

NAVY BLUEPRINT



For a Modern Enterprise Information Ecosystem

VERSION 2.0 | JANUARY 2025

UNCLASSIFIED

MESSAGE FROM OPNAV N2N6

VADM Karl O. Thomas
Deputy Chief of Naval Operations for
Information Warfare

The United States of America is a maritime nation. The seas are the lifeblood of our economy, our national security, and our way of life. With 90% of global commerce traveling by sea, the U.S. Navy safeguards the world's economy from hostile nations and organizations that threaten international waters. Alongside our allies and partners, we defend freedom, preserve global economic prosperity, and keep the seas open and free. In both times of peace and war, the Navy can be found in and on the sea, the air, space and in the cyber realm, so that our citizens can remain prosperous and secure.

The speed and reach at which information flows through the global environment has fundamentally changed the character of modern warfare. This global competitive space spans all warfighting domains -- where operations heavily depend on the flow of information for assured and resilient command and control. This global competitive space is also a place where individuals, organizations, and global markets are interconnected at a depth and scale we have only begun to understand.

Our nation is engaged in long-term competition with near peer adversaries who operate within multiple domains, including the information domain. In order to operate effectively in this 21st century information environment, the Navy must have a modern, secure, and adaptable information technology ecosystem based on the policies, standards, services, infrastructure, technical design, and components necessary to deliver efficient, effective, and resilient IT capabilities for users across the Navy enterprise.

The Navy Blueprint for a Modern Enterprise Information Ecosystem builds on decades of constant effort to improve our information systems, infrastructure, and processes. This updated version to the Navy Blueprint expands on the north star for network modernization articulated last year, aligning strategic guidance across the Department of Defense, Department of Navy, and Chief of Naval Operations, to provide critical information warfare architectural design to outpace our competitors through information advantage and the agile availability of AI.

This Blueprint outlines our holistic approach to implementing a modernized information ecosystem. It will, among other aspects, define the characteristics that will support the future operating environment; leverage emerging technologies; standardize terminology for better alignment; identify and close capability gaps; and prioritize innovation.

With this version of the Blueprint, we commit to the belief that this document serves as a living document, responding to Navy mission needs, and maturing implementation plans through the partnership of the Navy community. Use it as your sailing direction to chart a course for managing our Enterprise Information Ecosystem for warfighting success.

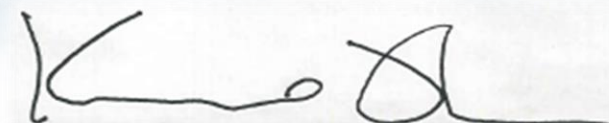


TABLE OF CONTENTS



From the Desk of N2N6	1
AN UPDATED BLUEPRINT FOR AMERICA’S WARFIGHTING NAVY	
Navy Blueprint 2.0	5
Evolving the Blueprint to Align with Strategic Guidance	6
NAVY ENTERPRISE INFORMATION ECOSYSTEM OVERVIEW	
Reviewing the Navy Enterprise Information Ecosystem	8
Understanding the Information Ecosystem End State	9
Achieving Our End State through Priorities & Partnerships	10
Blueprint 2.0 Updated Strategic Priorities & Desired Outcomes	11
STRATEGIC PRIORITY 1: CYBERSPACE WORKFORCE	
Evolving the Workforce to Meet Mission Need	13
How to Implement the DoD 8140 Qualification	14
Timeline for Transition to DoD 8140 Qualification	15
STRATEGIC PRIORITY 2: INFORMATION ECOSYSTEM MODERNIZATION	
Understanding the Navy Process for Ecosystem Modernization	17
What Makes a Good Enterprise Architecture?	18
Navy Enterprise Architecture Roadmap	19
Measuring Our Progress: Enterprise Architecture Maturity Levels	20
Navy Target DoDAF Architectural Views & Status	21
Enterprise Architecture Used as Reference Architecture	22
Starting Simple: Portfolio Product Lines	23
Adding Fidelity: Technology Business Management (TBM) 4.0	24
Using TBM to Establish an Enterprise Services Model	25
Using Model-Based Engineering (MBE) to Assess Requirements	26
Model-Based Engineering Practice Areas	27

ENTERPRISE INFORMATION ECOSYSTEM REQUIREMENTS	
Introduction to Requirements Section	29
OV-1: Navy Enterprise Information Ecosystem	30
CV-1: Navy Concept of Employment for Command and Control	31
Operationally Across Tactical and Enterprise Networks	32
The Importance of Data Management	33
Requirements for the Target Enterprise Data Framework	34
Why is Enterprise Data Management a Core Requirement	35
IMPLEMENTING ECOSYSTEM MODERNIZATION	
Pathways to Ecosystem Modernization	37
Milestones for Modernization	38
Modernization Implementation Checklist	39
STRATEGIC PRIORITY 3: NAVY CYBER READY TRANSFORMATION	
With Capability Comes Vulnerability	41
Cyber Ready Future State	42
Integrating Cybersecurity into the Systems Lifecycle	43
NAVY BLUEPRINT GLOSSARY	
Navy Blueprint Glossary	52

AN UPDATED BLUEPRINT FOR AMERICA'S WARFIGHTING NAVY

NAVY BLUEPRINT 2.0

WHAT IS THE BLUEPRINT

Upon publication in 2023, the Navy Blueprint introduced the **unifying technical framework** documenting the strategic design of the Navy's IT and Network Ecosystem. It captured high-level architectural guidance to address Navy use cases across tactical and business mission areas, while highlighting strategic priorities and a 3 year roadmap of activities to modernize the Navy's Enterprise Information Ecosystem.

The Blueprint is **informed by the current state of the Navy's IT structure** and governance, and provides a forward looking vision into modernization priorities aimed at unifying architectures across operating forces, platforms, and services. It serves as a reference document to the larger information warfare community enabling all components to leverage IT tools, information, and services where and when they need them.

WHAT HAS EVOLVED IN VERSION 2.0

With this, the second formal iteration of the Navy Blueprint, the Navy reinforces its commitment to the Blueprint serving as an iterative, and evolving record to document the Navy's information system architecture, objectives, and mission requirements related to its IT portfolio.

Version 2.0:

- **Expands upon strategic objectives** for the IT Enterprise, capturing critical workforce requirements to achieve successful Ecosystem modernization.
- Prioritizes **focus on tactical IT requirements** to meet mission objectives defined by the Chief of Naval Operations *Navigation Plan for America's Warfighting Navy*.
- Refines directed activities to recognize progress to date, and **critical next steps** based on Community feedback.

HOW TO UTILIZE THE BLUEPRINT

The Blueprint is as much about self-reflection as it is direction. Use the Navy Blueprint to inform your understanding of the Navy's Enterprise Information Ecosystem, and identify the ways in which you, your investments and technical contributions support the Navy's Information Warfighting advantage.

Use the Blueprint to:

- **Prioritize innovation** & system/network modernization efforts.
- Achieve economies of scale and **reduce redundancy** through the identification and use of Enterprise Services.
- **Improve communication** through a common lexicon for IT architectures.
- **Magnify the impact** of your efforts through alignment to the Navy's Enterprise Architecture model.

EVOLVING THE BLUEPRINT TO ALIGN WITH STRATEGIC GUIDANCE

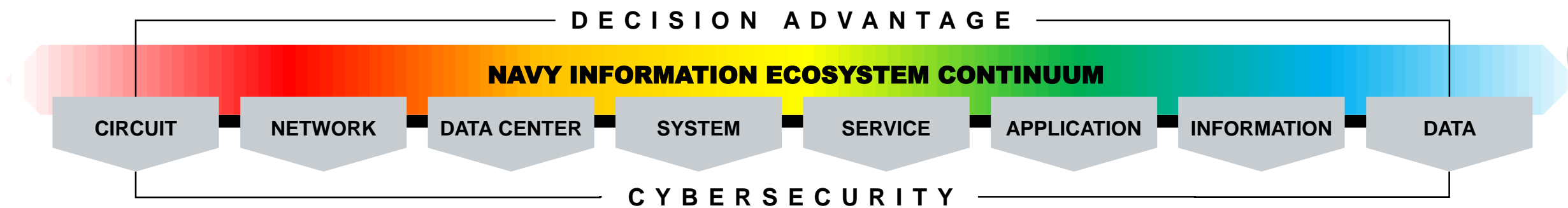


Blueprint 2.0 **iterates on prior direction**, while **expanding to meet themes from new guidance**. The Navy must expand its Information Network architectural approach, optimizing a secure Enterprise Architecture that delivers decisive capabilities for both tactical and enterprise mission requirements.

NAVY ENTERPRISE INFORMATION ECOSYSTEM OVERVIEW

REVIEWING THE NAVY ENTERPRISE INFORMATION ECOSYSTEM

An ecosystem is a layered network of interconnected system with shared dependencies. Those who cooperate in the ecosystem create compounding, outsized effects over those who do not. The warfighting ecosystem operates much the same – a system in which the layered capabilities of each of our military services enable and are enabled by each other. [Chief of Naval Operations Navigation Plan for America’s Warfighting Navy, 2024]



The Navy Enterprise Information Ecosystem is an integrated system of systems, containing people, processes, and technologies capable of connecting users with data, applications, and information to accomplish a mission.

This ecosystem is made up of tangible elements such as physical information systems, networks, and applications, and intangible elements, such as visualizations of information and workflows, serving as a foundation for all Navy business and mission functions.

The term “ecosystem” is used to describe this enterprise architecture due to the high levels of interaction and dependency that exist between applications, systems, and assets in support of a user goal. The investment in all aspects of this ecosystem is critical in the delivery of mission readiness, and optimization of our information warfare operations.

MISSION

Navy will deliver and sustain secure, interoperable, and effective mission performance.

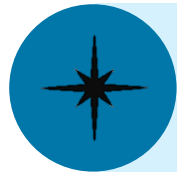
VISION

By the end of FY28, Navy will modernize its information ecosystem and deploy an integrated and virtualized set of cyberspace defense solutions, common where possible, and unique only where mission dictates.

STRATEGIC PRIORITIES

1. Cyberspace Workforce
2. Information Ecosystem Modernization
3. Cyber Ready Transformation

UNDERSTANDING THE INFORMATION ECOSYSTEM END STATE



NORTH STAR END STATE

A modern, virtualized, hyper-converged, remotely monitored and operated, cyber ready Navy information ecosystem that provides interoperable mission performance to meet tactical and business mission needs while exhibiting the characteristics:

BUILT ON

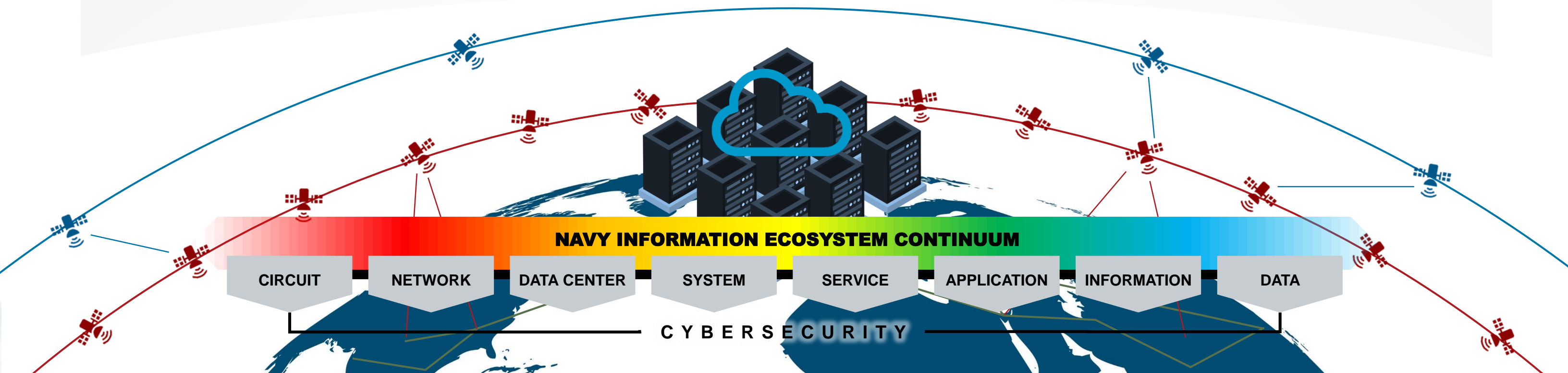
- Diverse Transport Network (Line of Sight, Undersea Cable, LEO, GEO, etc.)
- Military & Commercial Networks

CHARACTERIZED BY

- Zero Trust
- Software Defined Capabilities
- Agility

ENABLING

- Agile delivery of containerized applications developed through DevSecOps
- Command & Control
- Decision Advantage



ACHIEVING OUR END STATE THROUGH PRIORITIES & PARTNERSHIPS

PRIORITIES:

PEOPLE: Support the Navy's Military, Civilian, and Contractor personnel with Quality of Service, develop career paths to stay on the cutting edge of Information Warfare, and ensure appropriate training to increase operational readiness.

PRODUCTS: Accelerate delivery of critical Information Warfare capabilities, modernizing the Information Ecosystem to meet the Lines of Effort within the Warfighting Design.

PROCESSES: Streamline workflows to accelerate delivery of innovative capabilities that drive mission and decision advantage.

PEOPLE

PRODUCTS

PROCESSES

FLEET

ACQUISITION

RESOURCES

Delivery of the Information Ecosystem North Star within the critical timeline set by the Chief of Naval Operations *Navigation Plan for America's Warfighting Navy* will rely on efforts along **Priority lines** utilizing **Partnerships** built across the Navy at all Echelons.

PARTNERSHIPS:

FLEET: Capture mission requirements and reduce barriers to delivery and execution of new and innovative capabilities.

RESOURCES: Coordinate resourcing decisions across all Echelons to meet CNO priorities, and identify opportunities for realignment to drive efficiency.

ACQUISITION: Optimize resources within year of execution to manage risk and drive acceleration of critical Warfighting Design capabilities.

BLUEPRINT 2.0 UPDATED STRATEGIC PRIORITIES & DESIRED OUTCOMES

2.0 UPDATE HIGHLIGHTED

CYBERSPACE WORKFORCE **NEW**

- Evolve the Navy's Cyberspace Workforce program to build, protect, and defend Navy's cyber platform (across all domains); to effectively align to DOD 8140 by providing policy oversight and guidance, while advocating for resources. Specific tasks:
 - Validate and reconcile data between authoritative manpower, personnel, and readiness databases
 - Identify and track qualification requirements and provide program implementation guidance for personnel performing cyber functions
 - Develop and enhance cyber workforce data analytics
 - Train, Recruit, and Develop the cyber workforce
 - Oversee cyber workforce hiring authorities, to include Cyber Excepted Service
 - Validate DoD Cyberspace Workforce Framework (DCWF) Work Roles to ensure it evolves with technology

DESIRED OUTCOME

- Deliver, define, and provide strategic guidance, metrics, and requirements to accomplish cyber readiness by a qualified cyber workforce who can adapt to the dynamic cyber environment and provide resources to meet mission requirements.

INFORMATION ECOSYSTEM MODERNIZATION

INTEGRATED ZERO TRUST ARCHITECTURE

- Modernize the Navy's Information Technology Ecosystem, reducing dependence on end-of-service/end-of-life equipment, while implementing an Enterprise Architecture, informed by Model-Based Systems Engineering methods to drive outcome-driven investments that support resilient infrastructure across enterprise and excepted networks. Specific tasks:
 - Develop and Adopt Enterprise Architecture Guidance for Navy Information Ecosystem
 - Eliminate Time Division Multiplexing & SONET Circuits
 - Implement and Monitor Performance of Zero Trust Architecture
 - Consolidate Enterprise IT Services and Networks
 - Deliver Crypto Modernization devices across enterprise and fleet

DESIRED OUTCOME

- Define a 5-year Network Modernization Plan outlining executable roadmap to deliver cost-effective, Enterprise Architecture aligned information systems, leveraging Enterprise IT Services where ever possible.

NAVY CYBER READY TRANSFORMATION

- Shift cybersecurity away from compliance-based bureaucracy, towards a dynamic "Cyber Ready" state that improves the development to deployment pipeline, rapidly delivering hardened systems and capabilities to the warfighter, in alignment with the DON Cyber Ready effort.
 - Integrate cybersecurity into existing acquisition and certification processes
 - Utilize cyber survivability thresholds and cybersecurity testing to support risk decisions
- Shift to a model of vigilance where programs have ongoing visibility of risk so that they can proactively respond to emerging risks and continue to earn their authorization every day
 - Automated risk calculation
 - Command and Control construct for DCO
 - Navy Cyber Situational Awareness ICD

DESIRED OUTCOME

- Secure and resilient systems with a real-time awareness of cybersecurity risk.

STRATEGIC PRIORITY 1

CYBERSPACE WORKFORCE

EVOLVING THE CYBER WORKFORCE TO MEET MISSION NEED

The Blueprint 2.0 introduces a critical new Strategic Priority, noticeably absent from Version 1.0: **the Warfighter and Civilian workforce**. As noted in CNO’s *Navigation Plan for America’s Warfighting Navy, 2024*, the warfighter is the Navy’s asymmetric advantage. To maintain this advantage we must remain **diligent and focused on the training** and learning of our community, to stay ahead of and pace cyberspace threats and best practices.

In the timeline of the Navy, Cyberspace and Information Warfare remains one of the youngest disciplines within our team. However, this legacy does not reflect the criticality of this discipline against near-peer adversaries. Recognizing this importance, the Blueprint 2.0 highlights the strategic priority to overhaul and evolve our workforce to build, protect, and defend Navy’s cyber platform (across all domains), ensuring cyber readiness of our workforce.

The Navy will adhere to the **DoD 8140 Qualification Program***, built to set cyber workforce standards for the Department while allowing for flexibility in Component implementation and workforce management.

ROLE-BASED CODING REQUIREMENTS	FOUNDATIONAL VERIFICATION OF KNOWLEDGE	RESIDENTIAL VERIFICATION OF CAPABILITY	CONTINUOUS PROFESSIONAL DEVELOPMENT
<p>Qualifications are outlined based on DoD Cyberspace Workforce Framework (DCWF) work roles to enable career progression by using three levels of proficiency:</p> <ul style="list-style-type: none">• Basic,• Intermediate• Advanced	<p>Requisite knowledge is verified through one of the following for each work role assigned:</p> <ul style="list-style-type: none">• Education,• Training,• Personnel Certification, or• Experience (Conditional requirements)	<p>Requisite capability is verified through on-the-job and, if appropriate environment-specific qualification to ensure cyber personnel can meet mission needs.</p>	<p>Personnel must complete at least 20 hours of cyber training/activities each year to ensure skillsets evolve along with changes to the environment.</p>

* For a complete detail of the DoD Cyber Workforce Framework including Work Elements and Work Role Codes, please see *DON CIO Transition Memorandum, dtd 4 May 2023*.

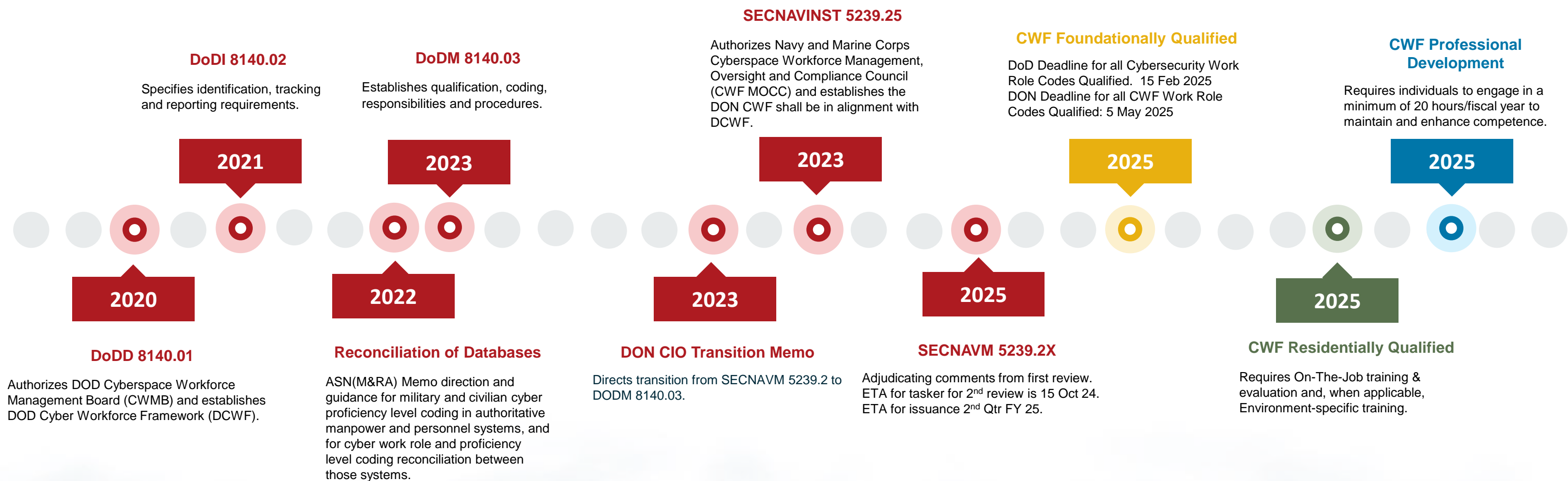
HOW TO IMPLEMENT THE DoD 8140 QUALIFICATION

All personnel performing cyber duties must be designated in writing via a command letter of designation.

	Civilian & Military Personnel	Contractor
Foundational Qualification	Within 9 months of assignment to the Cyber Workforce	Waiting for approval of DFARs language pointing to 8140
Residential Qualification: Environment-specific & On-the-Job	Within 12 months of assignment to Cyber Workforce	Once new DFARS clause is approved, the contract must include language to indicate requirement and how it will be achieved
Continuous Professional Development	Commences in the fiscal year after the employee has completed both foundational and resident qualification requirements. Requires individuals to engage in a minimum of 20 hours/fiscal year to maintain and enhance competence.	

Source: DoD 8140 Qualification Matrices – DoD Cyber Exchange

TIMELINE FOR TRANSITION TO DoD 8140 QUALIFICATION



STRATEGIC PRIORITY 2

INFORMATION ECOSYSTEM MODERNIZATION

UNDERSTANDING THE NAVY PROCESS FOR ECOSYSTEM MODERNIZATION

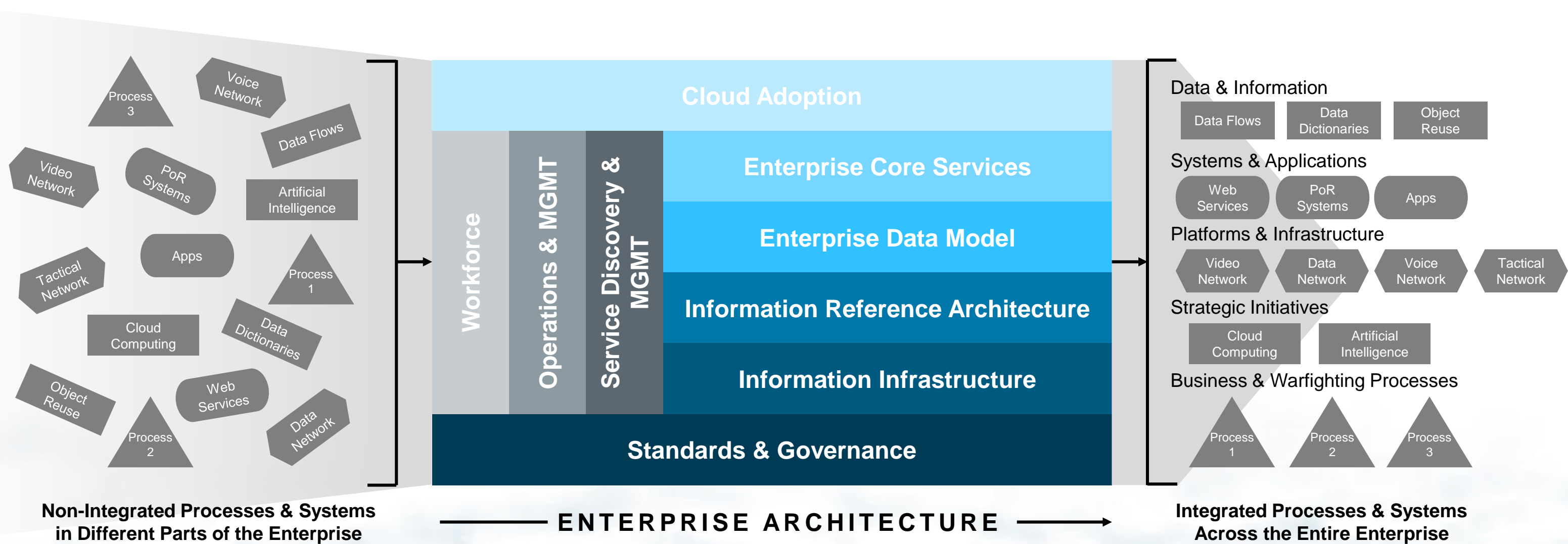
For the purposes of the Navy Blueprint, Information Ecosystem Modernization is defined by the **alignment of IT assets, services, and processes along the Information Ecosystem Continuum** to ensure delivery of an optimized Enterprise Architecture that is virtualized, hyper-converged, remotely monitored and operated, providing interoperable mission performance to meet tactical and business mission needs while exhibiting the characteristics of Zero Trust. This ecosystem is defined as “modern” based on its reduced reliance on end-of-service/end-of-life equipment, and managed **utilizing data-driven methodologies built on the principles of Model Based Engineering**, which enable the agile integration of new technologies at speed to deliver warfighting advantage.

To achieve Information Ecosystem Modernization, the Navy will develop Department of Defense Architecture Framework (DoDAF) Enterprise Architectural views, while utilizing Model Based Engineering to assess current network performance and map current and future capabilities to the Navy’s Enterprise Architecture.

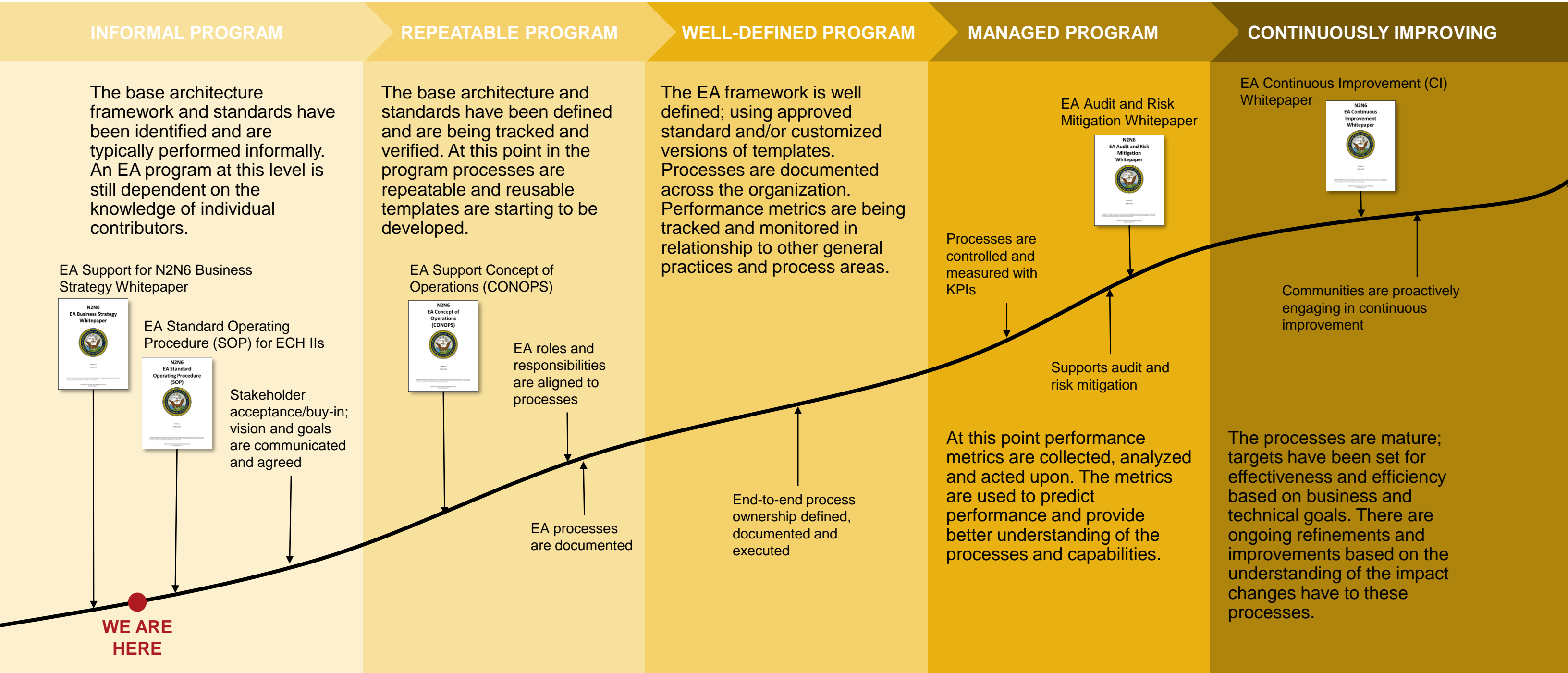


WHAT MAKES A GOOD ENTERPRISE ARCHITECTURE?

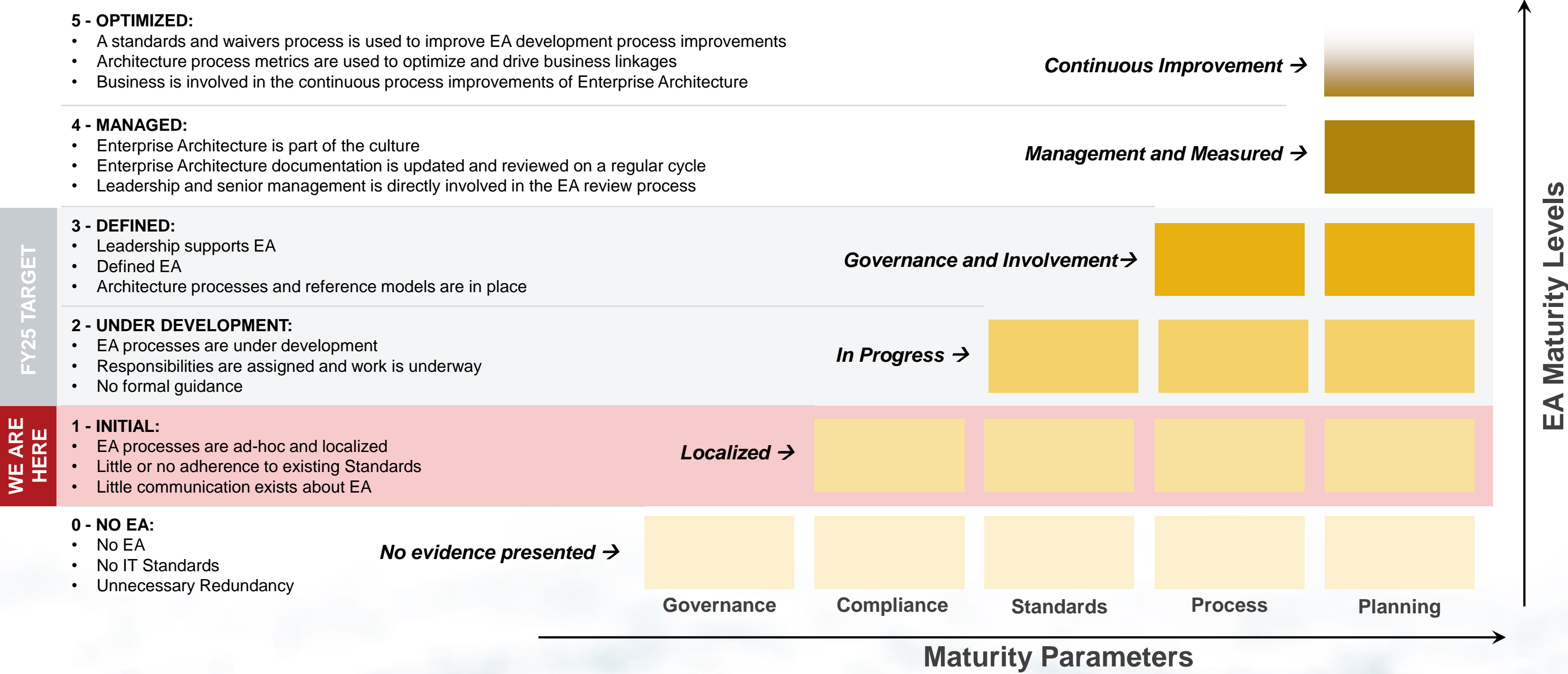
A unified Enterprise Architecture organizes and re-structures stove-piped, fragmented capabilities and standardizes ad-hoc processes. **This enables a globally integrated Information Environment** that delivers Information to the Navy throughout the battlespace and to their supporting elements and organizations. Use of the Enterprise Architecture unites efforts across the navy, **ensuring effective and efficient portfolio management** in support of warfighting success.



NAVY ENTERPRISE ARCHITECTURE ROADMAP



MEASURING OUR PROGRESS: ENTERPRISE ARCHITECTURE MATURITY LEVELS



NAVY TARGET DoDAF ARCHITECTURAL VIEWS & STATUS

EAMM* AREA (*Enterprise Architecture Maturity Model)	ARTIFACT	DESCRIPTION	STATUS
Administration/Governance	All Viewpoint 1 (AV-1)	Describes the Enterprise Architecture Visions, Goals, Objectives, Plans, Activities, Events, Conditions, Measures, Effects (Outcomes), and Produced objects	Projected for completion FY25 Q2
	Operational Viewpoint 4 (OV-4)	The organizational context, role or other relationships among organizations	Will support Information Governance Updates
Framework	Services Context Description (SvcV-1)	The identification of services, service items, and their interconnections	Leveraging TBM4.0 and Portfolio Product Lines as primary SvcV-1
	Network/System Offerings Mapping	Mapping of Navy As-Is offerings to services model (SvcV-1)	Completed by Ech IIs following directive from Blueprint v1.0
Foundation/Design	Operational Viewpoint 1 (OV-1)	The high-level graphical/textual description of the operational concept	Included in Blueprint v1.0
	All Viewpoint 2 (AV-2)	An architectural data repository with definitions of all terms used throughout the architectural data and presentations	Included in Blueprint v1.0 (Glossary)
	Capability Viewpoint 1 (CV-1)	Addresses the enterprise concerns associated with the overall vision for transformational endeavors and thus defines the strategic context for a group of capabilities	Included in Blueprint v2.0
	Standards Viewpoint 1 (StdV-1)	The listing of standards that apply to solution elements	Incomplete
	Standards Viewpoint 2 (StdV-2)	The description of emerging standards and potential impact on current solution elements, within a set of time frames	Incomplete

ENTERPRISE ARCHITECTURE USED AS REFERENCE ARCHITECTURE

WHAT IS REFERENCE ARCHITECTURE?

A Reference Architecture provides a template solution for an information system implementation across a particular domain. It uses various DoDAF views to show high-level components including domains, services, and capabilities along a common vocabulary, with the aim to stress commonality across implementations. This promotes the delivery of an effective IT solution that supports a global plug and play architecture between distributed nodes.

The Navy Enterprise Architecture and its included Department of Defense Architecture Framework (DoDAF) artifacts (mainly System & Service Views) provide a critical template for Enterprise Information Ecosystem requirements. As performance gaps and redundancies are identified, Network and System owners should utilize the Enterprise Architecture as reference for modernization. Utilizing these views as reference support the Blueprint Strategic Priority by:

- Improving the interoperability of information systems by establishing a standard solution and common mechanisms for information exchange.
- Reducing development costs of software products through the reuse of common assets.
- Improving communication inside the organization as stakeholders share the same architectural mindset.

HOW THE NAVY ENTERPRISE ARCHITECTURE SHOULD BE USED AS REFERENCE ARCHITECTURE

The Navy Blueprint Enterprise Architecture serves as a starting point for system design and implementation of new technologies. This reference architecture will provide recommended information flows and solutions to avoid “reinventing the wheel,” as well as providing standard product lines and network views for which a system can easily integrate to leverage common enterprise investments and ultimately reduce the need for bespoke information services. Some actions aligned to Reference Architecture that you can take today include:

1

Align system components to portfolio product lines (supports SvcV-1)

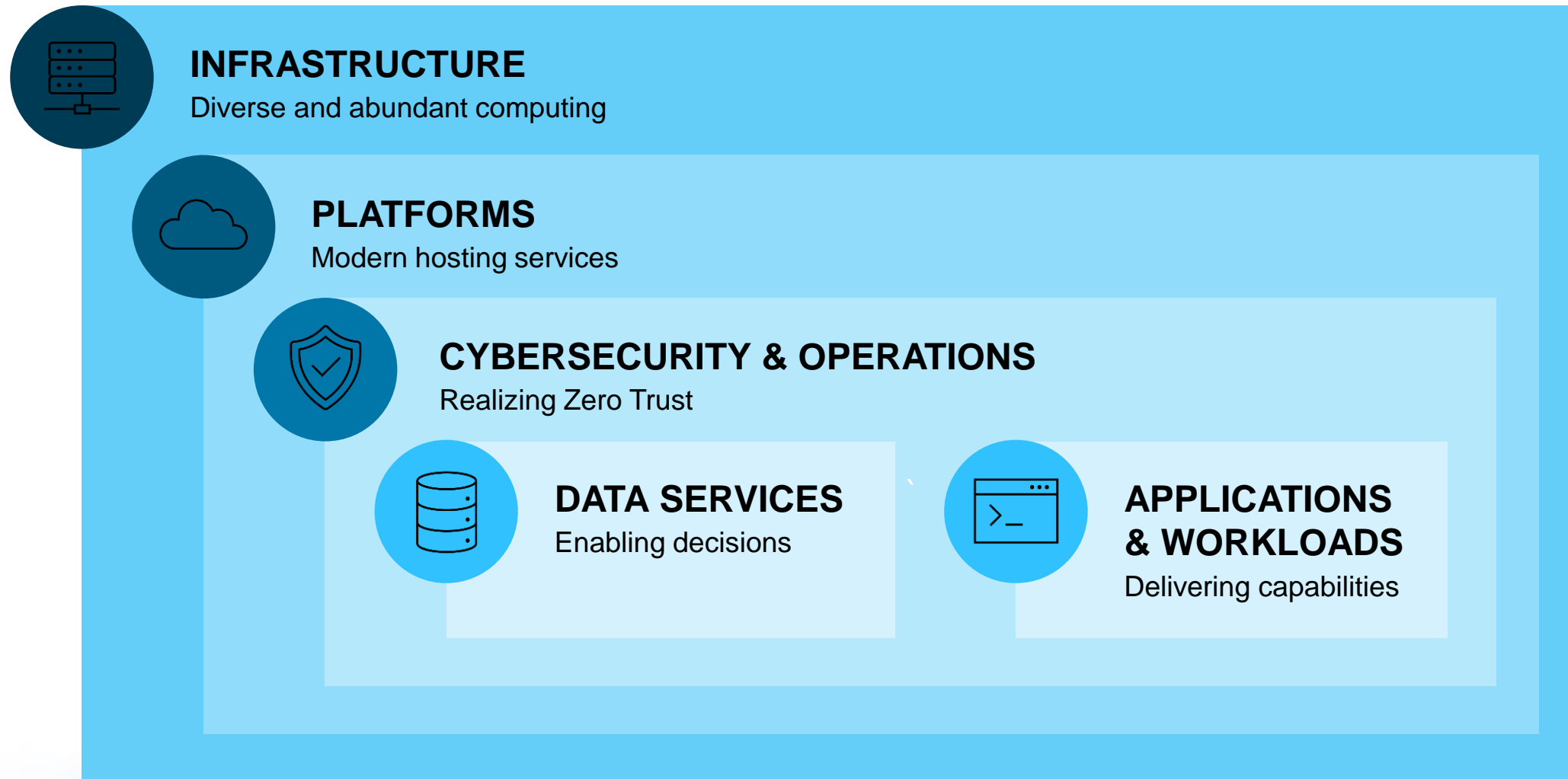
2

Characterize systems along the TBM Framework (SvcV-1)

3

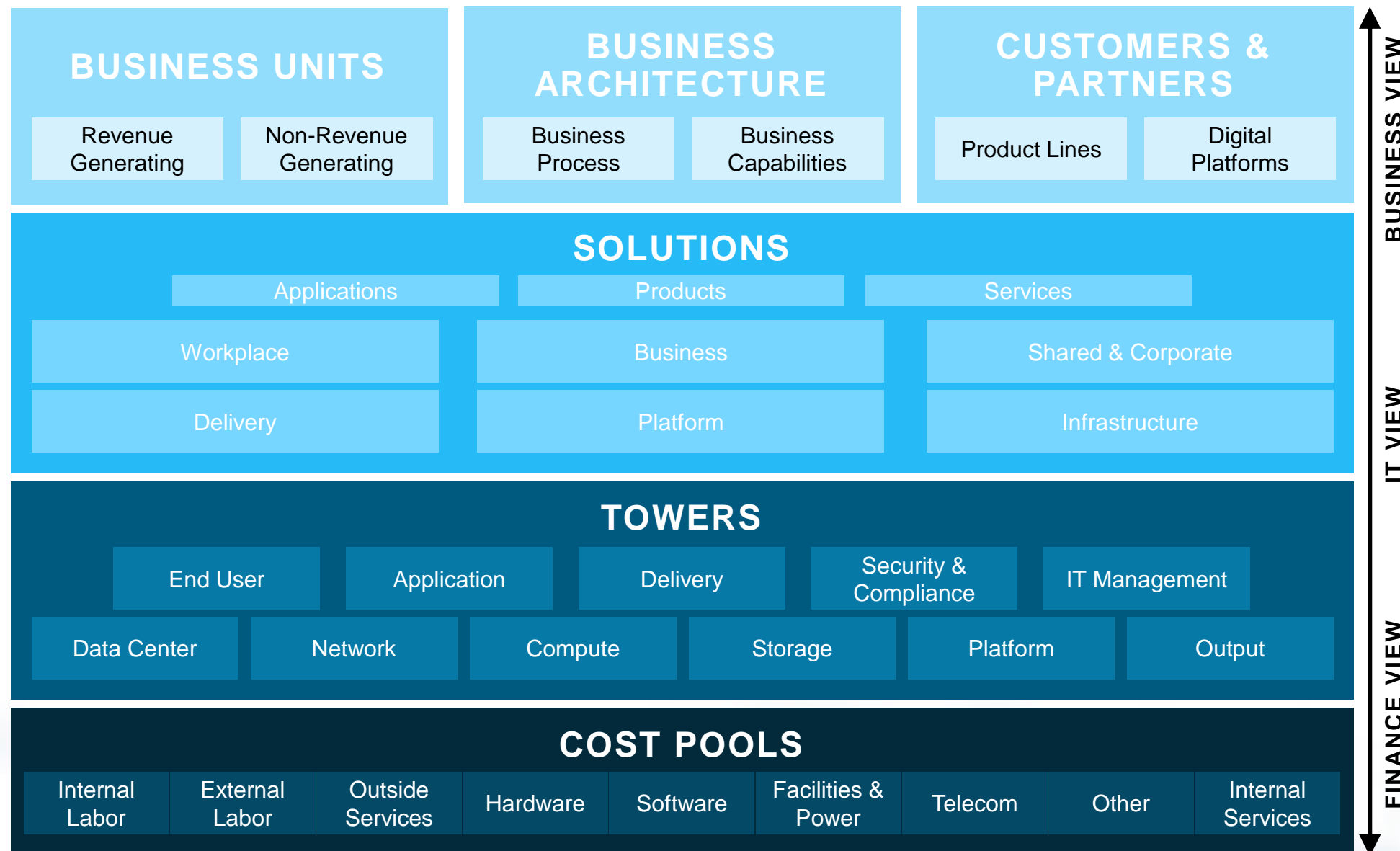
Identify common architectural solutions where available

STARTING SIMPLE: PORTFOLIO PRODUCT LINES



- While the Technology Business Management (TBM) Framework 4.0 is leveraged by Navy as the foundation for the Enterprise Architecture SvcV-1, Portfolio Product Lines offer a simplified view aligned to the “Solutions” and “Towers” models of this framework, and offer a high-level view for how to understand your As-is architecture.
- Portfolio Product Lines as defined provide solution categories for high level characterization of investments across the information ecosystem continuum.
- The diagram notes the hierarchical relationship between these product lines from infrastructure to enterprise IT services that serve cybersecurity, data, and application requirements.
- By utilizing Portfolio Product Lines and the TBM framework, we can trace performance gaps, compare similar offerings, and identify the total level of investment to deliver components of the Navy Enterprise Information Ecosystem.

ADDING FIDELITY: TECHNOLOGY BUSINESS MANAGEMENT (TBM) 4.0



- TBM 4.0 serves as the foundation of the Navy's Services View 1 (SvcV-1) in the Enterprise Architecture, encapsulating the context of service categories, from which offerings can be compared.
- The implementation of TBM 4.0 for this purpose aligns with OMB A-11 Section 55 (2022) which is driven by common financial management methodologies across Federal Agencies.
- By aligning to the TBM framework, Navy IT portfolio and financial management are aligned utilizing terms that map to enterprise architecture.

USING TBM TO ESTABLISH AN ENTERPRISE SERVICES MODEL

WHAT IS AN ENTERPRISE IT SERVICE?

Enterprise Services are part of a business model **that enables resources across an organization** to deliver value to consumers for a common purpose.

Enterprise IT Services cover software, hardware, and support services that cover a variety of Information Technology (IT) and Operational Technology (OT) use cases. They consist of a technology solution paired with an appropriate use case(s), **enabling reuse whenever those use cases are encountered by multiple users.**

Enterprise IT Services include but are not limited to collaboration and productivity solutions, Identity, Credential, and Access Management (ICAM), Model Based Systems Engineering (MBSE), cloud, and data analytics capabilities.

These **services maximize efficient use of resources** eliminating investment in duplicative capabilities, and reduce organizational complexity by honing in on a limited number of operating entities and control points.

Navy's pursuit of an Enterprise Architecture characterized by the use of Enterprise IT services aligns to the DoD Modular Open Systems Approach to integrating complex IT systems, through the creation of an IT service marketplace that allows consumers to discover an IT service, integrate with it on their own, and replace it with something better when available with minimal impact to the larger operationality of their specific use case.

Some key design patterns that enable Enterprise IT Service utility include:

- **Microservices:** An architectural style that structures an application as a set of loosely coupled and independently deployable services, each owned by a small team.
- **OpenAPIs:** A standard way of describing application program interfaces, or APIs, so that they are easily discoverable by people inside or outside of any given organization.
- **OpenTDF:** An open-source implementation of Trusted Data Format (TDF), which is a government open standard that allows data-centric security services to be interoperable.

Prioritization and selection of Navy Enterprise IT Services will focus on Outcome driven assessments, to identify critical services that meet the market needs of the Navy community measured on Customer Experience, Operational Resilience, Best Value Cost, and other World Class Analytic Metrics.

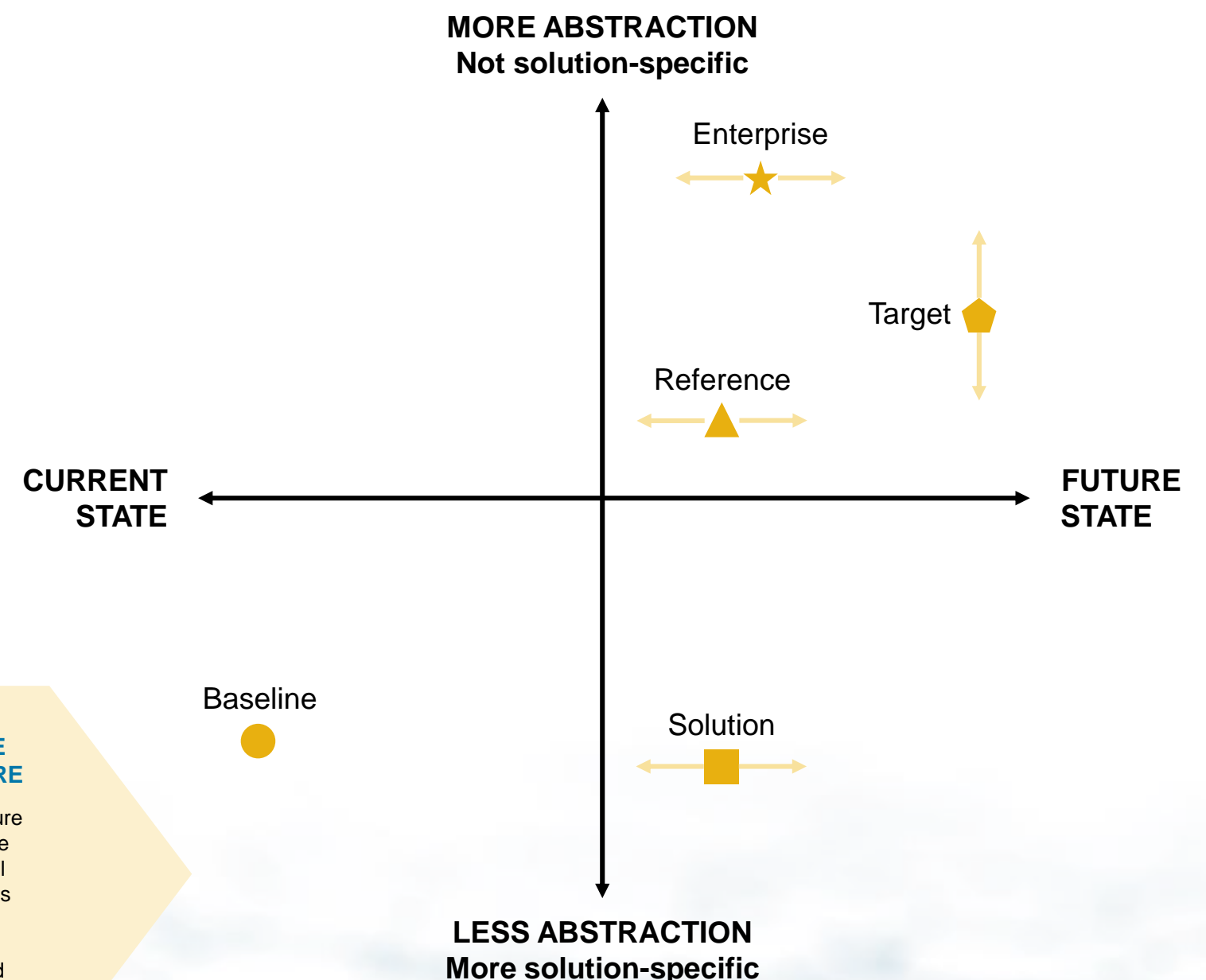
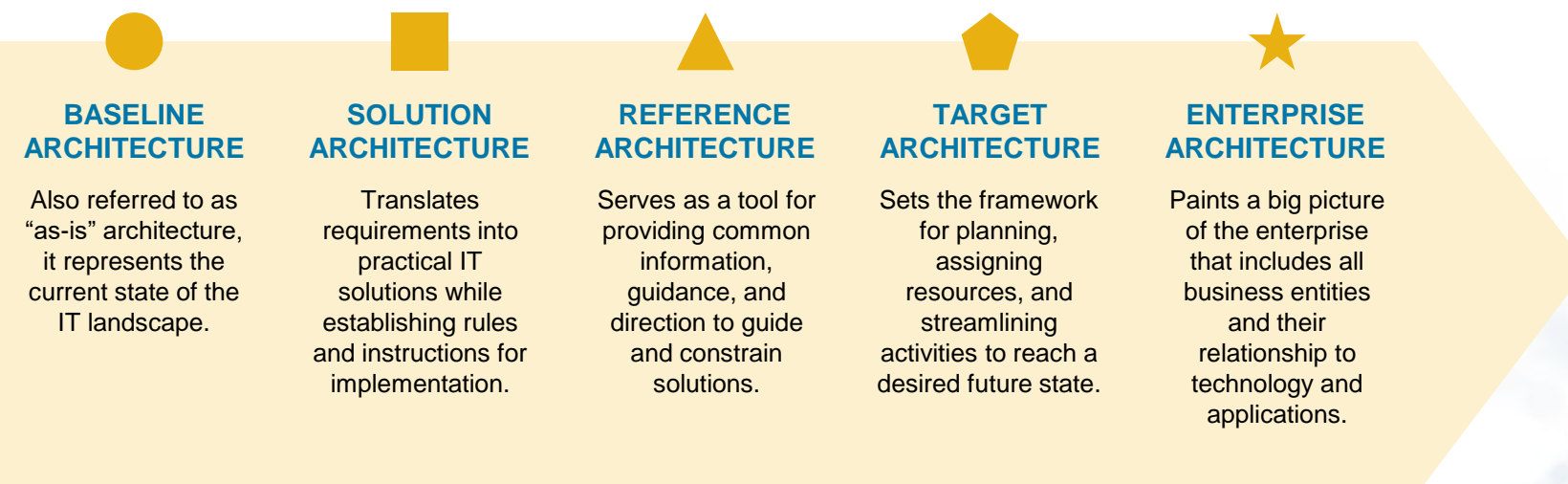
USING MODEL-BASED ENGINEERING (MBE) TO ASSESS REQUIREMENTS

Fundamental to the Navy's Modernization is the use of MBE, a component of Digital Engineering (DE). Using this disciplined approach to assessing requirements, and measuring performance of as-is and projected system architectures, enables a data-driven approach to Enterprise Information Ecosystem Modernization.

By employing MBE, the Navy can capture, and align stakeholder requirements, system designs, engineering approaches, while precisely targeting modernization of specific ecosystem components that drive mission performance within a resource constrained environment.

Through this process, a variety of models can be utilized to support a diverse set of planning and execution requirements. These models can be organized based on their level of **detail and complexity** as well as their relative perspective in time, **current state vs. future state**, to better articulate their purpose and utility, as well as which stakeholders are responsible for each.

ARCHITECTURAL VIEWS

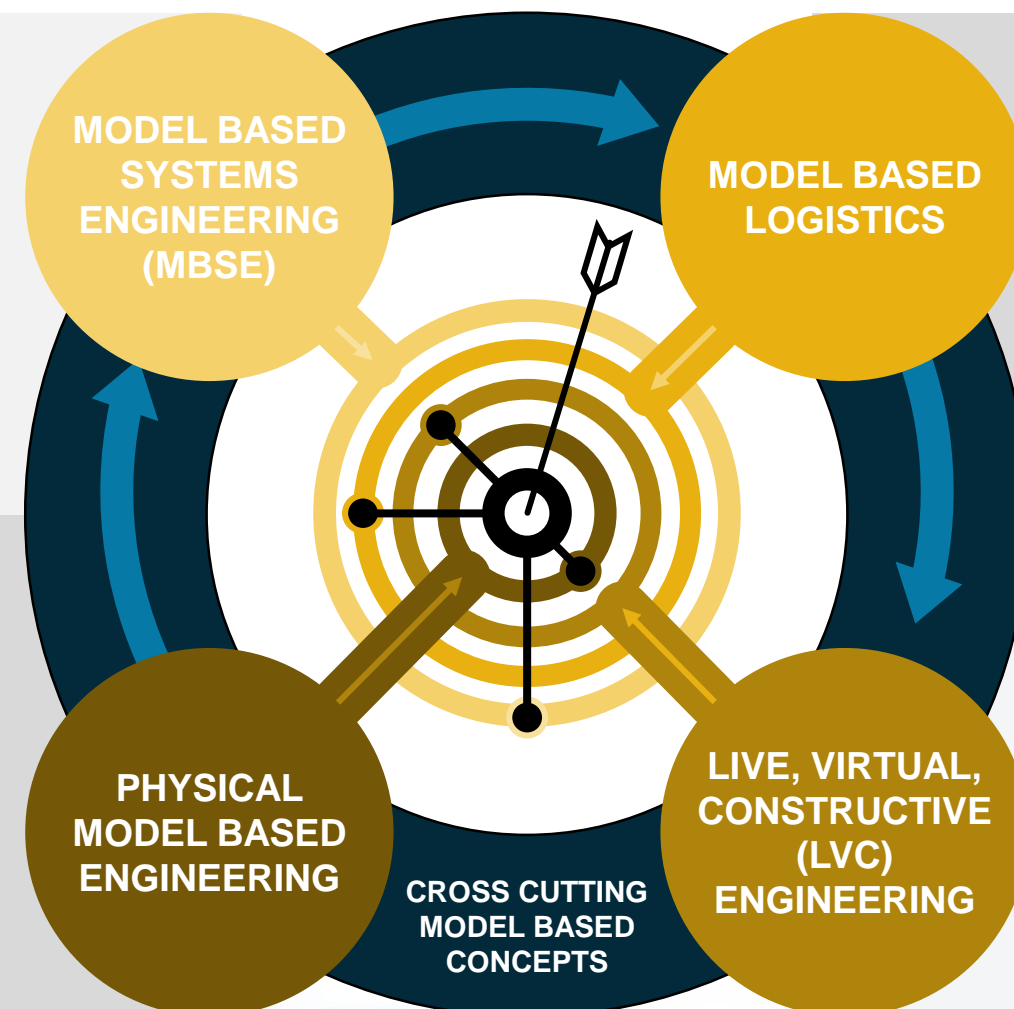


MODEL-BASED ENGINEERING PRACTICE AREAS

Commands are encouraged to deploy MBE across various practice-areas, enabling full IT portfolio management of a Modern Enterprise Information Ecosystem.

A formalized methodology that is used in the development of complex systems. MBSE puts models at the center of system design vice traditional documentation. MBSE relies heavily on model templates, libraries & shared elements which can be pulled from reference and enterprise architectures.

Software representative models of physical systems that may include electrical, hydraulic, mechanical, optical, thermal, or pneumatic components. The system may include passive and active devices. Physical Model Based Engineering is critical in understanding baseline architectures.



A model-based approach to logistics to manage configuration management, provisioning, readiness modeling, and technical data management logistics. The approach supplies support data to predict changes to system readiness.

Model-based Engineering that includes simulation utilizing: “LIVE”, real, people operating real systems; real people operating “VIRTUAL” systems; “CONSTRUCTIVE” computer programs that determine the resulting effects of both LIVE and VIRTUAL components.

Several requirements apply to all applications of MBE, including infrastructure support, model discoverability & reusable assets, MBE knowledge management, MBE support desks, and MBE tools.

The Navy has identified the Naval Integrated Modeling Environment (Naval IME) as the Authoritative environment for MBE.

ENTERPRISE INFORMATION ECOSYSTEM REQUIREMENTS

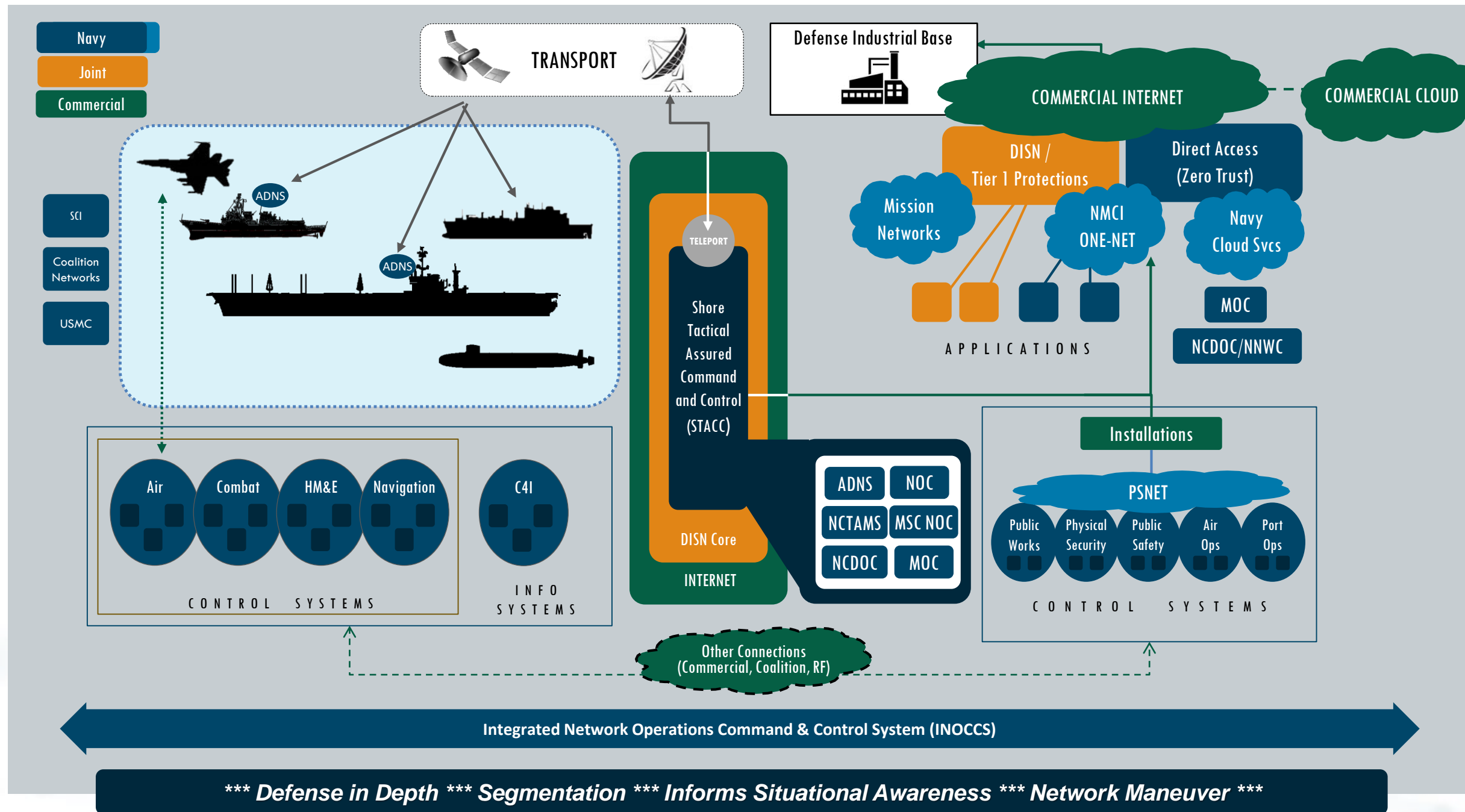
INTRODUCTION TO REQUIREMENTS SECTION

While Blueprint v1.0 and its directed prioritized network assessments to drive modernization and optimization of Enterprise resources, **the OV-1 provided in this section covers mission use cases both afloat and ashore**, across both tactical and enterprise mission areas. Similarly, the provided CV-1 gives a tactically focused look at the Navy Concept of Employment for Command and Control, outlined by both the DCNO for Information Warfare's *Information Warfighting Design*, and CNO's *Navigation Plan for America's Warfighting Navy, 2024*.

At the heart of Navy operations and the bridging element between our enterprise business systems ashore, **and the tactical networks afloat and ashore, are the Maritime Operations Centers (MOC)**. These critical nodes in our Enterprise Information Ecosystem rely on a spectrum of assets across the Information Ecosystem Continuum, and represent a priority area for network modernization for the Blueprint v2.0.

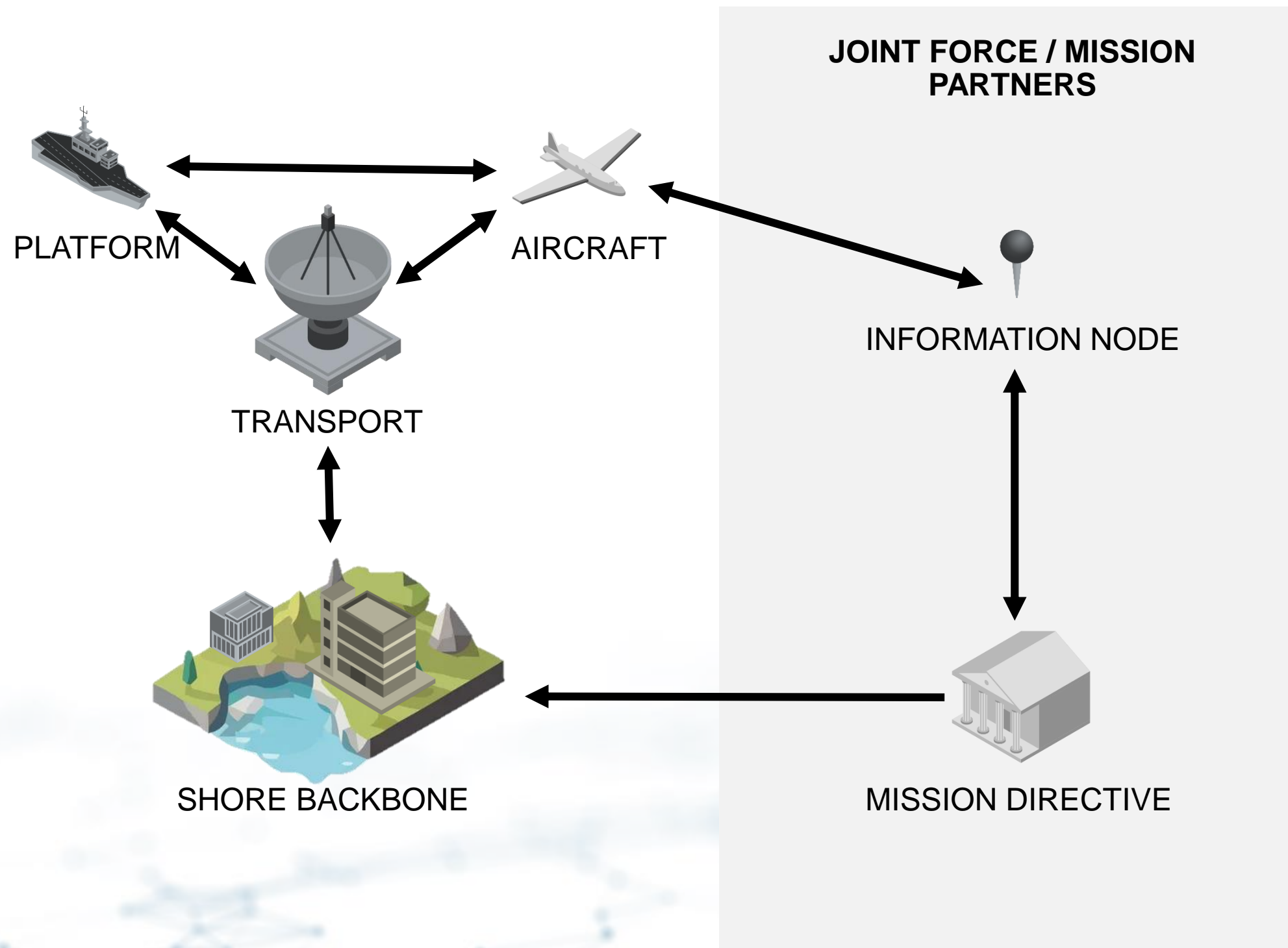
As the Navy continues to modernize its networks, **the role of the MOC will be central** to the modeled requirements in the Navy's future Enterprise Architecture artifacts, to ensure a resilient transport architecture exists to provide exchange of information between both tactical and enterprise network environments.

OV-1: NAVY ENTERPRISE INFORMATION ECOSYSTEM



- The **Navy Enterprise Information Ecosystem** is an integrated system of systems, containing people, processes, and technologies
- This ecosystem view is applicable to information systems across Navy mission Afloat, and Ashore both on Enterprise and Excepted Networks

CV-1: NAVY CONCEPT OF EMPLOYMENT FOR COMMAND AND CONTROL



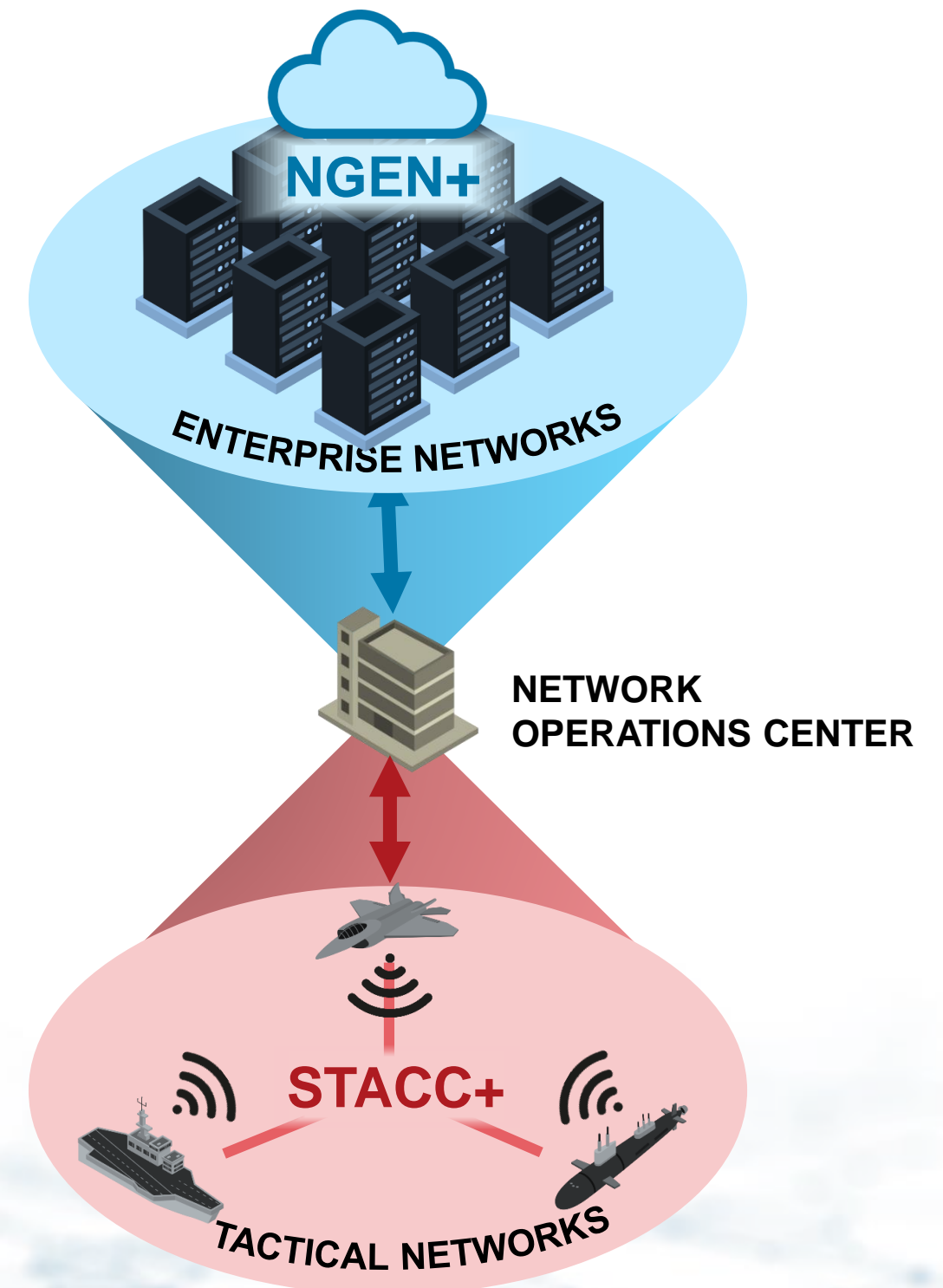
- With the Blueprint v2.0 taking a closer look at the **tactical implications** of the Enterprise Information Ecosystem, Command and Control (C2) represents a driving use case in the architectural requirements of the Navy's Enterprise Information Ecosystem.
- The Concept of Employment outlined in the diagram represents a high-level flow of information that rides on this Ecosystem for the execution of critical warfighting capabilities defined by N2N6's Information Warfighting Design.
- Expanded details of the individual nodes of this Concept of Employment are available at higher classification outlining target architectures to ensure resilient connectivity.

OPERATIONALITY ACROSS TACTICAL AND ENTERPRISE NETWORKS

While Blueprint v1.0 directed prioritized network assessments to drive modernization and optimization of Enterprise resources, the OV-1 provided covers mission use cases both afloat and ashore, across both tactical and enterprise mission areas. The CV-1 provides a tactically focused look at the Navy Concept of Employment for Command and Control, outlined by both the DCNO for Information Warfare's *Information Warfighting Design*, and CNO's *Navigation Plan for America's Warfighting Navy, 2024*.

At the heart of Navy operations and the bridging element between our enterprise business systems ashore, and the tactical networks afloat and ashore, are the Maritime Operations Centers (MOC). These critical nodes in our Enterprise Information Ecosystem rely on a spectrum of assets across the Information Ecosystem Continuum, and represent a priority area for network modernization for the Blueprint v2.0.

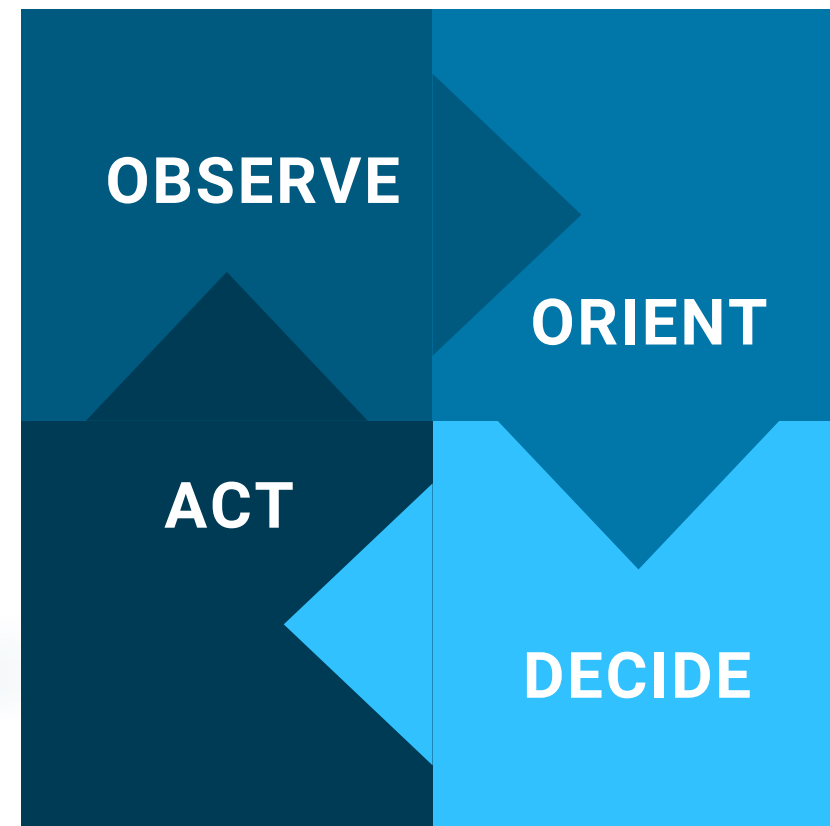
As the Navy continues to modernize its networks, **the role of the MOC will be central** to the modeled requirements in the Navy's future Enterprise Architecture artifacts, to ensure a resilient transport architecture exists to provide exchange of information between both tactical and enterprise network environments.



THE IMPORTANCE OF DATA MANAGEMENT

As reflected across the Information Ecosystem Continuum, the Enterprise Information Ecosystem provides a critical transport network architecture for the secure delivery of information. However, the design of this ecosystem and its Enterprise Architecture also is influential on the quality and effectiveness of the data provided across it. In today's warfighting environment, the ability to leverage data by means of Artificial Intelligence (AI) or traditional data analytic methods is imperative for rapid decision making and delivering military advantage that outpaces our adversaries.

We must include the design of our data management model into our Enterprise Architecture to ensure access to and the availability of the right data, at the right time, where it is needed to deliver competitive military advantage at the speed of relevance. When one makes a decision, they apply the 4-step OODA loop:



- **Observe:** Gather data from relevant sources. This step is expedited by strong data management practices.
- **Orient:** Individuals apply context to data collected, creating situational awareness.
- **Decide:** Carefully weigh data gleaned from observations to enable the right decisions.
- **Act:** After developing and assessing multiple options, the decision is put into action.

Data is the **FUEL** that drives the Enterprise Information Ecosystem

REQUIREMENTS FOR THE TARGET ENTERPRISE DATA FRAMEWORK

DATA LIFECYCLE & USAGE

CREATE

Data is created through the execution of business and mission functions in systems and applications.

1

DATA CONSUMPTION: KEY ROLES

- Mission Owner
- Data Consumer
- Data & Analytics Specialist

CURATE

Data from many sources is made available to purpose-built environments capable of data cleaning and integration.

2

DATA CURATION: KEY ROLES

- Data Steward
- Functional Data Manager
- Data & Analytics Specialist

CONSUME

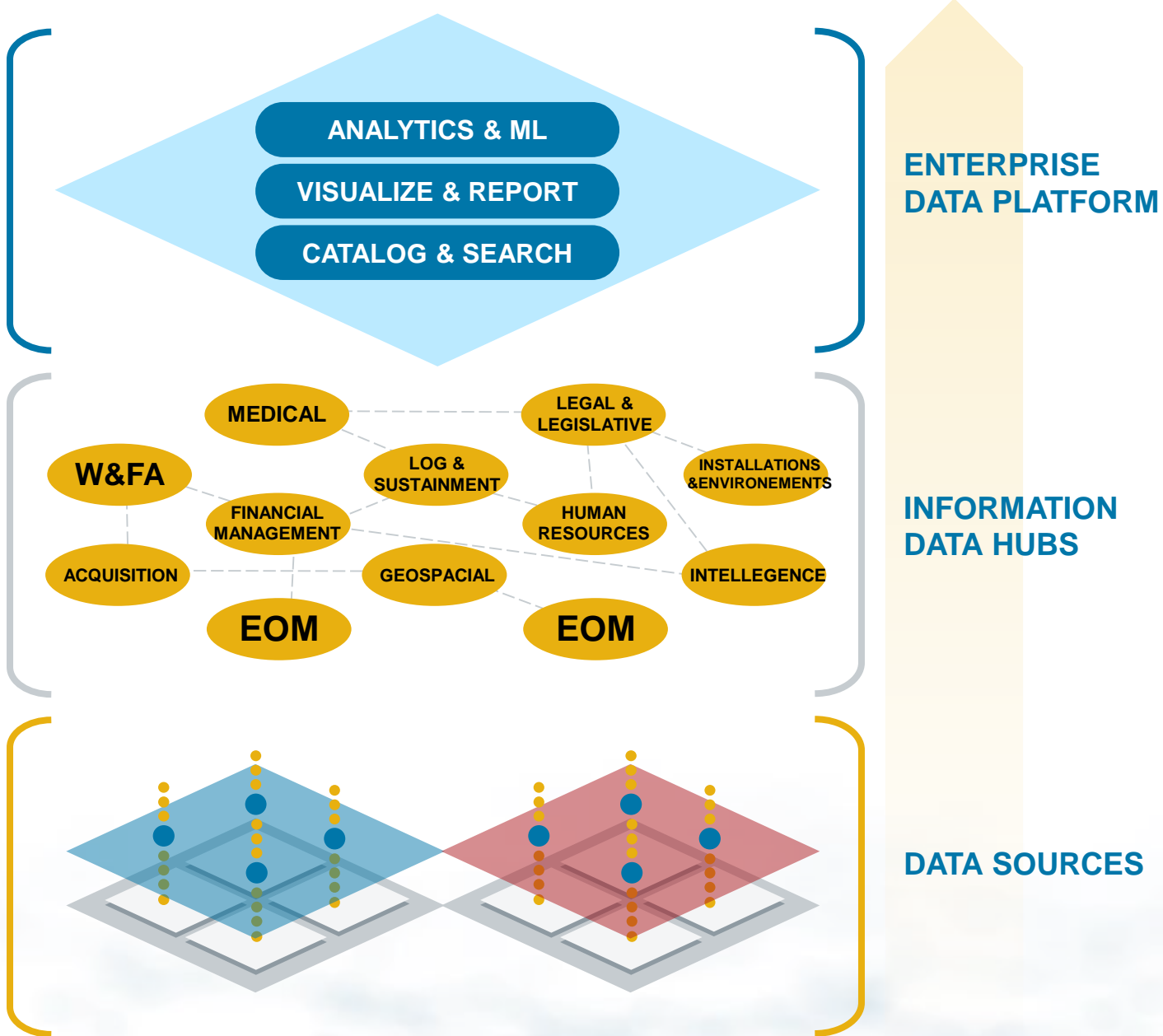
Data is consumed by human or machine using data services to discover, access, and populate workflows, analytics and visuals.

3

DATA CREATION: KEY ROLES

- IT Service (System) Owner
- Data Custodian
- Data Producer

DATA ARCHITECTURE



WHY IS ENTERPRISE DATA MANAGEMENT A CORE REQUIREMENT?

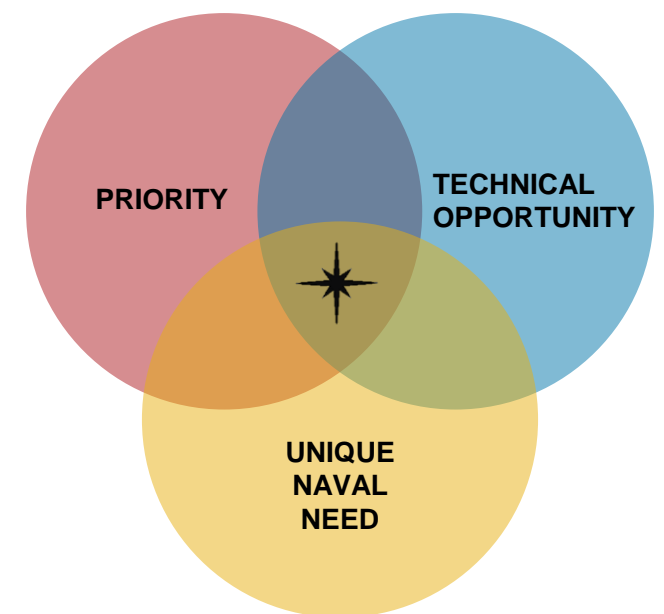
Per Executive Order 14110 on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, and the Chief of Naval Operations *Navigation Plan for America's Warfighting Navy*, the Navy is directed to promote and deploy at scale Artificial Intelligence (AI) to cause non-linear gains in Naval Operations. With this guidance, data management and effective AI are fundamental to the Ecosystem requirements aligned to the Information Warfighting Design.

AI will be deployed on both tactical & enterprise corporate functions, and influence workforce development into the future.

WHILE AI IS A DISRUPTOR, DATA IS USELESS WITHOUT CONTEXT

To bring context and understanding to the Navy's data resources, we must drive towards an enterprise data model, which serves as a global "master" data model distributed across the Digital Fabric of the Enterprise Information Ecosystem. This data model will pull key data attributes from various data sets hosted in data sources across the enterprise, to describe authoritative data attributes for purpose, and serve as a data integration map from originating data sources to authoritative data sets, no matter the distribution of attributes between systems

In order to mature the Navy Data Management and inform Ecosystem requirements, Data models outlined below will be included in the Navy's pursuit of Model Based Engineering practices.



1

CONCEPTUAL MODEL

- Assign properties for each component
- Identified data relationships

2

LOGICAL MODEL

- Creates unique data identifiers and determines the source of data
- Provides explicit identification of data sources
- Provides the data architecture framework that will guide the physical model

3

PHYSICAL MODEL

- Dictates the structure of the actual database implementation
- Allows data custodians to move forward with standards implementation

IMPLEMENTING ECOSYSTEM MODERNIZATION

PATHWAYS TO ECOSYSTEM MODERNIZATION

Once a specific network capability within the Navy's Ecosystem has been identified and assessed against the tactical and corporate system and data requirements of the organization, **the last step is to identify a pathway to modernization**, which can include one of two options, though some networks may see a combination, as some system capabilities can migrate, while others can not and require modernization.

OPTION 1: Migrate

- Offload network workloads to existing Zero Trust (ZT) capable enterprise architecture
- For example: Existing Flank Speed cloud enabled architecture utilized by Enterprise Network (NGEN) environment meets ZT IOC requirements today

OR

OPTION 2: Modernize

- Upgrade network capabilities to deliver ZT and remove reliance on End-of-service/End-of-life equipment
- Utilize Enterprise IT Services aligned to Enterprise Architecture where possible to reduce duplicative investments

Determination for which course of action, or combination there of, will be informed by the completion of Network Assessments, mapping to Navy Enterprise Architecture artifacts, and the use of mission outcome driven metrics to determine the level of effectiveness for the implementation of Enterprise IT Services for the defined use case or network workload.



Time Lost

All computing transaction times



Operational Resilience

Cyber, Uptime, Fighting hurt



Customer Satisfaction

All subjective input (e.g. NPS)



Cost Per User

All costs (e.g. seats, sites, licenses)



Adaptability

Time to change (e.g. infrastructure, contracts, people)

MILESTONES FOR MODERNIZATION

1

ASSESSMENT AND MODELING OF AS IS NETWORK ENVIRONMENTS

- **Objective:** Engineering level assessments for each network environment
- **Model Development:** Requirements, Topologies (circuits, comms, security, and interfaces), Functions (services, systems, applications), Information, and Data
- **Planning:** Create a high level modernization plan illustrating a timeline for network segment assessment
- **Deliverables:** Network assessment plans to support Target Enterprise Architecture (TEA) assessment tools

✓ COMPLETED BY Q4 FY24

2

NETWORK ENVIRONMENT RECONFIGURATION

- **Objective:** Assessment of each network environment to determine redundancies, requirements for continuity of operations, and candidates for cloud migration/consolidation
- **Model Development:** Utilizing the Naval IME develop network models to guide planning and execution
- **Planning:** Develop a modernization plan for network reconfiguration, migration, and/or consolidation
- **Deliverables:** Network modernization plans

COMPLETED BY Q4 FY25

3

EXECUTION

- **Objective:** Complete the movement of applications and data to the cloud, consolidation of on-prem infrastructure, and demonstrate divestment of redundant systems
- **Model Development:** Update network models to reflect system modernization
- **Planning:** Revise modernization plans as needed to reflect changing mission requirements and capabilities
- **Deliverables:** Network modernization plans, network modernization outcomes validated by data-driven measures

COMPLETED BY Q4 FY27

MODERNIZATION IMPLEMENTATION CHECKLIST

To assist in the determination of which courses of action should be taken for a given network or system therein, Commands are directed to utilize the checklist below, which outlines the critical steps and deliverables to ensure a network capability meets the expected end state identified by the Navy Blueprint.

1

- ✓ Maintain authoritative registry of all IT systems, networks, and applications in DITPR-DON & DADMS
- ✓ Assess Enterprise & Excepted Networks to identify investments which fall within Enterprise IT Services and can be provided by a consolidated enterprise network

FY24

2

- ☐ Identify Networks for divestment, migrating applicable capabilities to the Cloud where possible (Q2FY25)
- ☐ Ensure all remaining networks have network monitoring capabilities aligned with Comply 2 Connect directive (Q3FY25)
- ☐ Build network models within Naval IME of as-is architecture (Q1FY25)
- ☐ Mature Enterprise Architecture products including Standard Operating Procedures (SOPs) and Concepts of Operations (CONOPS) (Q3FY25)
- ☐ Perform gap analysis for outstanding networks to meet Zero Trust compliance (Q4FY25)
- ☐ Submit POM issues for network modernization requirements (Q1FY26)

FY25

3

- ☐ Adopt Enterprise IT Services to fill gaps in Zero Trust compliance
- ☐ Catalog data sources and align to master data model
- ☐ Catalog analytic use cases and map authoritative data to AI and analytic workflows

Ongoing

STRATEGIC PRIORITY 3: **NAVY CYBER READY** **TRANSFORMATION**

WITH CAPABILITY COMES VULNERABILITY

While the Navy Enterprise Information Ecosystem delivers incredible mission performance capabilities to our warfighter, the design and scale of this ecosystem is a critical variable in the **defining our vulnerabilities to cyber attack** from our adversaries.

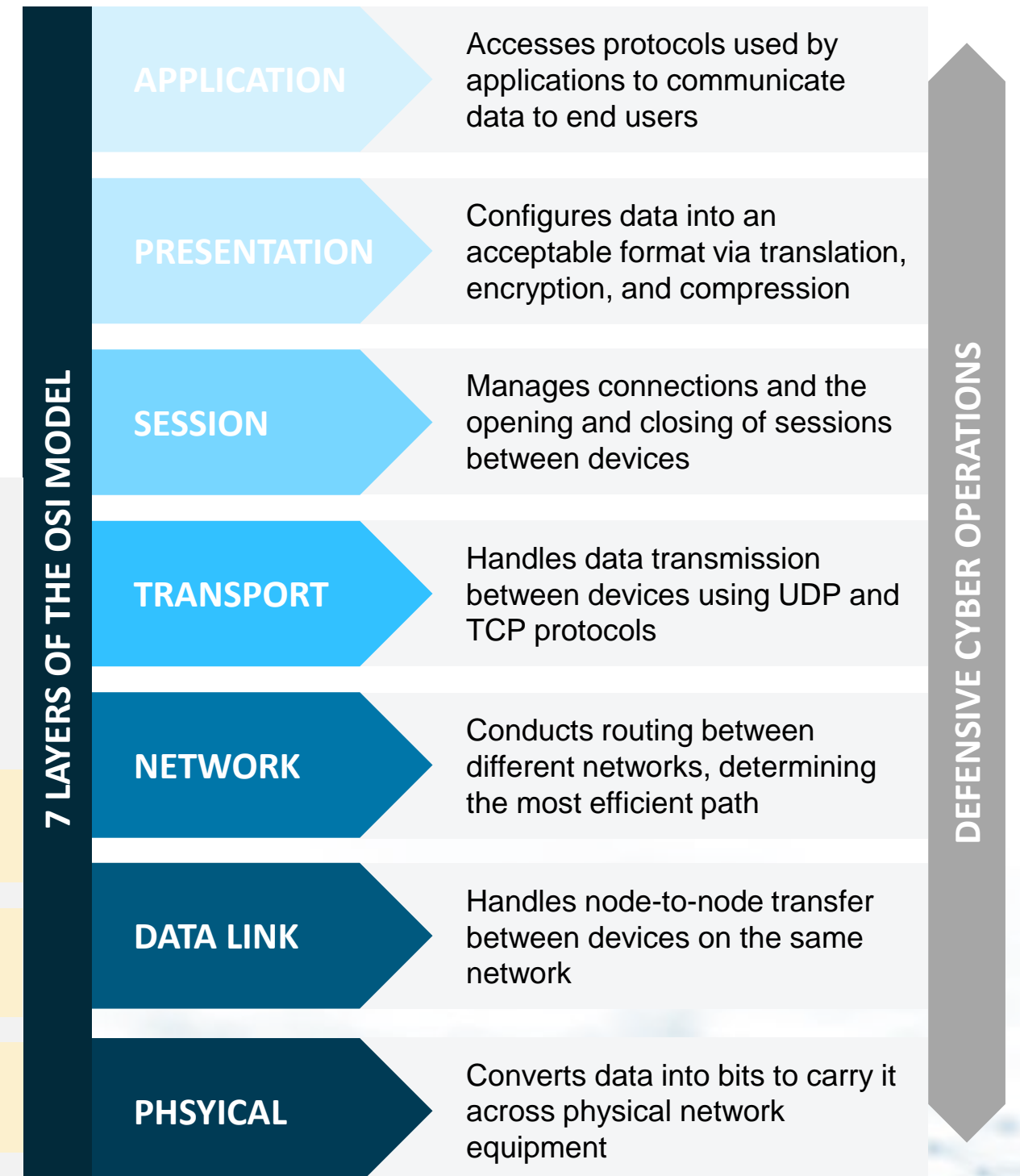
Cyber attacks are possible against all components of the Navy Information Ecosystem Continuum, driving our requirements:

- Design for cybersecurity from the beginning, reducing the cyber attack space where possible
- Protect all elements of our Information Ecosystem at each layer of the OSI Model, used to describe network data interconnections from physical implementation to application by the end user. COTS vendors often embed protections across these layers in delivered products.

SHIFTING AWAY FROM COMPLIANCE BASED CYBERSECURITY

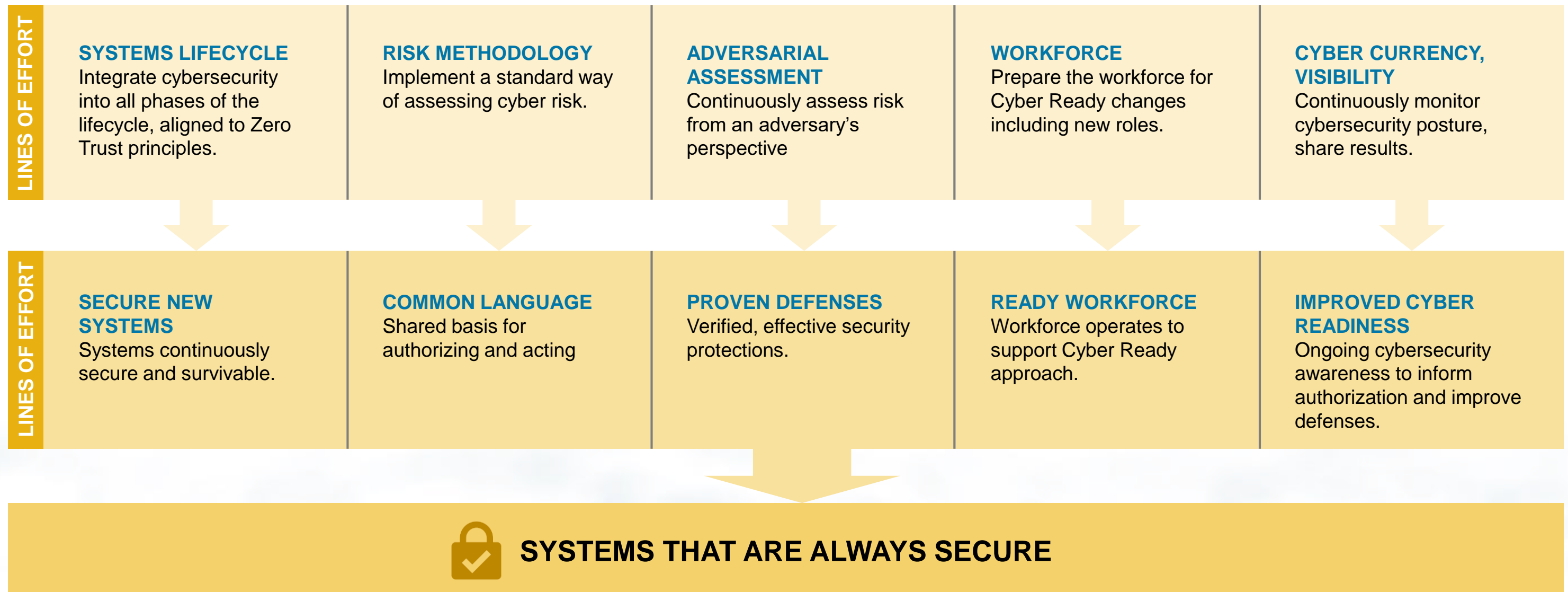
Defense of our increasingly capable Information Ecosystem to be **Cyber Ready** is characterized by 3 activities:

- 1 Reduce Attack Space:** Consolidate networks into defensible architecture integrating cybersecurity into existing acquisition and certification processes
- 2 Implement Zero Trust:** Establish least privilege access with constant verification
- 3 Defensive Cyber Operations:** Shift to a model of vigilance, including continuous network monitoring operations

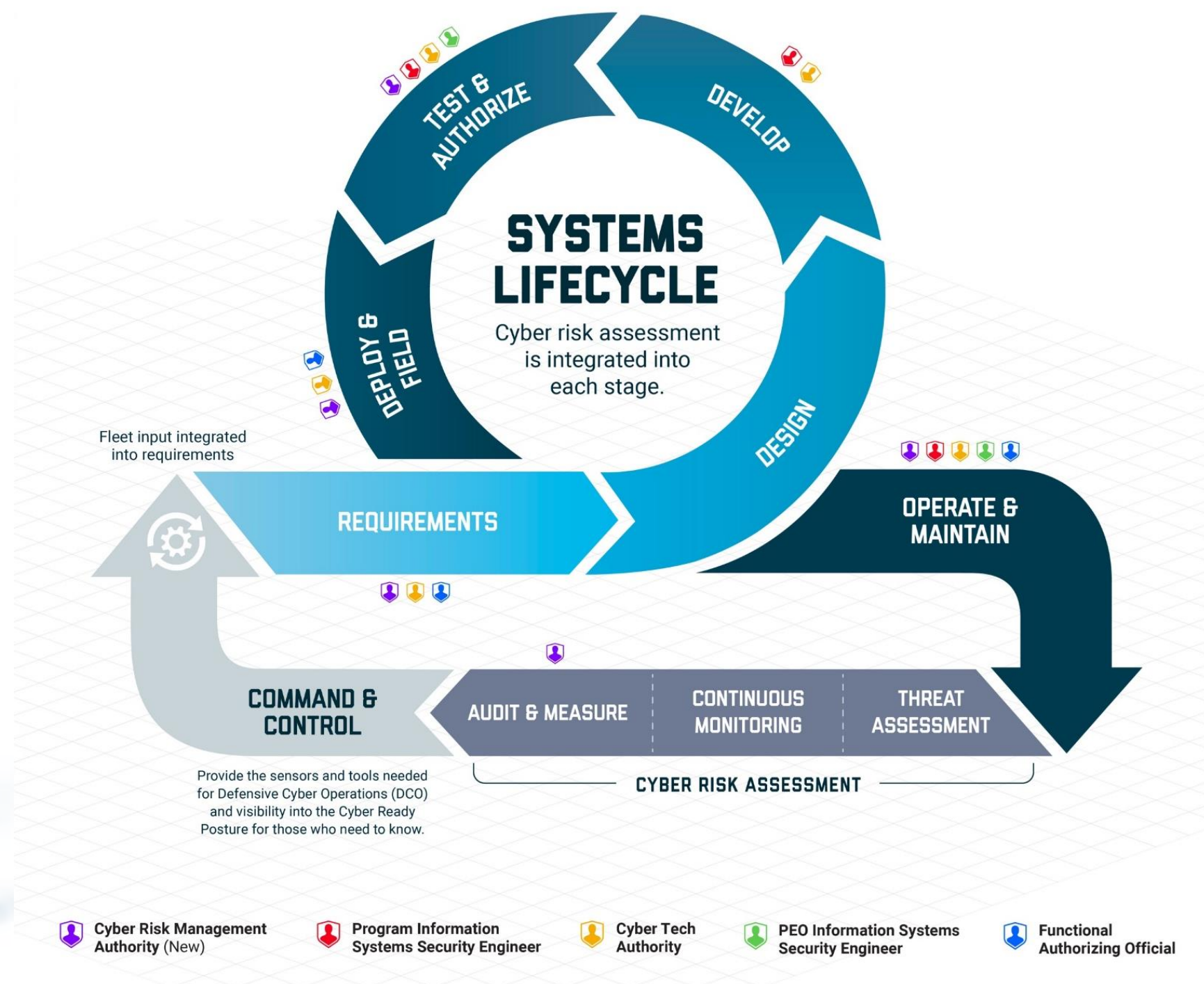


CYBER READY FUTURE STATE

The Navy has set the goal to move to a culture of cyber readiness, where the right to operate is earned and managed every day, eliminating non-value add Risk Management Framework (RMF) steps and the traditional compliance-based bureaucracy for assessing cybersecurity risk.



INTEGRATING CYBERSECURITY INTO THE SYSTEMS LIFECYCLE



NAVY BLUEPRINT GLOSSARY

(AV-2)

WHY A NAVY BLUEPRINT GLOSSARY?

The words we use matter. The Navy Blueprint offers a common lexicon for information systems and corresponding common technical capabilities which fall within a larger Enterprise Information Ecosystem. The purpose of this glossary is to offer a clear indication of what is, and is not, meant within the scope of an activity or area of knowledge.

The Navy Blueprint Glossary serves as an appendix to the rest of the Navy Blueprint and includes common acronyms and definitions, as well as citations of sources for applicable definitions where required.

Some technical areas included in this glossary include:



CLOUD



DEVSECOPS



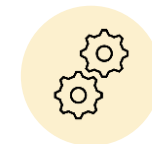
DATA MANAGEMENT



DATA ANALYTICS



NETWORKS



SYSTEM ACQUISITION



**SYSTEM & PORTFOLIO
MANAGEMENT**



TELEPHONY

For A Complete List of Definitions, See Appendix A

ACQUISITION ACRONYMS

ACRONYM	DEFINITION
3PAO	Third Party Assessor Organization
AO	Authorizing Official
AoA	Analysis of Alternative
API	Application Programming Interface
AT&L	Acquisition, Technology, and Logistics
ATO	Authorization to Operate
C&A	Certification & Accreditation
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CDD	Capability Development Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CL	Confidentiality Level
COMSEC	Communications Security
CONOPS	Concept of Operations
COTS	Commercial off-the-Shelf
CPD	Capability Production Document
CPI	Critical Program Information
DAA	Designated Accrediting Authority (older term replaced with Authoring Official)

ACRONYM	DEFINITION
DAG	Defense Acquisition Guidebook
DASD	Deputy Assistant Secretary of Defense
DAU	Defense Acquisition University
DBS	Defense Business System
DIACAP	DoD Information Assurance Certification and Accreditation Process (replaced with the Risk Management Framework (RMF))
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR	DoD IT Portfolio Repository
DoD	Department of Defense
DON	Department of the Navy (includes Navy and USMC)
DoDI	DoD Instruction
DoDIN	DoD Information Networks
DOT&E	Director of Operational Test & Evaluation
DT&E	Developmental Test and Evaluation
EMD	Engineering & Manufacturing Development
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act
FRP	Full Rate Production

ACQUISITION ACRONYMS

ACRONYM	DEFINITION
FRP/FD	Full Rate Production/Full Deployment
GOTS	Government off-the-Shelf
GSS	General Support System
IA	Information Assurance
IA	Independent Assessor (3PAO)
AM	Information Assurance Manager
IaaS	Infrastructure as a Service (Model)
IAS	Information Assurance Strategy (older term, now called Cybersecurity Strategy)
IATO	Interim Authorization to Operate
IC	Intelligence Community
ICD	Initial Capabilities Document
ID	Identification
IL	Impact Level
ILL	Information Impact Level
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IOT&E	Initial Operational Test and Evaluation
IPT	Integrated Product Team
IS	Information System
ISSO	Information System Security Office
IT	Information Technology
ITPR	Information Technology Procurement Request

ACRONYM	DEFINITION
JCIDS	Joint Capabilities Integration and Development System
KPP	Key Performance Parameter
LAN	Local Area Network
LCSP	Life-Cycle Sustainment Plan
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDD	Materiel Development Decision
MS	Milestone
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
O&S	Operations and Support
OMB	Operations and Support
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
P&D	Production and Deployment
PaaS	Platform as a Service (Model)
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PEO	Program Executive Office
PIA	Privacy Impact Assessment

ACQUISITION ACRONYMS

ACRONYM	DEFINITION
PIT	Platform Information Technology
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPP	Program Protection Plan
RA	Risk Assessment
RFP	Request for Proposal
RMF	Risk Management Framework
SA	Security Assessment
SaaS	Software as a Service (Model)
SAR	Security Assessment Report
SCA	Security Control Assessor (RMF terminology)
SCRM	Supply Chain Risk Management
SDD	System Design Document
SDLC	System Development Life Cycle
SDS	System Design Specificatio
SE	Systems Engineering
SEP	Systems Engineering Plan
SME	Subject Matter Expert
SP	Special Publication
SRR	System Requirements Review

ACRONYM	DEFINITION
SSE	Systems Security Engineering
SSP	System Security Plan
STIG	Security Technical Implementation Guide
T&E	Test and Evaluation
TA	Threat Assessment
TMRR	Technology Maturation and Risk Reduction
TSN	Trusted Systems and Networks
USD	Under Secretary of Defense
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
VA	Vulnerability Assessment
VRAM	ulnerability Remediation Asset Manager
WIPT	Working-Level Integrated Product Team

TERMS OF REFERENCE: CLOUD

TERM	DEFINITION
Adaptive Acquisition Framework (AAF)	A series of acquisition pathways to enable the workforce to tailor strategies to deliver better solutions faster. The AAF acquisition pathways provide opportunities for milestone decision authorities, DAs, and PMs to develop acquisition strategies and employ acquisition processes that match the characteristics of the capability being acquired.
Capabilities	Higher level solutions typically spanning multiple releases. Capabilities consist of multiple features to facilitate implementation.
Capability Needs Statement (CNS)	A high-level capture of mission deficiencies, or enhancements to existing operational capabilities, features, interoperability needs, legacy interfaces and other attributes that provides enough information to define various software solutions as they relate to the overall threat environment.
Cloud Service Provider (CSP)	A service provider that owns, maintains and enhances their services, and houses those service elements in a location that they own. Service is usually delivered via the internet or other network connection. Customers usually pay on a routine cycle and at a rate usually based on their usage that period or at a recurring standard rate
Commercial Cloud	Computing, storage, and network resources and services that a commercial provider maintains, operates, and manages and that are made available to multiple customers (as opposed to cloud resources and services owned and operated by an organization for their own benefit, for example). Depending on the contract, the commercial cloud service provider may be performing in commercial facilities or on-premises in Government facilities. As examples, JEDI Cloud will be performed in commercial facilities whereas milCloud 2.0 is on-premises in Government facilities.
Continuous Authority to Operate (cATO)	The core concept of cATO is to build software security into the software development methodology so that the authority to operate process (as with the testing process) is done alongside development. If done correctly, an authority to operate is nearly guaranteed once the software is release ready.
Continuous Operation	Continuous operation is an extension to continuous deployment. It is triggered by a successful deployment. The production environment operates continuously with the latest stable software release. The activities of continuous operation include, but are not limited to: system patching, compliance scanning, data backup, and resource optimization with load balancing and scaling (both horizontal and vertical

TERMS OF REFERENCE: CLOUD

TERM	DEFINITION
Cryptographic Certainty	Assurance [δ.7] unmediated data transfer does not occur.
Drawdown Accounts	An organizational method for paying for a cloud service. The consuming organization pays the provider a set amount of money. The provider decrements the money put into the account relative to what the consuming agency is using.
Decision Authority (DA)	The official responsible for oversight and key decisions of programs that use the software acquisition pathway in accordance with this issuance and related component policies. The official designates a PM and supports them in tailoring and streamlining processes, reviews, and decisions to enable speed of capability delivery. The official may be the Defense Acquisition Executive, Component Acquisition Executive, or the Program Executive Officer, or other designated official by the CAE.
Defense Business System (DBS)	Defined in Section 2222 of Title 10, United States Code.
DevSecOps	An organizational software engineering culture and practice that aims at unifying software development, security, and operations. The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. In DevSecOps, testing and security are shifted left through automated unit, functional, integration, and security testing – this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously.
Embedded Software	Software with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints, or software applications embedded in a platform (e.g., air vehicle, ground vehicle, or ship). In the context of this issuance, embedded software does not apply to firmware or software dedicated to controlling devices.
End User	Those who will ultimately use the software solution. Users convey operational concepts, requirements, and needs, participate in continuous testing activities, and provide feedback on developed capabilities.

TERMS OF REFERENCE: CLOUD

TERM	DEFINITION
Enterprise Services	Services that have the proper scope to play a productive role in automating business processes in enterprise computing, networking, and data services. Enterprise services include technical services such as cloud infrastructure, software development pipeline platforms, common containers, virtual machines, monitoring tools, and test automation tools. Responsibility for these functions is generally above the program manager.
Failover	Unanticipated migration of application operation with minimal downtime.
Fit-for-Purpose (F2P) Cloud	A DoD term. for a cloud environment that meets highly specialized mission requirements that cannot easily be met through a General Purpose Cloud solution and is suitable for scaling to adopt new DoD customers at the enterprise level. Determination criteria include utility for mission, ease of management (including provisioning and reporting), and contract terms.
Fit-for-Purpose Cloud (FPC)	A DON CIO term
Features	A service or distinguishing characteristic of a software item (e.g., performance, portability, or functionality) that fulfills a stakeholder need and includes benefit and acceptance criteria within one release. Features are used to complete capabilities and are comprised of multiple stories (or tasks, use cases, etc.).
General Purpose Cloud	Infrastructure and Platform as a Service offerings that meet the majority of the DoD's cloud computing needs across all Components of the enterprise organization.
Government Developmental Testing	Testing intended to verify and demonstrate how well the system under development meets its technical compliance requirements, to provide data to assess developmental risk for decision making, and to ensure that the technical and support problems identified in previous testing have been corrected.

TERMS OF REFERENCE: CLOUD

TERM	DEFINITION
Interoperability	The ability of systems, units or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. Interoperability includes information exchanges, systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with cybersecurity
Modern Software Development Practices	Practices (e.g., lean, agile, DevSecOps) that focus on rapid, iterative development and delivery of software with active user engagements. Small cross-functional software development teams integrate planning, design, development, testing, security, delivery, and operations with continuous improvement to maximize automation and user value.
Minimum Viable Capability Release (MVCR)	The initial set of features suitable to be fielded to an operational environment that provides value to the warfighter or end user in a rapid timeline. The MVCR delivers initial warfighting capabilities to enhance some mission outcomes. The MVCR is analogous to a minimum marketable product in commercial industry.
Minimum Viable Product (MVP)	An early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback on. Insights from MVPs help shape scope, requirements, and design.
Operational Acceptance	When one or more military units decides to use the software in military operations as informed by test and evaluation
Product Owner	A role on the program or development team that works closely with the user community to ensure that the requirements reflect the needs and priorities of the user community, and align to the mission objectives.
Product Roadmap	A high-level visual summary that maps out the vision and direction of product offerings over time. It describes the goals and features of each software iteration and increment.
Program Backlog	Program backlogs that identify detailed user needs in prioritized lists. The backlogs allow for dynamic reallocation of scope and priority of current and planned software releases. Issues, errors, and defects identified during development and operations should be captured in the program's backlogs to address in future iterations and releases.

TERMS OF REFERENCE: CLOUD

TERM	DEFINITION
Release	A grouping of capabilities or features that can be used for demonstration or evaluation. A release may be internal for integration, testing, or demonstration; or external to system test or as user delivery. A release may be based on a time block or on product maturity.
Software-Intensive	A system in which software represents the largest segment in one or more of the following criteria: system development cost, system development risk, system functionality, or development time.
Sponsor	The individual that holds the authority and advocates for needed end user capabilities and associated resource commitments.
Task	Individual activities to be completed to satisfy a user story or use case (e.g., implement code for a specific feature or complete design for a specific feature).
Technical Debt	Consists of design or implementation constructs that are expedient in the short term but that set up a technical context that can make a future change costlier or impossible. Technical debt may result from having code issues related to architecture, structure, duplication, test coverage, comments and documentation, potential bugs, complexity, coding practices, and style which may accrue at the level of overall system design or system architecture, even in systems with great code quality.
User Agreement (UA)	A commitment between the sponsor and PM for continuous user involvement and assigned decision making authority in the development and delivery of software capability releases.
User Acceptance	Verification by operational users that software is capable of satisfying their stated needs in an operationally representative environment.
Release	A grouping of capabilities or features that can be used for demonstration or evaluation. A release may be internal for integration, testing, or demonstration; or external to system test or as user delivery. A release may be based on a time block or on product maturity.
Use Case	In software and systems engineering, a use case is a list of actions or event steps, typically defining the interactions between a user and a system (or between software elements), to achieve a goal. Use cases can be used in addition to or in lieu of user stories.

TERMS OF REFERENCE: CLOUD

TERM	DEFINITION
User Story	A small desired behavior of the system based on a user scenario that can be implemented and demonstrated in one iteration. A story is comprised of one or more tasks. In software development and product management, a user story is an informal, natural language description of one or more features of a software system. User stories are written from the perspective of an end user or user of a system.
Value Assessment (VA)	An outcome-based assessment of mission improvements and efficiencies realized from the delivered software capabilities, and a determination of whether the outcomes have been worth the investment. The sponsor and user community perform value assessments at least annually, to inform DA and PM decisions.
Vulnerability Remediation Asset Manager (VRAM)	<p>VRAM is a web-enabled network vulnerability data repository and continuous monitoring analysis tool providing Navy Enterprise cyber directive compliance reporting capabilities. VRAM increases cyber security awareness for the Navy by providing visibility into enterprise network vulnerabilities and Cyber Directive compliance reporting for Centrally Managed Program/Program of Record (CMP/POR) systems, Corporate Asset (CA) systems, and individual command assets. VRAM works in conjunction with the DoD's Assured Compliance Assessment Solution (ACAS). ACAS, implemented as Tenable's Nessus Vulnerability Scanner, provides technically validated means to verify resident system vulnerabilities across a network.</p> <p>When ACAS scan data from the operational community is uploaded to VRAM, VRAM compares the vulnerabilities against the CMP/POR/CA baseline to identify deviations from the approved configuration. By segregating vulnerabilities according to those that have a remediation available from the system owner and those that do not, VRAM provides operational users with actionable and achievable tasks that empowers them to take control of their network.</p> <p>From a CMP or CA system owner perspective, VRAM provides a streamlined tool to proactively maintain, validate, and document a system configuration vulnerability baseline as well as maintain Certification and Accreditation (C&A) requirements, document Plans of Action and Milestones (POA&Ms) for mitigation of system vulnerabilities and monitor both the operational and baseline configuration of CMP/POR and CA systems.</p> <p>VRAM provides Navy Enterprise and Staff level compliance and scan data reporting capabilities with vulnerability, compliance, and configuration metrics for commands and CMP/POR/CA systems. Configurable reports are available with the ability to drill-down to system, command, and asset levels. Apply for a VRAM account at https://vram.navy.mil)</p>

CLOUD ACRONYMS

ACRONYM	TABLE
A&A	Assessment and Authorization
A&S	Acquisition and Sustainment
AI	Artificial Intelligence
AO	Authorizing Official
API	Application Programming Interface
ATC	Approval to Connect (ATC)
ATO	Authorization to Operate (ATO)
VMA	Assurance Vulnerability Management
BOM	Bill of Materials
CaC	Configuration as Code, or Compliance as Code (depending upon context)
CD	Continuous Delivery
CFR	Change Failure Rate
CI	Continuous Integration
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
CNAP	Cloud Native Access Point
CNCF	Cloud Native Computing Foundation
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction

ACRONYM	TABLE
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSA	Cyber Survivability Attribute
CSP	Cloud Service Provider
CSO	Cloud Service Offering
CSRP	Cyber Survivability Risk Posture
CSSP	Cybersecurity Service Provider
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Test
DCCSCR	DoD Centralized Container Source Code Repository
DCIO	Deputy Chief Information Officer
DBaaS	Database as a Service
DDOS	Distributed Denial of Service
DevSecOps	Development, Security, and Operations
DISA	Defense Information Systems Agency
DNS	Domain Name Service

TERMS OF REFERENCE: DevSecOps

TERM	DEFINITION
DevSecOps	An organizational software engineering culture and practice that aims at unifying software development, security, and operations. The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. In DevSecOps, testing and security are shifted left through automated unit, functional, integration, and security testing – this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously.
Software Artifact	<p>An artifact is a consumable piece of software produced during the software development process. Except for interpreted languages, the artifact is or contains compiled software. Important examples of artifacts include container images, virtual machine images, binary executables, jar files, test results, security scan results, Infrastructure as a Code, documentation, etc. Artifacts are usually accompanied by metadata, such as an ID, version, name, license, dependencies, build date and time, etc.</p> <p>Note that items such as source code, test scripts, configuration scripts, build scripts, and Infrastructure as Code are checked into the source code repository, not the artifact repository, and are not considered artifacts.</p>
Artifact Repository	<p>An artifact repository is a system for storage, retrieval, and management of artifacts and their associated metadata.</p> <p>Note that programs may have separate artifact repositories to store local artifacts and released artifacts. It is also possible to have a single artifact repository and use tags to distinguish the content types.</p>
Bare Metal Bare Metal Server	A bare metal or bare metal server refers to a traditional physical computer server that is dedicated to a single tenant and which does not run a hypervisor (a software program that allows multiple virtual machines (VMs) to run on a single physical server. This term is used to distinguish physical compute resources from modern forms of virtualization and cloud hosting.
Binary or Binary File	Binary refers to a data file or computer executable file that is stored in binary format (as opposed to text), which is computer readable, but not human-readable. Examples include images, audio/video files, exe files, and jar/war/ear files
Build or Software Build	The process of creating a set of executable code that is produced by compiling source code and linking binary code.

TERMS OF REFERENCE: DevSecOps

TERM	DEFINITION
Build Tools	Used to retrieve software source code, build software, and generate artifacts
Continuous Integration/Continuous Delivery (CI/CD) Orchestrator	CI/CD orchestrator is a tool that enables fully or semi-automated short duration software development cycles through integration of build, test, secure, store artifacts tools.CI/CD orchestrator is the central automation engine of the CI/CD pipeline
CI/CD Pipeline	CI/CD pipeline is the set of tools and the associated process workflows to achieve continuous integration and continuous delivery with build, test, security, and release delivery activities, which are steered by a CI/CD orchestrator and automated as much as practice allows.
CI/CD Pipeline Instance	CI/CD pipeline instance is a single process workflow and the tools to execute the workflow for a specific software language and application type for a software component. As much of the pipeline process is automated as is practicable
Cloud Native Computing Foundation (CNCF)	CNCF is an open source software foundation dedicated to making cloud native computing universal and sustainable
CNCF Certified Kubernetes	CNCF has created a Certified Kubernetes Conformance Program. Software conformance ensures that every vendor's version of Kubernetes supports the required APIs. Conformance guarantees interoperability between Kubernetes from different vendors. Most of the world's leading vendors and cloud computing providers have CNCF Certified Kubernetes offerings.
Cloud Native (Architecture)	"Cloud native computing uses an open source software stack to deploy applications as microservices, packaging each part into its own container, and dynamically orchestrating those containers to optimize resource utilization. Cloud native technologies enable software developers to build great products faster."
Code	Software instructions for a computer, written in a programming language. These instructions may be in the form of either human readable source code, or machine code, which is source code that has been compiled into machine executable instructions.

TERMS OF REFERENCE: DevSecOps

TERM	DEFINITION
Configuration Management	Capability to establish and maintain a specific configuration within operating systems and applications.
Container	A standard unit of software that packages up code and all its dependencies, down to, but not including the OS. It is a lightweight, standalone, executable package of software that includes everything needed to run an application except the OS: code, runtime, system tools, system libraries and settings.
Continuous Build	Continuous build is an automated process to compile and build software source code into artifacts. The common activities in the continuous build process include compiling code, running static code analysis such as code style checking, binary linking (in the case of languages such as C++), and executing unit tests. The outputs from continuous build process are build results, build reports (e.g., the unit test report, and a static code analysis report), and artifacts stored into Artifact Repository. The trigger to this process could be a developer code commit or a code merge of a branch into the main trunk.
Continuous Delivery	Continuous delivery is an extension of continuous integration to ensure that a team can release the software changes to production quickly and in a sustainable way. The additional activities involved in continuous integration include release control gate validation and storing the artifacts in the artifact repository, which may be different than the build artifact repository. The trigger to these additional activities is successful integration, which means all automation tests and security scans have been passed. The human input from the manual test and security activities should be included in the release control gate. The outputs of continuous delivery are a release go/no-go decision and released artifacts, if the decision is to release
Continuous Deployment	Continuous deployment is an extension of continuous delivery. It is triggered by a successful delivery of released artifacts to the artifact repository. The additional activities for continuous deployment include, but are not limited to, deploying a new release to the production environment, running a smoke test to make sure essential functionality is working, and a security scan. The output of continuous deployment includes the deployment status. In the case of a successful deployment, it also provides a new software release running in production. On the other hand, a failed deployment causes a rollback to the previous release

TERMS OF REFERENCE: DevSecOps

TERM	DEFINITION
Continuous Integration	Continuous integration goes one step further than continuous build. It extends continuous build with more automated tests and security scans. Any test or security activities that require human intervention can be managed by separate process flows. The automated tests include, but are not limited to, integration tests, a system test, and regression tests. The security scans include, but are not limited to, dynamic code analysis, test coverage, dependency/bill of materials (BOM) checking, and compliance checking. The outputs from continuous integration include the continuous build outputs, plus automation test results and security scan results. The trigger to the automated tests and security scan is a successful build.
Continuous Monitoring	Continuous monitoring is an extension to continuous operation. It continuously monitors and inventories all system components, monitors the performance and security of all the components, and audits & logs the system events.
Kubernetes	Kubernetes is an open-source system that automates the management, scaling, and deployment of containerized applications.

DevSecOps ACRONYMS

ACRONYM	TABLE
A&A	Assessment and Authorization
A&S	Acquisition and Sustainment
AI	Artificial Intelligence
AO	Authorizing Official
API	Application Programming Interface
ATC	Approval to Connect (ATC)
ATO	Authorization to Operate (ATO)
VMA	Assurance Vulnerability Management
BOM	Bill of Materials
CaC	Configuration as Code, or Compliance as Code (depending upon context)
CD	Continuous Delivery
CFR	Change Failure Rate
CI	Continuous Integration
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
CNAP	Cloud Native Access Point
CNCF	Cloud Native Computing Foundation
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction

ACRONYM	TABLE
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSA	Cyber Survivability Attribute
CSP	Cloud Service Provider
CSO	Cloud Service Offering
CSRP	Cyber Survivability Risk Posture
CSSP	Cybersecurity Service Provider
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Test
DCCSCR	DoD Centralized Container Source Code Repository
DCIO	Deputy Chief Information Officer
DBaaS	Database as a Service
DDOS	Distributed Denial of Service
DevSecOps	Development, Security, and Operations
DISA	Defense Information Systems Agency
DNS	Domain Name Service

TERMS OF REFERENCE: DATA

TERM	DEFINITION	SOURCE
Authorization	The process where the database manager gets information about the authenticated user. Part of that information is determining which database operations the user can perform and which data objects a user can access.	https://www.ibm.com/docs/en/db2-big-sql/5.0.2?topic=authorization-database
CEDC	A CEDC is a fixed DoD data center meeting DoD standards for network infrastructure, cybersecurity, technology, and operations and adhering to enterprise governance. They are intended to provide capabilities at an enterprise level. CEDCs will be built to the specifications necessary to deliver the technical and mission capabilities required by the owning Component. CEDCs intended to deliver services across installation boundaries to other entities must be built to meet mission requirements of affected parties. CEDCs will meet DoD standards for cybersecurity. CEDCs will be selected from existing Component data centers.	
Data Attribute	Any distinctive feature, characteristic, or property of a Data Object that can be identified or isolated quantitatively or qualitatively by either human or automated means. A Data Object can be made up of one or more Data Elements, and a Data Element will typically have Data Attributes as sub-units	Department of Defense Data Management Lexicon Memo (June 15, 2020)
Data Element	A discrete unit of data that has a unique meaning within a specific model or schema, and may be comprised of sub-units. Example data elements for a person may include last name, first name, and middle initial.	Department of Defense Data Management Lexicon Memo (June 15, 2020)
Data Entity	A classification [representation] of objects found to exist in the real world as part of describing persons, places, things, concepts, and events of interest to an enterprise function. Ex. Person, Contract, System, Platform, Capability	Derived from: IC DML Derived from: DAMA

TERMS OF REFERENCE: DATA

TERM	DEFINITION	SOURCE
Data Governance	Discipline comprised of responsibilities, roles, functions, and practices, supported by authorities, policies, and decisional processes (planning, setting policies, monitoring, conformance, and enforcement), which together administer data and information assets across an IC Element to ensure that data is managed as a critical asset consistent with the organization's mission and business performance objectives.	Department of Defense Data Management Lexicon Memo (June 15, 2020)
	Data governance provides the principles, policies, processes, frameworks, tools, metrics, and oversight required to effectively manage data at all levels, from creation to disposition. Data governance allows stakeholders to be heard and represented in an organized fashion. For DoD, data governance will be executed at cascading levels, with all issues being resolved at the lowest level possible. Data governance includes localized system decisions affecting data all the way through full records management of critical data assets within the Department. Further, it is essential for data management and records management to be properly implemented throughout the Department.	DoD Data Strategy
Data Model	A representation of the data describing real-world objects and the relationships between the objects, independent of any associated process. A data model includes the set of diagrams for each view along with the metadata defining each object in the model.	Derived from: DAMA
Data Modeler	The data modeler is responsible for reviewing and validating data requirements, providing technical data solutions, and designing logical and physical data structures in support of domain specific needs.	Department of Defense Data Management Lexicon Memo (June 15, 2020)
Data Object	A physical record, row or document representing the actual existence of an entity instance. A data object is made up of one or more data elements. For example, a row within a relational database or an image within an image library.	Derived from: DoD Federated Data Catalog
Data Set	One or more data objects that share common properties and characteristics and are managed as a unit.	Derived from: DoD Federated Data Catalog

TERMS OF REFERENCE: DATA

TERM	DEFINITION	SOURCE
Data Source	A specific data set or repository from which data is originated or collected for subsequent use by consumers. A data source may be the combination of multiple, separate data sets or repositories.	Department of Defense Data Management Lexicon Memo (June 15, 2020)
Data Structure	The physical or logical relationships among data elements that represent a specific, pre-defined schema or data model, used for organizing and storing data, and designed to support specific data manipulation functions. Examples include array, file, record, table, tree, queue, linked list, and edge/node	Department of Defense Data Management Lexicon Memo (June 15, 2020)
Data Type	A category of logical or physical data structures with common properties, uses, and technically feasible operations (e.g. addition, string concatenation) on values. Example data types include numeric, alphanumeric, packed decimal, floating point, date/time.	Department of Defense Data Management Lexicon Memo (June 15, 2020)
Database View	a subset of a database and is based on a query that runs on one or more database tables. Database views are saved in the database as named queries and can be used to save frequently used, complex queries.	https://www.ibm.com/docs/en/control-desk/7.6.1.2?topic=structure-views
Foreign Key	A foreign key is a field (or collection of fields) in a table that refers to the primary key of another table. It establishes relationships between data entities and maintains referential integrity.	https://www.w3schools.com/sql/sql_foreignkey.asp
Index	an efficient way to quickly access the records from the database files stored on the disk drive. It optimizes the database querying speed by serving as an organized lookup table with pointers to the location of the requested data.	https://www.solarwinds.com/resources/it-glossary/database-index
Lineage	A description of data's pathway from its source to its current location and the alterations made to the data along that pathway, which should be represented as a reproducible ancestry of the data object. Lineage can include traceability between parent and children data objects.	Department of Defense Data Management Lexicon Memo (June 15, 2020)

TERMS OF REFERENCE: DATA

TERM	DEFINITION	SOURCE
Master Data	Master Data objects are core business objects used in different application across an organization, along with their associated Meta Data, attributes, definitions, roles, connections, and taxonomies. Master Data represents those "things" that matter most to an organization – those that can be logged in transactions, reported on, measured, or analyzed.	DMBOK 2 nd Edition (Loshin, 2008)
Metadata	<p>Literally, “data about data”; administrative or descriptive data attributes that are consistent across mission and business disciplines, domains, and data encodings, and are used to improve business or technical understanding of data and data-related processes.</p> <p>Information describing the characteristics of data; data or information about data; or descriptive information about an entity’s data, data activities, systems, and holdings.</p>	<p><i>The Intelligence Community Data Management Lexicon, Office of the Director of National Intelligence, dated January 2020</i></p> <p><i>DoD Metadata Guidance Memorandum (March 2023)</i></p>
Primary Key	A primary key is a unique identifier for each record in a data entity. It ensures that each row in a table can be uniquely identified and serves as a reference for relationships with other tables.	
Profile	a set of limits on the database resources and the user password. Once you assign a profile to a user, then that user cannot exceed the database resource and password limits.	https://www.oracletutorial.com/oracle-administration/oracle-create-profile/
Provenance	Description of the origin or source of data, its history of stewardship or custodianship and location(s), which can be used to form assessments about its quality, reliability, or trustworthiness. Within a specific mission context only selective provenance attributes may be considered as relevant.	<i>Department of Defense Data Management Lexicon Memo (June 15, 2020)</i>
Relationships	Describe the types of relationships that can exist between entities, such as one-to-one, one-to-many, or many-to-many.	https://www.solarwinds.com/resources/it-glossary/database-index

TERMS OF REFERENCE: DATA

TERM	DEFINITION	SOURCE
Security	Detail the security measures and access controls relevant to data models to protect sensitive information	
Unique Identifier	An identifier formatted following special conventions to support uniqueness within an organization and across all organizations creating identifiers.	https://csrc.nist.gov/glossary/term/globally_unique_identifier
Version Control	Outline the version control process for data models to manage changes and ensure proper collaboration.	

TERMS OF REFERENCE: INFRASTRUCTURE

TERM	DEFINITION	SOURCE
5ESS	A Class 5 telephone electronic switching system developed by Western Electric for the American Telephone and Telegraph Company	<i>https://dbpedia.org/page/5ESS_Switching_System</i>
Base Level Information Infrastructure (BLII)		<i>Google</i>
Base Modernization (USN Phase 2)	“On-base” (interior) base infrastructure and changing end points (phones, alarm systems, etc.)	<i>OPNAV (Charlie)</i>
Central Exchange (CENTREX)	(this is not CENTRIXS-M) is a base service that is wholly owned by a vendor from PBX to end point. Part of the DISA NETWORKX Contract	<i>PMW790</i>
Circuit	Communication media (usually Fiber). Internal circuit refers to on base media between buildings or to base edge devices. External circuit refers to off base media to DoDIN or industry	<i>OPNAV (Charlie)</i>
Commercial Ethernet Gateway (CEG)	Contract through DISA with industry partners to provide IP external circuit to and from USN installations. Speeds range from 1, 10, or 100 Gigabit offerings. Managed by NCMO and PEO DES for USN.	<i>DISA/NAVIFOR/NCMO</i>
Defense Information Systems Agency (DISA)	Provides a global infrastructure for information sharing and communication across the Department of Defense, from the President down to the lowest level.	<i>Google</i>
Defense Information Systems Network (DISN)	The United States Department of Defense's enterprise telecommunications network for providing data, video, and voice services.	<i>Google</i>
Defense Switched Network (DSN)	Provides the worldwide non-secure voice, secure voice, data, facsimile, and video teleconferencing services for DOD Command and Control (C2) elements, their supporting activities engaged in logistics, personnel, engineering, and intelligence, as well as other Federal agencies.	<i>Google</i>

TERMS OF REFERENCE: INFRASTRUCTURE

TERM	DEFINITION	SOURCE
DoD Information Network (DoDIN)	The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.	<i>Google</i>
DoD365 Integrated Phone Service (DIPS)	An integrated Microsoft's M365 (Teams) product offering for in and outbound phone call processing	<i>OPNAV (Charlie)</i>
Enterprise Classified Voice over IP (ECVoIP)	A technology that allows the user to make C2 voice calls using a broadband Internet connection instead of a regular (or analog) phone line.	<i>Google</i>
Global Network Services(GNS) OCONUS	Contract through DISA with industry partners to provide IP external circuit to and from USN installations.	<i>DISA/NAVIFOR</i>
GSA's Enterprise Infrastructure Solutions(EIS)	Contract through DISA with industry partners to provide IP external circuit to and from USN installations.	<i>DISA/NAVIFOR</i>
Indo-Pacific Transport Services (IPTS)	A contract through Liedos with industry partners to provide IP external circuit to and from USN installations for bases in the IndoPacom AOR	<i>DISA/NAVIFOR</i>
Inquiry/Route/Order(IQO)	Competitive lease contract through DISA with industry partners to provide IP external circuit to and from USN installations.	<i>DISA/NAVIFOR</i>
Internet Protocol Conversion (IPC) (USN Phase 1)	USN effort to allow elimination of legacy external TDM circuits in two parts; 1) insertion of a TDM to IP conversion device (aka. IPC Router or MMGW) 2) replacement of TDM circuit with IP circuit (aka. CEG, MLPS, or IPTS)	<i>OPNAV (Charlie)</i>
Internet Protocol Conversion (IPC) Router	A PMW 790 project for "off-base" IP communications (WAN trunks) via a TDM to IP conversion capability to be placed at critical entry/exit points to connect to an IP Circuit	<i>PMW790</i>
Low Speed TDM (LSTDM)	T-1 and below circuits connected to EOL(2017) Promina devices.	<i>PMW790</i>

TERMS OF REFERENCE: INFRASTRUCTURE

TERM	DEFINITION	SOURCE
Multi-Level Precedence and Preemption (MLPP)	Service allows validated users to place priority calls, and if necessary, to preempt lower-priority calls.	Google
Multi-Media Gateway (MMGW)	A PMW790 project replace PBX switches and convert endpoint TDM signals to IP (e.g. Alarms, Sensors, SCADA/ICS systems)	PMW790
ONE-Net	A contract initiative by the U.S. Navy to provide a unified computing environment to the OCONUS Navy commands.	Google
Pacific Enterprise Services – Hawaii (PES-HI)	Several bases, including joint, located on the island of Hawaii servicing on island bases (including Joint Base Hickam) and Far East OCONUS locations.	OPNAV (Charlie)
Public Exchange System (PBX)	A legacy call management system for TDM phone calls from the end user device in or outbound	OPNAV (Charlie)
Public Safety Answering Points (PSAP)	An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy.	Google
Public Safety Communication (PSC)	Any voice, text, video, or imagery communicated via an information system or network that supports law enforcement, fire and rescue services, emergency medical response, and EM operations on a military installation. Communications may be between individuals or system to system and may be contained within the installation or to mission partners outside the DoD to support mutual-aid agreements, defense support to civil authorities, and other joint response operations.	DoDD 8422.01E
Public Switch Telephone Network (PSTN)	The world's collection of interconnected voice-oriented public telephone networks. PSTN is the traditional circuit-switched telephone network.	Google
Puerto Rico Area Wideband System(PRAWS II)	Contract through DISA with industry partners to provide IP external circuit to and from USN installations.	DISA/NAVIFOR
Regional Unified Capabilities Node (RUCN)	A hub-and-spoke convergence point for Voice and Video into single platform, combining session management systems for VVoIP creating efficiencies.	OPNAV (Clayton)

TERMS OF REFERENCE: INFRASTRUCTURE

TERM	DEFINITION	SOURCE
Session Initiation Protocol (SIP) Trunk	An IP data connection to establish calls to a PBX to replace Public Switching Telephone Network (PSTN)	Google
Switch	A switch routes and connects end user calls/device connects with a larger enterprise.	OPNAV (Chris/Clayton)
Time-Division Multiplexing (TDM)	1) A method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. 2) Legacy protocol for analog data transfer historically used for telephone, alarm, and sensing data	1) https://www.techtarget.com/whatis/definition/time-division-multiplexing-TDM?Offer=abt_pubpro_AI-Insider 2) OPNAV (Charlie)
Voice over IP (VoIP)	A technology that allows the user to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.	Google
Voice over Secure IP (VoSIP)	Technology used to securely transmit voice communications, but with VoSIP, the security is provided by separate devices in the network (such as network encryptors) rather than the secure phones themselves.	Google

TERMS OF REFERENCE: NETWORKS

TERM	DEFINITION	SOURCE
Network Operations	The Network operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain cyberspace and to create and preserve the confidentiality, availability, and integrity of a given network.	
Zero Trust	An evolving set of CS paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.	CNSSI 4009 (CNSSI Named Source - NIST SP 800-207)

TERMS OF REFERENCE: PORTFOLIO MANAGEMENT

TERM	DEFINITION	SOURCE	URL
DITPR	DoD IT Portfolio Repository	DITPR Guidance Memo	DITPR Guidance Memo 20090810.pdf
DITPR-DON	DoD IT Portfolio Repository Department of the Navy	DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY PORTFOLIO REPOSITORY - DEPARTMENT OF THE NAVY (DITPR-DON) PROCESS GUIDANCE (VI.0)	DITPR-DON Process Guidance (v1.0)_20111128_signed_memo.pdf
DADMS	DON Application and Database Management System	DITPR/DADMS front page	DITPR/DADMS Integrated IT Portfolio Management (navy.mil)
BMA	Business Mission Area. The BMA ensures that the right capabilities, resources, and materiel are reliably delivered to our warfighters: what they need, where they need it, when they need it, anywhere in the world. In order to cost-effectively meet these requirements, the DoD current business and financial management infrastructure - processes, systems, and data standards - are being transformed to ensure better support to the warfighter and improve accountability to the taxpayer. Integration of business transformation for the DoD business enterprise is led by the Deputy Secretary of Defense in his role as the Chief Operating Officer of the Department.	DoDI 8115.02; IT PFM Implementation	DoDI 8115.02 - IT PfM Implementation.pdf
DIMA	DoD portion of Intelligence Mission Area. The DIMA includes IT investments within the Military Intelligence Program and Defense component programs of the National Intelligence Program. The USD(I) has delegated responsibility for managing the DIMA portfolio to the Director, Defense Intelligence Agency, but USD(I) retains final signature authority. DIMA management will require coordination of issues among portfolios that extend beyond the Department of Defense to the overall Intelligence Community.	DoDI 8115.02; IT PFM Implementation	DoDI 8115.02 - IT PfM Implementation.pdf

TERMS OF REFERENCE: PORTFOLIO MANAGEMENT

TERM	DEFINITION	SOURCE	URL
EIEMA	Enterprise Information Environment Mission Area. The EIEMA represents the common, integrated information computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, provide transport for, and/or assure local area networks, campus area networks, tactical operational and strategic networks, metropolitan area networks, and wide area networks. The EIE includes computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DoD enterprise hardware, software operating systems, and hardware/software support that enable the GIG enterprise. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG.	DoDI 8115.02; IT PFM Implementation	DoDI 8115.02 - IT PfM Implementation.pdf
WMA	Warfighting Mission Area. The WMA provides life cycle oversight to applicable DoD Component and Combatant Commander IT investments (programs, systems, and initiatives). WMA IT investments support and enhance the Chairman of the Joint Chiefs of Staff's joint warfighting priorities while supporting actions to create a net-centric distributed force, capable of full spectrum dominance through decision and information superiority. WMA IT investments ensure Combatant Commands can meet the Chairman of the Joint Chiefs of Staff's strategic challenges to win the war on terrorism, accelerate transformation, and strengthen joint warfighting through organizational agility, action and decision speed, collaboration, outreach, and professional development.	DoDI 8115.02; IT PFM Implementation	DoDI 8115.02 - IT PfM Implementation.pdf

TERMS OF REFERENCE: PORTFOLIO MANAGEMENT

TERM	DEFINITION	SOURCE	URL
OSS	Open Source Software. Public Law 115-232 defines OSS as “software for which the human-readable source code is available for use, study, re-use, modification, enhancement, and re-distribution by the users of such software”. This definition is essentially identical to what the DoD has been using since publication of the 16 October 2009 memorandum from the DoD CIO, “Clarifying Guidance Regarding Open Source Software (OSS)”.	<i>DoD CIO FAQ Page</i>	Open Source Software FAQ (defense.gov)
Portfolio	The collection of capabilities, resources, and related investments that are required to accomplish a mission-related or administrative outcome. A portfolio includes outcome performance measures (mission, functional, or administrative measures) and an expected return on investment. “Resources” include people, money, facilities, weapons, IT, other equipment, logistics support, services, and information. Management activities for the portfolio include strategic planning, capital planning, governance, process improvements, performance metrics/measures, requirements generation, acquisition/development, and operations.	<i>DoDI 8115.02; IT PFM Implementation</i>	DoDI 8115.02 - IT PFM Implementation.pdf
BEA (DoD)	Business Enterprise Architecture In accordance with 10 U.S.C. § 2222(c), the BEA is the enterprise architecture developed and maintained as a blueprint to guide the development of integrated business processes within the DoD. It must be sufficiently defined to effectively guide implementation of interoperable defense business system solutions and consistent with the policies and procedures established by the Director of the Office of Management and Budget. The BEA is the DoD’s blueprint for improving DoD business operations and the reference model for DBC certification.	<i>Defense Business Systems Investment Management Guidance, V4.1, June 2018</i>	DBS Investment Management Guidance.docx (defense.gov)

TERMS OF REFERENCE: PORTFOLIO MANAGEMENT

TERM	DEFINITION	SOURCE	URL
NSS	National Security System The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).	Title 44; §3552. Definitions; CHAPTER 35-COORDINATION OF FEDERAL INFORMATION POLICY SUBCHAPTER II-INFORMATION SECURITY	44 USC 3552: Definitions (house.gov)
Business System	Business systems are information systems that are operated by, for, or on behalf of the Department of Defense, including: financial systems, financial data feeder systems, contracting systems, logistics systems, planning and budgeting systems, installations management systems, human resources management systems, and training and readiness systems. A business system does not include a national security system or an information system used exclusively by and within the defense commissary system or the exchange system or other instrumentality of the DoD conducted for the morale, welfare, and recreation of members of the armed forces using nonappropriated funds.	DoDI 5000.75	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF

TERMS OF REFERENCE: PORTFOLIO MANAGEMENT

TERM	DEFINITION	SOURCE	URL
BCAT	Business system Category	DoDI 5000.75	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF
BCAT I	Priority defense business system expected to have a total amount of budget authority over the period of the current Future Years Defense Program (FYDP) in excess of \$250,000,000; or DoD CMO designation as priority based on complexity, scope, and technical risk, and after notification to Congress.	DoDI 5000.75	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF
BCAT II	Does not meet criteria for category I. Expected to have a total amount of budget authority over the period of the current FYDP in excess of \$50,000,000.	DoDI 5000.75	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF
BCAT III	Does not meet criteria for category II.	DoDI 5000.76	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF
JCA	Joint Capability Area – Collections of like DoD capabilities functionally grouped to support capability analysis, strategy development, investment decision making, capability portfolio management, and capabilities-based force development and operational planning. JCAs provide a common capabilities language for use across the activities and processes of the DoD.	CJCSI 5123.01I	Instructions, Manuals, and Notices (jcs.mil)

