1.5 Wired Communication Services	This service enables the transmission of data over a wire-based communication technology, typically via telephone lines, cables, and fiber-optic communication.
S1.1.6 Computing and Data Storage Services	This service provides the ability to compute, process, and control information within the network to support client services at the edge of, and throughout the network. Subcategories include server computing, production, mass storage, and web hosting.
S1.1.6.1 Storage on Demand Services	This service provides for the centralized storage of data. This includes the execution of periodic data back-up to safeguard against data loss as a result of catastrophic events.
S1.1.6.2 Computing on Demand Services	This service provides computing resources to DOD enterprise users on an as-needed basis.
S1.1.7 End User Device Services	This service provides end user computing devices and the management of those devices.
S1.2 Access Services	The set of services that provide the functionality required to grant or deny available information assets to human and machine users.
S1.2.1 Access Control Services	This service provides a way of authenticating and authorizing users to gain access to web applications and services while allowing the features of authentication and authorization to be factored out of the application code. This provides users the

	benefit of being able to log in to multiple applications with a reduced number of authentications, and in some cases only one authentication.
S1.2.2 Identification and Authentication Services	This group of services manage identities, access rights, and entitlements. These services include user provisioning, passwords, single sign-on, access control, and synchronization of user information across directories.
S1.2.2.1 Identity Management Services	This service provides the ability to identify individuals, and devices, authorized to access an information system and controls the access to the resources in that system by placing restrictions on the established identities.
S1.2.2.2 Attribute Management Services	This service provides the ability to distribute DOD person, persona and personnel attributes to applications and services in a controlled, consistent, and secure manner.
S1.2.2.3 Credential Management Services	This service provides the functionality required to provide network entry points and monitor authentication information changes.
S1.2.2.4 Authentication Management Services	This service includes measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual or device authorization to receive specific categories of information.
S1.2.3 Directory Management Services	This service includes a shared information infrastructure for locating, managing, administering, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects.
S1.3 Share Services	The set of services that provide the functionality required to enable information and information assets to be used within and across mission areas.
S1.3.1 Content Management Services	This service enables the collection, managing, and publishing of information in any form or medium.
S1.3.1.1 Content Discovery Services	This group of services provides a means by which users and applications can find data and services on the GIG, such as through catalogs, registries, and other search services.
S1.3.1.2 Content Delivery Service	This service supports the efficient delivery of mission critical information and products to the warfighter.
S1.3.2 Information Management Services	This service provides the functionality to support the planning, budgeting, manipulating, and controlling of information throughout its life-cycle (e.g., creation or collection, processing, dissemination, use, storage, and disposition).
S1.3.2.1 Information Sharing Services	This group of services enable secure, seamless information management and collaboration across information or security domains and provides a full suite of secure sharing solutions for collaboration across networks, enclaves and COIs and with mission partners.

S1.3.2.2 Cross Domain Services	This service provides high assurance guard systems to bridge disparate information domains and a robust and secure architecture within which guards are operated.
S1.3.3 Enterprise Collaboration Services	This service allows individuals and commands to effectively coordinate data, ideas, and processes at local, regional, and enterprise levels.
S1.3.3.1 Enterprise Email Services	This service provides access to email from DOD data centers through the network rather than from local email servers at each installation.
S1.3.3.2 Social Networking Services	service provided to the DOD that execute sets of required functionalities around the provisioning of information resources, assets, and processes, and that enables the execution of Defense IE Capabilities.
S1.3.3.3 Instant Messaging Services	This service provides the exchange of text messages in real time between two or more people logged into an instant messaging (IM) service.
S1.3.4 Standard Web Office Application Services	This service provides access to applications that reside on networked computers to support users in the performance of job-related tasks. Software applications include commercial off the shelf and government owned solutions.
S1.3.5 Custom Application Services	This service provides a computer program designed for a specific task or use is made according to the specifications of an individual purchaser.
S1.3.6 Cloud Computing Services	This group of services provides shared resources, software, and information to computers and other devices over a network (typically the Internet).
S1.3.6.1 Software as a Service	This service delivers software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support.
S1.3.6.2 Infrastructure as a Service	This service provides computer infrastructure (servers, software) as a service, along with storage and networking.
S1.3.6.3 Platform as a Service	This service provides a computing platform and/or solution stack as a service and facilitates deployment of applications in the cloud.
S1.3.7 Language Translation Services	This service provides analysis of a source text in one language and produces a translated text in a target language without human intervention.
S1.3.8 Audit Services	This service provides the ability to perform an evaluation of a person, organization, system, process, enterprise, project or product in order to ascertain the validity and reliability of information and to provide an assessment of a system's internal control.
S2 Operate and Defend Services	The set of services that provides the ability to ensure IE networks, services, and underlying physical assets can be

	dynamically allocated and configured, and data and services are secured and trusted across DOD.
S2.1 Operate Services	The set of services that provide the functionality required to support real-time situational awareness, protection, and operational management of the IE.
S2.1.1 Change Management Services	The ability to automatically disseminate and implement configuration changes to networks, data assets, services, applications, and device settings in conformance with standard configuration processes.
S2.1.2 Virtual Test Platform Services	This service provides the functionality required to provide a virtualized platform for testing new software.
S2.1.3 Common Development Platform Services	This service provides the functionality needed for an integrated development environment.
S2.2 Defend Services	This set of services that provides the functionality required to ensure data and services are secured and trusted across DOD.
S2.2.1 Security Metadata Management Services	This service provides the ability to mark a data asset to accurately reflect the security classification or sensitivity guidance required (e.g., classification, dissemination controls, releasability, declassification) so that it can be identified and inform authorization and dissemination decisions.
S2.2.2 Information Assurance Management Services	This service enables the protection and defense of information systems by ensuring the confidentiality, availability, integrity, authentication, and non-repudiation of the information and supporting systems.
S2.2.3 Cryptography Management Services	This service provides the ability to encrypt and decode information transmissions.
S3 Govern Services	The set of services that provides the functionality needed to support policy and oversight for the development, deployment, use, and overall management of the IE.
S3.1 Processes and Models Services	The set of services that enable the provision of procedures and tools to support the analysis IE management.
S3.2 Standards and Policy Services	The set of services that provides the functionality required to identify patterns and provide strategic direction to interoperability across DOD.
S3.2.1 Digital Access Policy Management Services	This service provides policy automation to Access Control Policy, Spectrum Management Policy, Security Policy, Network Policy, Configuration Policy, Export Control Policy, etc.
S3.3 Monitoring and Compliance Services	The set of services that provides the ability to enable effective oversight of the development, deployment, and use of the IE.

5.4 Acronym List

Table 8: Acronym List

Acronym	Definition
AAP	Automated Account Provisioning
ABAC	Attribute-Based Access Control
ACL	Access Control List
API	Application Programmability Interface
AI	Artificial Intelligence
BGP	Border Gateway Protocol
BYOAD	Bring Your Own Authorized Device
CASB	Cloud Access Security Brokers
CAC	Common Access Card
CCIRs	Commanders Critical Information Requirements
CDS	Cross Doman Solution
CIO	Chief Information Officer
CMFA	Continuous Multi Factor Authentication
COP	Common Operating Picture
CRL	Certificate Revocation List
CSP	Credential Service Provider
CSRC	Computer Security Resource Center
CV	Capability Viewpoint
DAAS	Data, Applications, Assets, Services
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DOD	Department of Defense
DODAF	DOD Architecture Framework
DODIN	DOD Information Networks

DRM	Data Rights Management
DRP	Disaster Recovery Plan
ECA	External Certification Authority
EDIPI	Electronic Data Interchange Person Identifier
IaaS	Infrastructure as a Service
IAL	Identity Assurance Level
IA TA	Information Assurance Technical Authority
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
IdP	Identity Provider
IE	Information Enterprise
IEA	Information Enterprise Architecture
IoT	Internet of Things
IP	Internet Protocol
ISCM	Information Security Continuous Monitoring
IT	Information Technology
JIE	Joint Information Environment
LAN	Local Area Network
MFA	Multi-Factor Authentication
MNIS	Multi-National Information Sharing
MOA	Memorandum of Agreement
MPLS	Multi-Protocol Layer Switching
MPR	Mission Partner Registration
MUR	Master User Record
NETCONF	Network Configuration Protocol
NGO	Non-Governmental Organizations
NIPRNET	Non-classified Internet Protocol Router Network

NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security System
OCCI	Open Cloud Computing Interface
OCSP	Online Certificate Status Protocol
OCONUS	Outside the Continental United States
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OV	Operational Viewpoint
PAM	Privilege Access Management
PDP	Policy Decision Point
PDR	Person Data Repository
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RA	Reference Architecture
RADIUS	Remote Authentication Dial in User Services
REST API	Representational State Transfer Application Program Interface
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SIEM	Security Information and Event Management
SDC	Software Defined Compute
SDN	Software Defined Network
SDS	Software Defined Storage

SDDC	Software Defined Data Center
SIPRNET	Secret Internet Protocol Router Network
SNMP	Simple Network Management Protocol
SOAR	Security, Orchestration, Response & Automation
SSH	Secure Shell
TLS	Transport Layer Security
USCYBERCOM	US Cyber Command
USM	User-based Security Model
VPN	Virtual Private Networks
WAC	Wireless Access Control
WAN	Wide Area Network
ZT	Zero Trust
ZTA	Zero Trust Architecture

APPENDIX A: CAPABILITY TAXONOMY & DESCRIPTIONS (CV-2)

Table A-1: Capability Taxonomy and Descriptions (CV-2)

ID	Zero Trust Capability Name	Zero Trust Capability Definition (CV-2)
Z1	**User**	**A Zero Trust user is any person, entity or service attempting to gain access to a system, resource or service to which, by default, from inside or outside the network, authentication and authorization is required in order to gain access to that resource on the network. Identity is an attribute or set of attributes that uniquely describe a subject within a given context.**
Z1.1	Authentication	The ability to verify the identity of a user, often as a prerequisite to allowing access to a system's resources.
Z1.2	Authorization	The ability to grant or deny device access to data, assets, applications, or services after a prerequisite check.
Z1.3	Privileged Access Management (PAM)	The ability to secure, control, and manage privileged access on critical assets and applications.
Z2	**Device**	**Any hardware or software that access applications, services or data, including desktop and laptop computers, smartphones and tablets**
Z2.1	Authentication	The ability to verify the identity of a process or device, often as a prerequisite to allowing access to a system's resources.
Z2.2	Authorization	The ability to grant or deny user access to data, assets, applications, or services after a prerequisite check.
Z2.3	Compliance	The ability to validate associated policies on endpoints to include mobile devices, laptops, desktop PCs, servers, and hardware within data centers
Z3	**Network/Environment**	**Physical and virtual resources that support the flow, storage, processing and analysis of data. These can include on premise or remote systems.**
Z3.1	Software-Defined Networking (SDN)	The ability for software to provision and manage network configurations on programmable infrastructure such as routers, switches, and firewalls.

Z3.2	Macro Segmentation	The ability to segment traffic on the network using broad categories. These categories can be defined by items such as location, network type, branch, organization and segmentation are typically achieved through the application of additional hardware, SDN or VLANs.
Z4	**Application & Workload**	**Applications and workloads include tasks on systems or services on-premise, as well as applications or services running in a cloud environment**
Z4.1	Software Defined Compute	The ability for software to provision and manage compute configurations on programmable infrastructure such as physical and virtual servers.
Z4.2	DevSecOps	The ability to develop software in concert with the operations and security teams to maximize the protection, quality integrity of applications while shortening the development life cycle
Z4.3	Software Supply Chain	The ability to validate the security on a binary, library, or source code used to build an application.
Z4.4	Application Delivery	The ability to control resource authorization on applications and services typically implemented via an identity-aware proxy.
Z4.5	Micro Segmentation	The ability to divide or isolate logical segments on a network at the individual workload or process level. Security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted.
Z5	**Data**	**Data is defined as quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on media.**
Z5.1	Storage	The ability for software to provision and manage storage configurations on programmable infrastructure such as physical and virtual network attached storage, storage area networks, and hyperconverged platforms.
Z5.2	Data Tagging	The ability to assign metadata on a file for use in policy to allow or deny access. Access control can be implemented in a granular fashion based on the specific attributes and tags associated to data, users, and devices.

Z5.3	Data Loss Prevention (DLP)	The ability to detect and prevent potential data breaches and ex-filtration transmissions. This is accomplished through monitoring, analysis and control of data while in use, in motion, and at rest.
Z5.4	Data Rights Management (DRM)	The ability to align access controls to encryption on a file that prevents unauthorized users or devices from modifying, accessing or distributing, data.
Z6	**Visibility & Analytics**	**Vital, contextual details provide greater understanding of performance, behavior and activity baseline across five other Zero Trust pillars (Data, Users, Devices, Applications/Workloads, and Network/Environment).**
Z6.1	Discovery & Baselining	The ability to identify characteristics of networks, environments, applications, devices to determine normal operating parameters. This capability allows for the establishment of a baseline for use in policy evaluations.
Z6.2	Security Information and Event Management (SIEM)	The ability to collect and analyze security events on all aspects of the network, environment, device and application to support threat detection, compliance, and incident management
Z6.3	Machine Learning	The ability to study data on security events regarding all aspects of the network, environment, device and application to improve the security, performance, and execution of future policy and risk scoring decisions.
Z7	**Automation and Orchestration**	**Automating manual processes to take policy-based actions across the enterprise with speed and at scale**
Z7.1	API Standard	The ability to provide a standard method of communication between disparate technologies to allow for automated activities. These standards are critical to the automation of security policy and executing dynamic access controls
Z7.2	Incident Response	The ability to respond to a security event or issue on the environment, device, application or data. Automation of incident response is enabled by workflows integrated into SOAR, SIEM, and infrastructure.
Z7.3	Security, Orchestration, Automation & Response (SOAR)	The ability to automate detection, response and remediation of security incidents. The SOAR capability will integrate with the SIEM for analysis of security events and execute automated workflows in response to threats.
Z7.4	Artificial Intelligence	The ability of machines to perform tasks that normally require human intelligence – for example, recognizing

		patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems.[12]

12 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY, 2018.

APPENDIX B: REFERENCES

1. Cyber Security Reference Architecture (CS RA) Version 4.0, July 2016 *This version of the CS RA is located on SIPRNet; link will be provided once classification of this document is completed.*
2. Identity, Credential, and Access Management (ICAM) Reference Design Version 1.0, June 2020, *https://dodcio.defense.gov/library*
3. DoD Digital Modernization Strategy, *DoD Information Resource Management Strategic Plan FY19-23*, July 2019, *https://dodcio.defense.gov/library*
4. DoD Information Enterprise Architecture (DoD IEA), Version 2.0, Volume II, July 2012, *https://dodcio.defense.gov/library*
5. DoD IT Standards Registry (DISR) 20-2, October 2020, *gtg.csd.disa.mil/disc/dashboard.html*
6. NIST SP 800-207, Zero Trust Architecture, August 2020, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf*
7. NIST SP 800-63-3, Digital Identity Guidelines, June 2017, *https://doi.org/10.6028/NIST.SP.800-63-3*
8. DoD Architecture Framework, DoD Deputy Chief Information Officer, version 2.02, August 2010, *https://dodcio.defense.gov/library/DoD-Architecture-Framework/*
9. DoD Zero Trust Strategy, Predicisional, DoD CIO, 2020, *https://dodcio.defense.gov/library*
10. Department of Defense Artificial Intelligence Strategy, DoD CIO, 2018, *https://dodcio.defense.gov/*
11. Forrester, *developing a Framework to Improve Critical Infrastructure Cybersecurity*, April 2013, NIST RFI# 130208119-3119-01, *https://nist.gov/*
12. American Council for Technology – Industry Advisory Council (ACT-IAC), *Zero Trust Cybersecurity Current Trends,* April 2019, *https://actiac.org/zero-trust-cybersecurity-current-trends*