NAVY BLUEPRINT

For a Modern Enterprise Information Ecosystem

VERSION 1.0 - SEPTEMBER 2023

DISTRIBUTION STATEMENT D. DISTRIBUTION AUTHORIZED TO DEPARTMENT OF DEFENSE (DOD) AND U.S. CONTRACTORS ONLY. TECHNICAL OR OPERATIONAL, 29 SEPTEMBER 2023. OTHER REQUESTS MAY BE REFERRED TO THE DIRECTOR ENTERPRISE NETWORKS AND CYBERSECURITY. HEADQUARTERS U.S. NAVY, 2000 NAVY PENTAGON, WASHINGTON, DC 20350-2000.

MESSAGE FROM
OPNAV N2N6

Jennifer L. Edgin, SES
Assistant 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 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 connected 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 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.

This Navy Blueprint for a Modern Enterprise Information Ecosystem builds on decades of constant effort to improve our information systems, infrastructure, and processes. From the creation of the then-revolutionary Navy Marine Corps Intranet, to the consolidation of over 2,000 network environments, and on to current efforts to move to the Cloud; it is now time to build on those successes and lessons learned and rapidly accelerate our modernization approaches so that the Navy is positioned to out-maneuver and outpace our competitors.

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

This is just the first step. Implementation plans and additional updates will follow. This will be a living document that provides the framework for continued improvement. Use it as your sailing direction for managing our Enterprise Information Ecosystem for warfighting success.

PLANNED TABLE OF CONTENTS

FOUNDATIONAL TENETS

MODERNIZATION TENETS

INFORMATION GOVERNANCE

IMPLEMENTATION OF ECOSYSTEM MODERNIZATION

*Individual modernization implementation plans projected for V1.1 of the Navy Service Blueprint pending inputs from Navy Commands

NAVY BLUEPRINT GLOSSARY

INTRODUCING THE NAVY BLUEPRINT

NAVY BLUEPRINT: DEFINED

WHAT IS THE NAVY BLUEPRINT?

- The Navy Blueprint is the unifying technical outline and business model documenting the design of the Navy's IT Enterprise. It captures the policies, standards, services, infrastructure, technical design, and assets that deliver IT capabilities to users across the enterprise. The Blueprint shall serve as an iterative, and evolving record that documents the Navy's information system architecture, objectives, and mission requirements related to its IT portfolio. The Blueprint's aim is to provide a holistic summary and guide to the Navy Enterprise Information Ecosystem.
- The Navy Blueprint is informed by the current state of the Navy's IT structure and governance, as captures future vision and modernization initiatives aimed at unifying architectures across operating forces, platforms, and services. It shall serve as a reference document to the larger information warfare community; enabling all components to leverage IT tools, information, and services where they need them. The Blueprint contents support key decision-making processes within the Navy and sets the foundation for an iterative functional design approach to define requirements and capabilities.

PURPOSE

The Navy Blueprint informs enterprise IT investments and implementation and sets a common lexicon for IT modernization

END STATE

Navy will deliver and sustain secure, resilient, survivable, integrated, and interoperable mission performance through out the life cycle of information systems

HOW TO UTILIZE THE NAVY BLUEPRINT

The Navy Blueprint contains a set of views to assist the reader in understanding and visualizing a modern Navy Enterprise Information Environment. These provided fit-for-purpose views show the core business processes and how they are executed within an efficient Information Technology environment.

Use the Navy Service Blueprint as the basis for planning and decision making related to:

- **Identifying capability gaps** to drive Research and Development (R&D) priorities.
- **Leveraging emerging technology** to better manage Navy information and consistently integrating those technologies into the ecosystem.
- Achieving economies of scale and **reducing redundancy** by sharing services across the enterprise.
- **Improving organizational communication** through a standardized vocabulary.
- Improving consistency, accuracy, timeliness, quality, availability, access, and **sharing of information**.
- **Prioritizing innovation** efforts.

The future state of warfare requires the Navy to **think differently**, **encourage innovation**, and embrace **new business models** for change that focus on enhancing access, capabilities, and user experience throughout the Information Environment. This blueprint unites and aligns efforts to digitally equip the Navy for the future.

NAVY ENTERPRISE INFORMATION ECOSYSTEM

NAVY ENTERPRISE INFORMATION ECOSYSTEM

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 address a mission.

This ecosystem is made up of tangible elements such as physical information systems and networks, and intangible elements, such as visualizations of information and workflows.

The Enterprise Information Ecosystem serves both as a foundation for all Navy business and mission functions, and the critical investment in the Navy Information Warfare posture.

Critical to this ecosystem view, is the level of interaction and dependency that exists between applications, systems, and assets in support of a user goal.

7 LAYERS OF THE OSI MODEL

APPLICATION
- End User layer
- HTTP, FTP, IRC, SSH, DNS

PRESENTATION
- Syntax layer
- SSL, SSH, IMAP, FTP, MPEG, JPEG

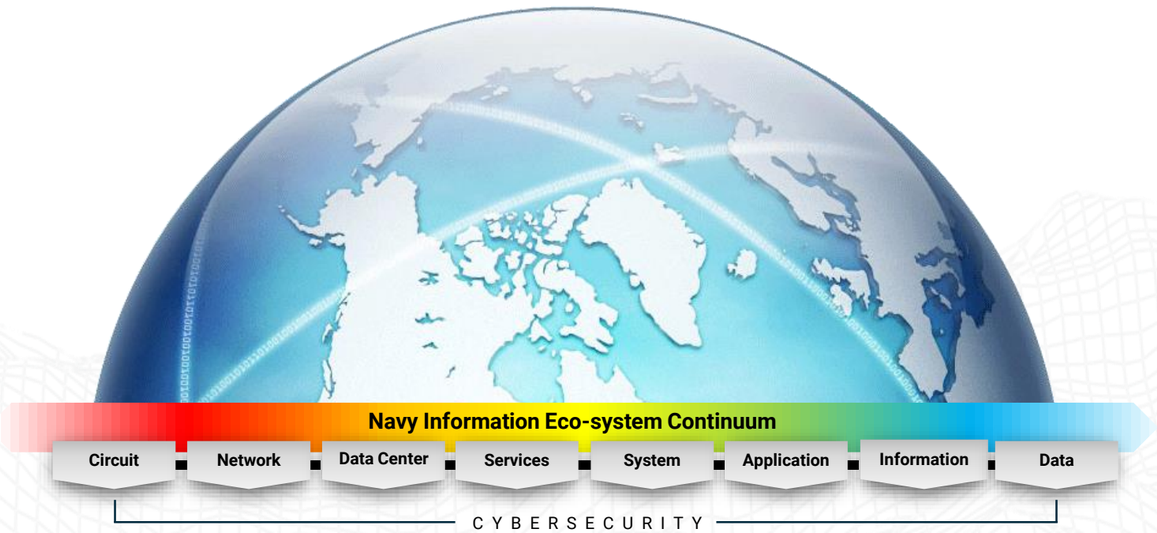
SESSION
- Synch & send to port
- API's, Sockets, WinSock

TRANSPORT
- End-to-end connections
- TCP, UDP

NETWORK
- Packets
- IP, ICMP, IPSec, IGMP

DATA LINK
- Frames
- Ethernet, PPP, Switch, Bridge

PHYSICAL
- Physical structure
- Coax, Fiber, Wireless, Hubs, Repeaters



MISSION

Navy will deliver and sustain secure and interoperable 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. Information Ecosystem Modernization
2. Zero Trust Implementation
3. Cyber Ready Transformation

DEFINING STRATEGIC PRIORITIES & DESIRED OUTCOMES

INFORMATION ECOSYSTEM MODERNIZATION

- Migrate towards a modern information system architecture with upgraded, resilient infrastructure adept to meet the needs of modern day information warfare. These capabilities include:
  - TDM-IP
  - Network Modernization
  - Cloud Migration
  - Data Center Consolidation
  - System Rationalization in support of modernization

DESIRED OUTCOME:

Cost effective delivery of effective state-of-the-art information systems leveraging enterprise architectures where possible

ZERO TRUST IMPLEMENTATION

- Threats exist both inside and outside traditional network boundaries
- The Zero Trust Architecture security model **assumes that a breach is inevitable** or has **likely already occurred**
  - Constantly limits access to only what is needed
  - Looks for anomalous or malicious activity
- Focus on **protecting data in real-time** within a dynamic threat environment
- Data-centric security model
  - **Least privileged access** applied for every access decision
  - **Who, what, when, where, and how** are critical for appropriately allowing or denying access

DESIRED OUTCOME:

A resilient enterprise architecture designed with security at the core of infrastructure, network, system, application and data delivery

CYBER READY TRANSFORMATION

- Cyber Ready is our ongoing effort to **shift cybersecurity away from rote compliance** bureaucracy and towards a “cyber ready” state that **enables acquisition speed and better defends** the service’s information.
- Cyber Ready seeks to change acquisition leverage the cybersecurity requirements "baked in" to meet the intent of Risk Management Framework which enables
  - **Integration** of cybersecurity into existing processes
  - Utilization of **cybersecurity testing and validation** to support **risk decisions** and inform future development
- Cyber Ready will apply a model of currency so that programs **continue to earn and re-earn** their authorization every day through establishing **ongoing awareness of risk**

DESIRED OUTCOME:

Deliver and maintain secure and resilient systems while maintaining a real-time awareness of cybersecurity risk

ENTERPRISE INFORMATION ECOSYSTEM REFERENCE ARCHITECTURE

REFERENCE ARCHITECTURE DEFINITION AND PURPOSE

DEFINITION

A Reference Architecture provides a template solution for an information system implementation across a particular domain. It uses various perspectives and templates 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.

GOALS/OBJECTIVES

- Adopting an Enterprise Reference Architecture has common benefits:
  - improvement of the interoperability of the information systems by establishing a standard solution and common mechanisms for information exchange
  - reduction of the development costs of software projects through the reuse of common assets
  - improvement of the communication inside the organization because stakeholders share the same architectural mindset
- Components should be distributed and scaled according to their mission across Navy components including enterprise, operational, and tactical nodes, with each component leveraging the services of its supporting organizations, while maintaining localized control of its unique assets for administration and management.

HOW TO USE A REFERENCE ARCHITECTURE

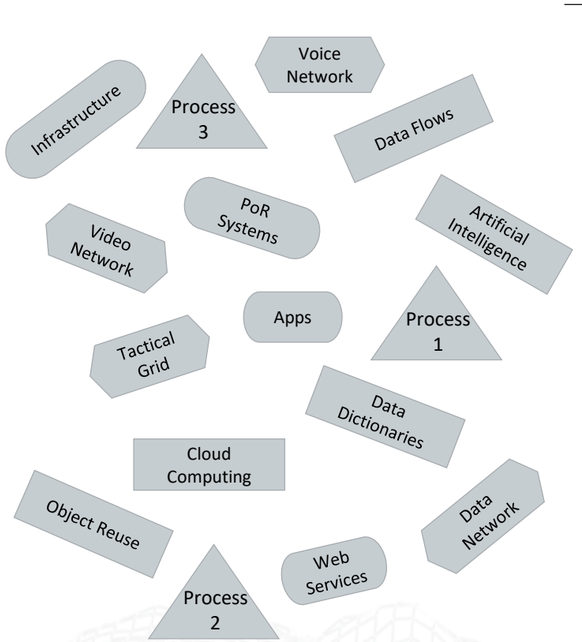
The Navy Blueprint Enterprise Reference Architecture serves as a starting point for system design and implementation of new technologies. The reference architecture will provide recommended solutions to avoid "reinventing the wheel," as well as providing standard product lines and network views for which a system can easily integrate to leverage common enterprise investments and ultimately reduce the need for bespoke information services.

To leverage this reference architecture:

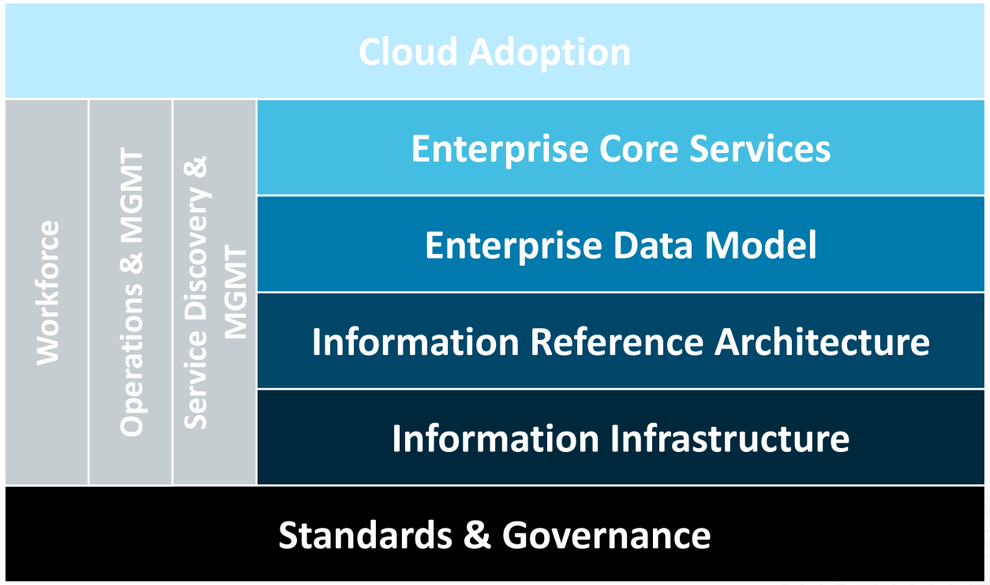
1. Characterize systems along TBM model,
2. Align system components to portfolio product lines,
3. Identify common architectural solutions where available

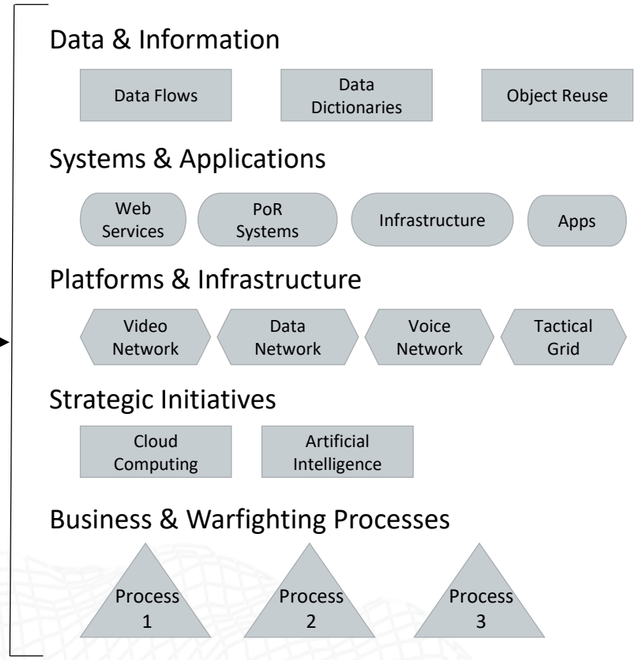
ENTERPRISE ARCHITECTURE END STATE:
WARFIGHTING SUCCESS

A unified Enterprise Architecture organizes and re-structures stove-piped, fragmented capabilities and standardizes ad-hoc process. 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.



Non-Integrated Processes & Systems in Different Parts of the Enterprise



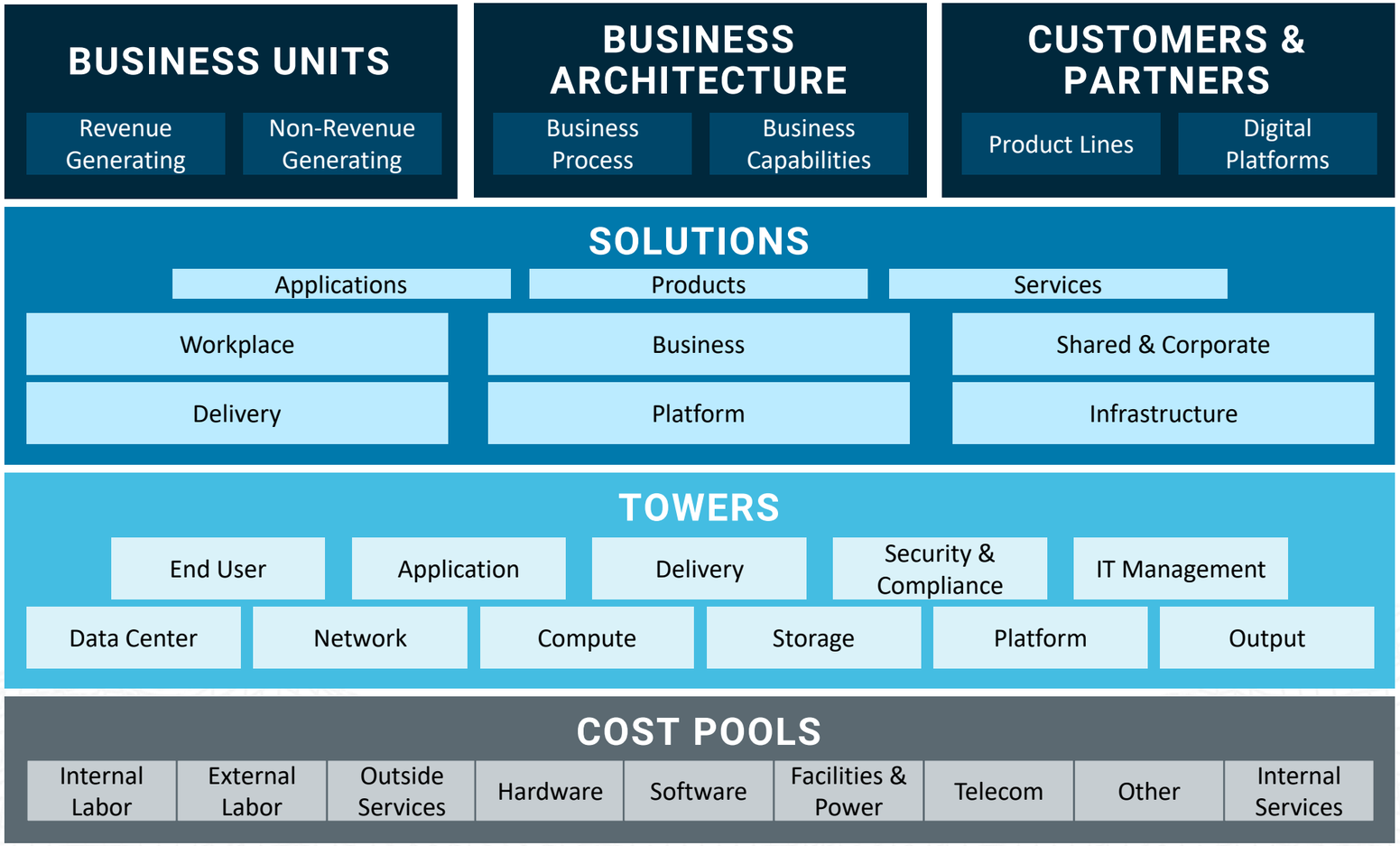


Integrated Process & Systems Across the Entire Enterprise

Enterprise Architecture

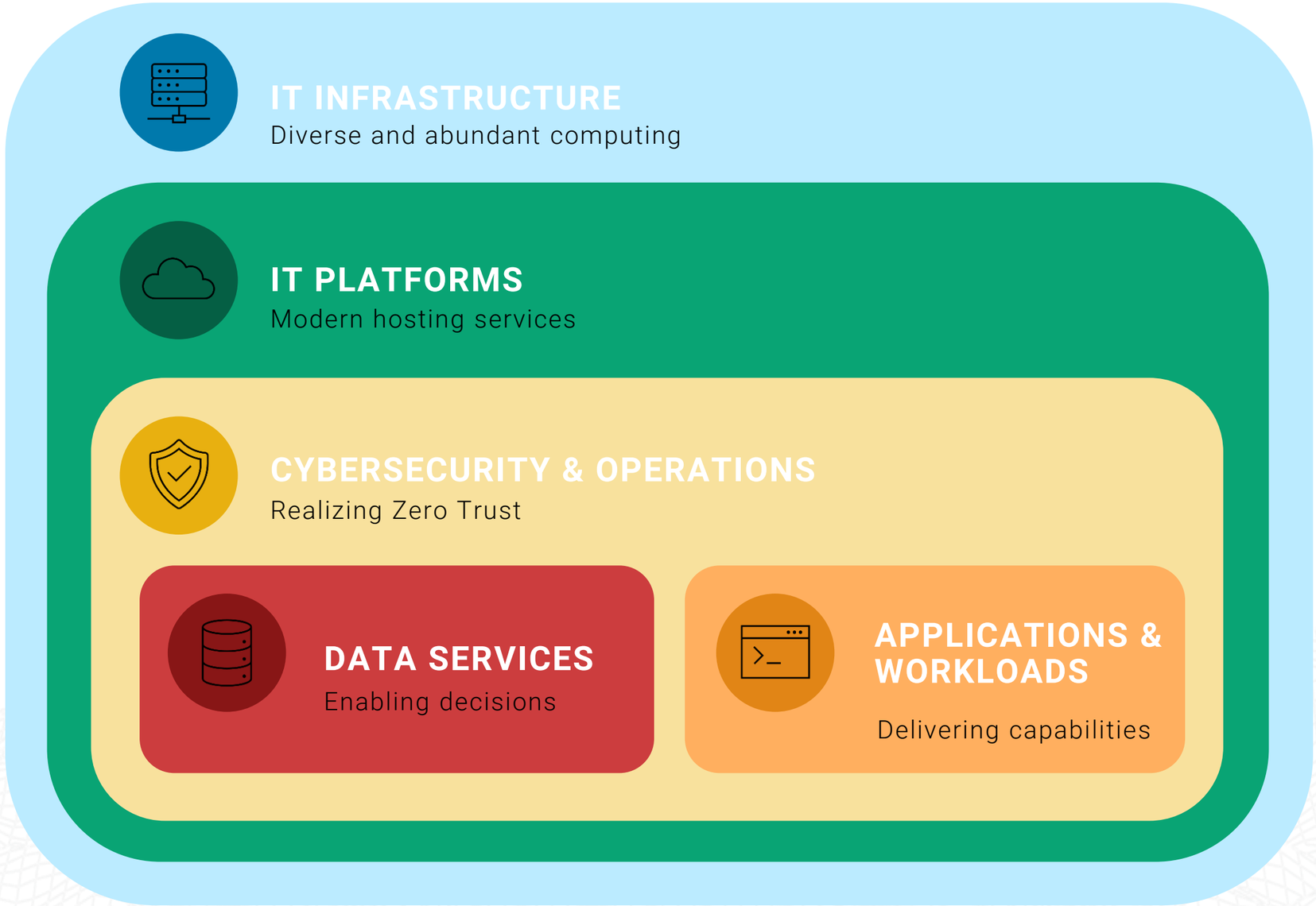
A UNIFIED LEXICON FOR PORTFOLIO MANAGEMENT OF INVESTMENTS SUPPORTING FINANCIAL SUCCESS

TECHNOLOGY BUSINESS MANAGEMENT (TBM) 4.0



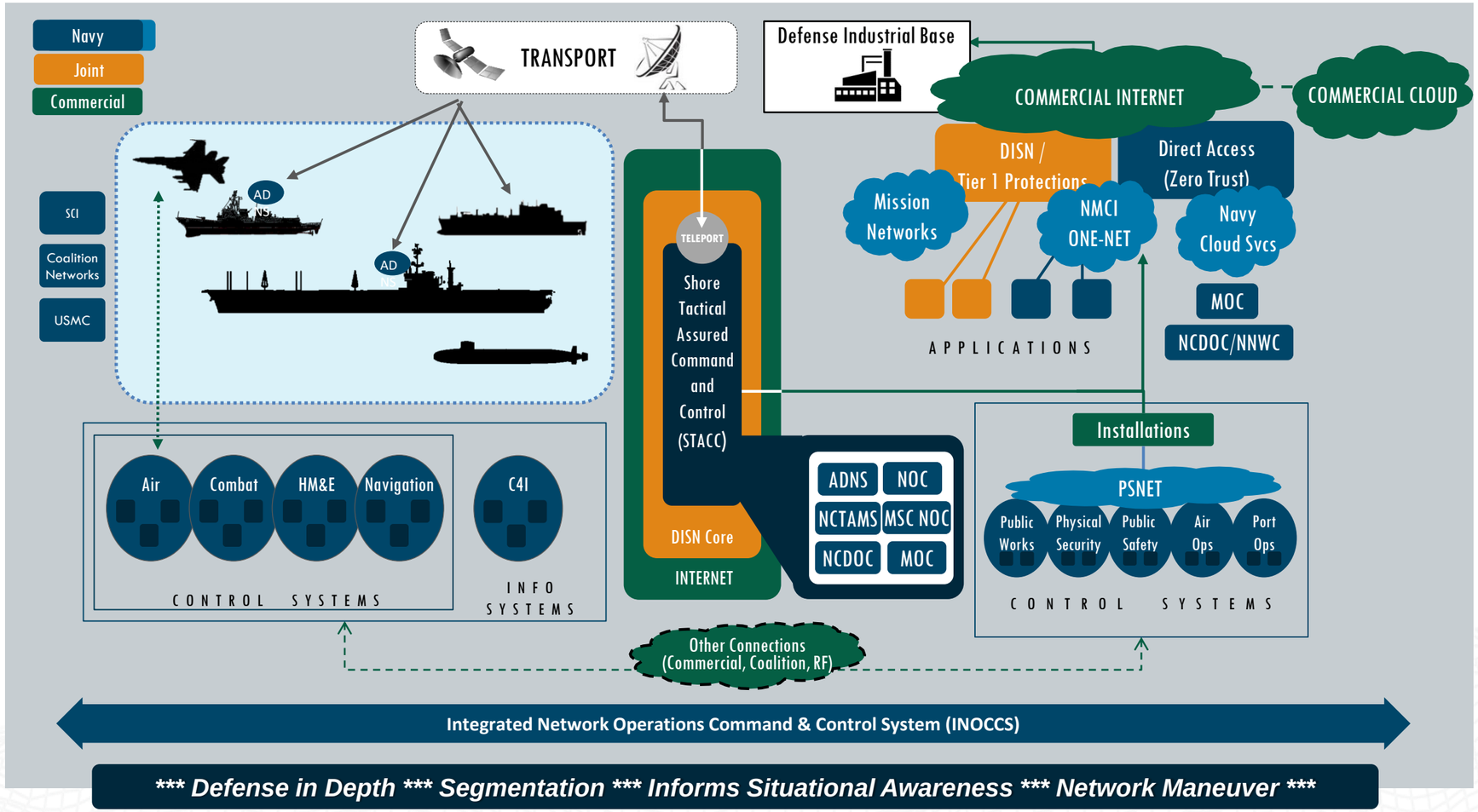
- TBM 4.0 implementation required by OMB A-11 Section 55 (2022)
- Navy implementation of TBM in IT asset management provides a solution to support Navy IT investment planning along product lines
- By aligning to the TBM framework, Navy portfolio and financial management are aligned utilizing terms that map to enterprise architecture and portfolio product lines

PORTFOLIO PRODUCT LINES



- Portfolio Product Lines as identified will provide **architectural categories for investment**, characterizing assets and services across the information ecosystem continuum.
- The diagram indicates the **hierarchical relationship** between these product lines from infrastructure to enterprise services serving cybersecurity, data and applications.
- By utilizing Portfolio Product Lines and the TBM framework for financial management, we can trace the impact of investments to delivery of components of the Navy Enterprise Information Ecosystem

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
- Understanding the total picture of the as-is enterprise information ecosystem, allows for the definition of individual reference architectures applied to various workflows throughout this OV-1

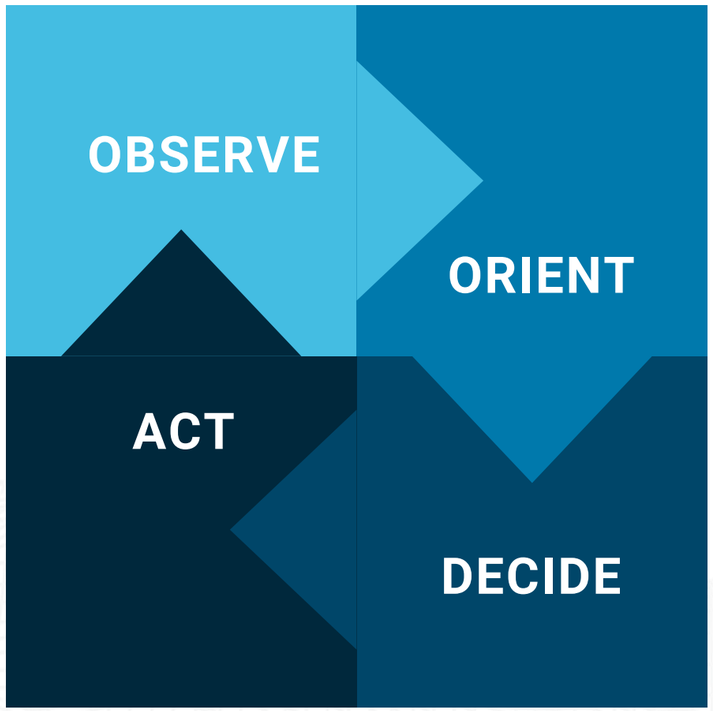
ENTERPRISE DATA MODEL

THE IMPORTANCE OF DATA MANAGEMENT

EFFECTIVE DATA MANAGEMENT INCREASES MILITARY ADVANTAGE

In today's warfighting environment, the ability to leverage data throughout the Navy enterprise is imperative for rapid decision-making and delivering military advantage that outpaces our adversaries.

We must ensure access to and the availability of the right data, at the right time, and where it is needed to deliver competitive military advantage at the speed of relevance.



- **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.

THE VALUE OF DATA IS DETERMINED BY ITS ACCELERATION OF EFFECTIVE WARFIGHTING ACTION

TARGET ENTERPRISE DATA FRAMEWORK

1 CREATE

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

2 CURATE

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

3 CONSUME

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

DATA CONSUMPTION: KEY ROLES

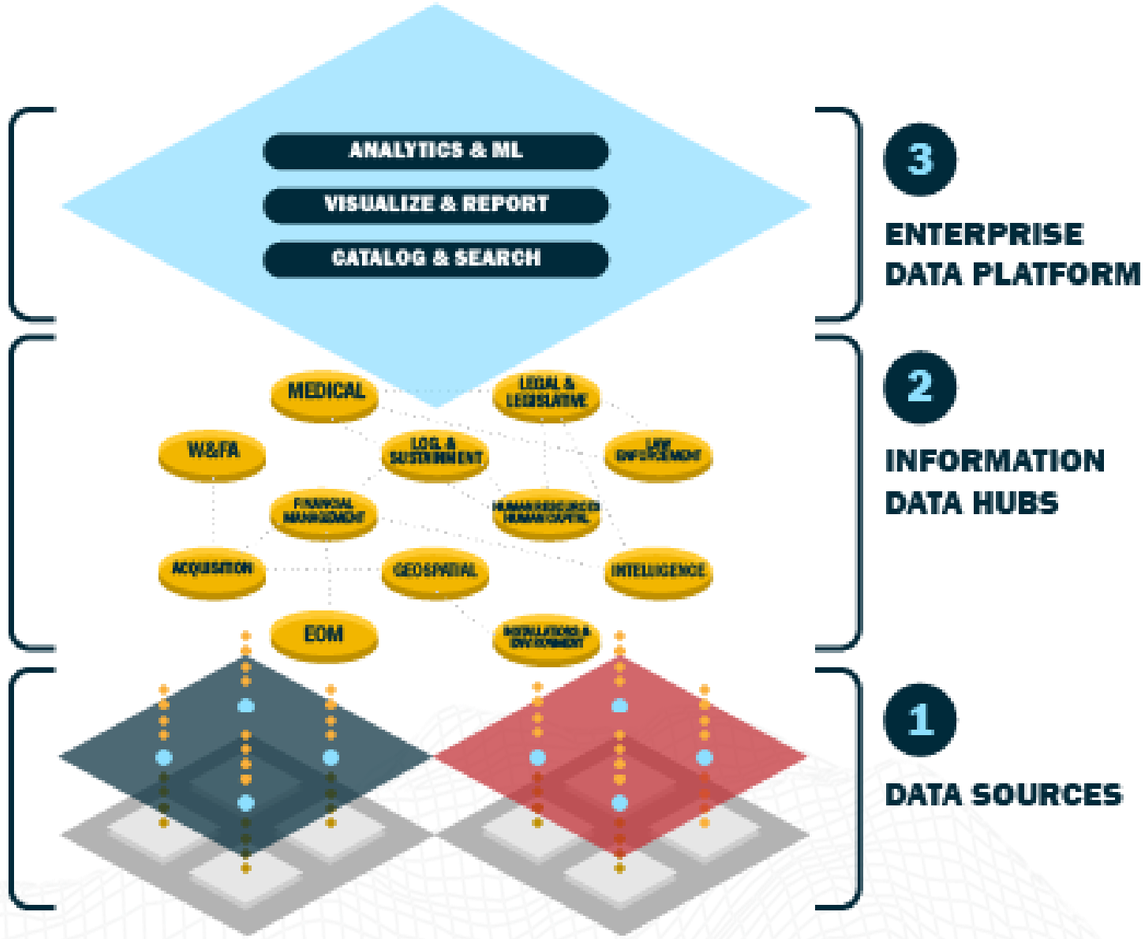
- Mission Owner
- Data Consumer
- Data & Analytics Specialist

DATA CURATION: KEY ROLES

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

DATA CREATION: KEY ROLES

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



ENTERPRISE DATA MODEL

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. This data model will pull key data attributes from various data sets hosted in data sources across the enterprise, to describe authoritative data attributes fit for purpose, and serve as an data integration map from originating data sources to authoritative data sets, no matter the distribution of attributes between systems.

Once this enterprise data model is identified, data standards can me developed or adopted from industry and applied to data sources, or captured as requirements for future data management investments to either modernize or sunset legacy data platforms which do not support enterprise-wide data discovery, access controls, and security needs.

PHASE 1: CONCEPTUAL MODEL

- Assign properties for each component
- Identified data relationships

PHASE 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

PHASE 3: PHYSICAL MODEL

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

ENTERPRISE MICROSERVICES MODEL

ESTABLISHING AN ENTERPRISE MICROSERVICES MODEL

MICROSERVICE MODELS AND STRATEGIES ALIGN CAPABILITIES

With the focus on mission, the Blueprint Reference Architecture is driven by requirements set forth in an Enterprise Microservices Model. This model defines a collection of information microservices which must **work together** to deliver capabilities addressing strategic priorities along cybersecurity, delivery of applications, and management of data to meet the needs of analysts, leaders, and supporting organizations.

Microservices can be characterized across various categories shown here, to describe **core functionalities that can be reused across various workflows** in the Enterprise Information Ecosystem to deliver **warfighting success.**

SOFTWARE AS A SERVICE	Provides software to users through a thin client (e.g. web browser) or program interface
DATA AS A SERVICE	Provides centralized data management services for cleansing, engineering, and transport to different systems, applications, and users.
SECURITY AS A SERVICE	Provides managed security services, such as cross-domain security, virus scanning, and patch management
PLATFORM AS A SERVICE	Provides services to develop, run, and manage applications, such as operating systems, middleware, and databases
INFRASTRUCTURE AS A SERVICE	Provides the foundational components that enable other services to work, such as power, processing, networking, and storage

ENTERPRISE MICROSERVICES ARE **DISCOVERABLE, REUSABLE,** AND **CAN BE UTILIZED BY ANY ENTITY**

ENTERPRISE REPRESENTATIVE MICROSERVICES & SERVICES CATALOG

THE CATALOG PROVIDES A FRAMEWORK FOR END STATE INFORMATION SERVICES DESCRIBING THE LIST OF FUNCTIONS WHICH CAN BE COMBINED TO DELIVER MISSION OUTCOMES.

SOFTWARE AS A SERVICE

Collaboration:
- Email
- Instant Messaging
- Web Conferencing
- Wiki

Planning & Collection:
- Collection Planning
- Production Planning
- Requirements Management
- Support to Targeting
- Supporting to Operations

Collection, Processing & Exploitation:
- Collection Management
- Sensor Control
- Asset Management
- Exploitation
- Processing Services

Production & Analysis:
- Predictive Analytics
- Advanced Analytics
- Product Development
- Translation Services
- Fusion Services
- Correlation

DATA AS A SERVICE

Data Discovery:
- Content Search
- Brokered Search
- Data Visualization
- Data Mediation
- Data Publishing
- Data Dissemination

Data Analysis:
- Data Mining
- Data Correlation
- Data Aggregation
- Data De-Duplication

Data Access & Organization:
- Metadata Tagging
- Data Storage
- Data Enrichment
- Data Processing

Data Standards:
- Metadata Standards
- Master Data
- Enterprise Data Model
- Data Taxonomy
- Cross-Domain Solution

SECURITY AS A SERVICE

Governance:
- Mediation
- Exception Management Policy Definitions
- Service Level Agreements
- Security Standards

Monitoring:
- Auditing
- Intrusion Detection
- Alert Management
- Service Agreement
- Access Monitoring
- Activity Management
- Malware/Virus Protection

Security:
- Authentication
- Authorization
- Identity Management
- Encryption
- Policy Enforcement
- Certificate Management
- Vulnerability Assessment

Incident Response:
- Forensics
- Security Routing/Brokering
- Threat & Vulnerability

PLATFORM AS A SERVICE

Provision/Monitoring:
- Capacity Management
- Load Balancing
- Scaling Integration
- Health Monitoring

Application Environment:
- Database
- Middleware
- Content Delivery
- Map Servers
- Configuration Management
- Service Bus

Development Environment:
- Web Servers
- Integration Services
- Release/Deploy Services

Operating Environment:
- Virtualized OS
- Virtual Desktop

INFRASTRUCTURE AS A SERVICE

Virtualization:
- Hypervisor
- Host Operating Systems

Hardware:
- Storage
- Computer Network
- Network Management
- Security Appliances
- Host Servers
- Switches

Facilities:
- Cooling
- Power Supplies
- Cabling
- Routing

Requirements:
- Electricity
- Buildings
- Internet Connectivity

HOW TO LEVERAGE THE SERVICES CATALOG

When developing solutions to address mission outcomes, **the services catalog serves as a "shopping list"** of characterized activities/products, which can be combined through assets to address mission need. In addition to this catalog, several tools can be leveraged to help define requirements and ensure **alignment to the Navy's Enterprise Architecture**.

SERVICE INTERACTION PATTERNS

- Trace user actions throughout components of the enterprise architecture
- Identify common critical assets and implementation requirements

LOGICAL RELATIONSHIP DIAGRAMS

- Highlight the interactions and dependencies of between services needed to deliver capabilities across the enterprise
- Identifies actions, assets, and actors that facilitate the codification of expected behaviors between components

DATA FLOW DIAGRAMS

- Support master data model development and identification of master data entities
- Drive database consolidation toward designated authoritative data sources

SERVICES MODELS ALL DRIVE TOWARD MISSION OUTCOMES

Effectiveness of implemented services can be defined utilizing **mission outcome driven metrics**:

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)

INFORMATION GOVERNANCE

AS IS INFORMATION GOVERNANCE FORUMS

CYBERSECURITY SENIOR OVERSIGHT COMMITTEE

CURRENT: Collaboration forum for peer Authorizing Officials that provides oversight of risk management framework decisions.

VISION: Authoritative decision making body for IT governance, responsible for enterprise risk decisions and cyber requirement prioritization and advocacy.

IT CYBERSECURITY TECHNICAL ADVISORY BOARD

CURRENT: Forum for the CHENGs to develop technical standards for USN.

VISION: Forum for the CHENGs to develop technical standards for USN, providing recommendations on evolving standards to the Oversight Committee.

Problem: Existing Information Governance is siloed and disjointed across subject areas and topical priorities

Future: Maximize existing forums to establish a unified Information Governance

OPNAV CYBERSECURITY CROSS FUNCTIONAL TEAM

CURRENT: A CFT with representation from all resource sponsors responsible for coordinating cyber priorities during the POM.

VISION: Collaboration forum for resource sponsors to discuss cyber requirements and provide recommendations on prioritization, as well as elevate funding concerns.

INVESTMENT REVIEW BOARD STEERING COMMITTEE

CURRENT: IT Portfolio management forum for reviewing portfolio investments and validating those investments toward enterprise solutions.

VISION: Authoritative decision making body for IT portfolio management and investment across lines of business.

DATA GOVERNANCE BOARD

CURRENT: DON Information Domain Steward authoritative body providing oversight of data management and analysis priorities.

VISION: Decision making body for enterprise data services and advising community for data governance across information portfolio.

AUTHORIZING OFFICIAL REPRESENTATIVE WORKING GROUP

CURRENT: Collaboration forum to discuss ongoing risk management framework efforts.

VISION: Decision making body for risk management framework decisions and changes.

INFORMATION GOVERNANCE VISION

Navy Information Governance is currently distributed across a range of bodies each focused on specific aspects of IT management but without any overarching oversight to integrate those singular aspects into a broader operational picture.

As Navy transforms its Enterprise Information Ecosystem, the governance structures must transform into a federated approach which reflects the multifaceted reality of IT authorities. Oversight for cybersecurity, IT portfolio management, risk management, and resourcing decisions will be unified within a clear hierarchy to allow for accountability.

In order to propel the portfolio forward, communication lines within this hierarchy must be formalized in order to allow stakeholders across the spectrum, from TYCOMs/Fleets to CHENGs to resource sponsors, to coordinate their concerns and develop a holistic governance vision.

GOVERNANCE GOAL

Navy will develop an Information Governance structure which integrates and aligns all key stakeholders to ensure communication and accountability.

IMPLEMENTATION OF ECOSYSTEM MODERNIZATION

TRANSFORMATION APPROACH

TRANSFORMATION AND WHY IT IS NEEDED

The Navy information ecosystem modernization is a holistic transformation approach implementing scaled incremental change from a history of legacy enclave systems to an enterprise services model aligning people, processes, capabilities, and data.

Transitioning from our current legacy architecture to a cloud-first service model to address the variety of Navy mission outcomes requires more than just a migration of data and applications to a remotely hosted environment. This migration requires infrastructure assessment and improvement, security posturing, and strategic risk management, as well as a careful consideration of effective implementation timelines balanced with highly constrained resource limitations.

All challenges noted, the transformation to a cloud-first service foundation will enable the Navy to leverage edge computing, analytics, machine learning, and artificial intelligence, revolutionizing Navy capabilities and user experiences through automated business processes, and expedition of delivered capability to users afloat and ashore.

THE PROCESS AND METHODOLOGY MOVING FORWARD

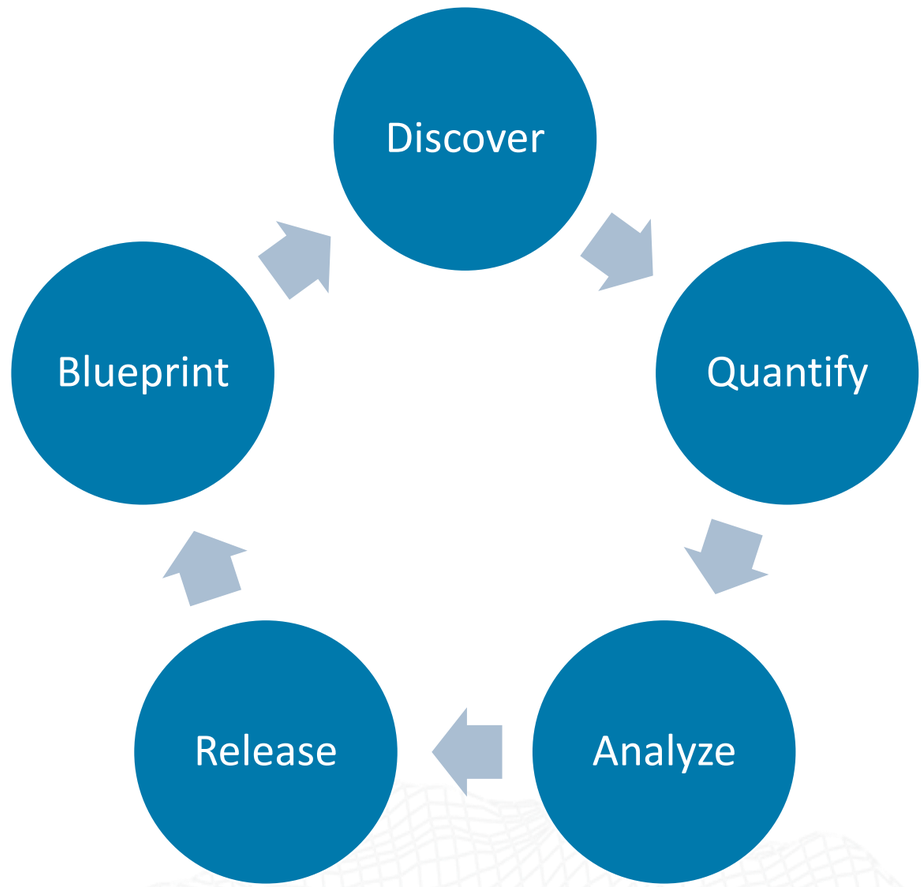
DELIVERING USER VALIDATED CAPABILITIES

The Navy Blueprint sets a framework for best practices from Agile methodologies by using **an iterative process** focused on the delivery of capabilities defined by and validated against user objectives, functional goals, and mission requirements.

The process focuses on:

- **Identifying capability gaps** based on user input, research, and analysis.
- Capturing and analyzing IT services, investment, user feedback, Measures of Effectiveness (MOE), and Measurers of Performance (MOP) to make strategic decisions.
- **Continuous engagement of users** and providers to define requirements for design, testing, and monitoring progress towards modernization.
- Maturing and developing the instantiation of Navy network and system assets that enable operation across all domains and warfighting functions to increase lethality, improve survivability, and support all Navy lines of business.

The initial publication/release of the Navy Service Blueprint is only the beginning. Following release, enterprise implementation plans will be developed via Technical Exchange Meetings (TEMs), Data Analysis, and Focus Groups.



THINK BIG. START SMALL. DRIVE TOWARDS ENTERPRISE SOLUTIONS.

PROCESS MODELING TUTORIAL

WHAT ARE PROCESS MODELS AND HOW TO USE THEM

Process Models are operational planning tools to be leveraged during Navy Blueprint Technical Exchange Meetings that:

- Show the stages of a particular user-centric process, aligned to the Navy Blueprint Services Model, and prioritized along the Services Catalog.
- Identify critical actions, actors, and assets involved in the execution of a service.
- Identify operational deficiencies, vulnerabilities, and aide in the conceptualization of changes to mitigate or eliminate them.

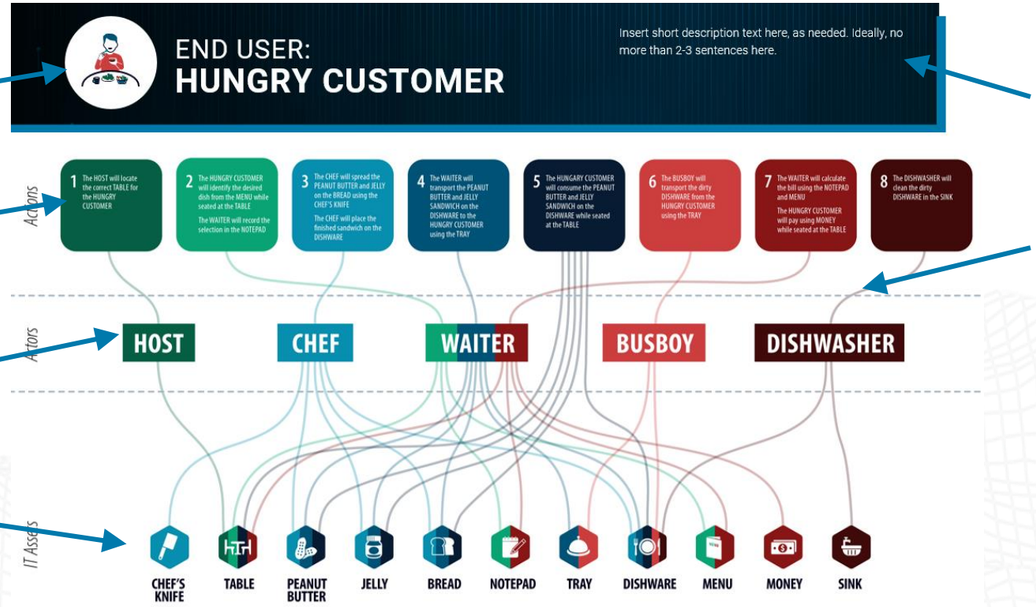
EXAMPLE:

End User: Identify the end user for whom the service provides an output

Actions: Describe actions executed by actors. Depending on the context, the user could be an individual, or a system

Actors: Identification of stakeholders or systems executing actions

Assets: Supporting applications, infrastructure and other equipment that the service requires in order to execute



Description: Describe the expected outcome of the service

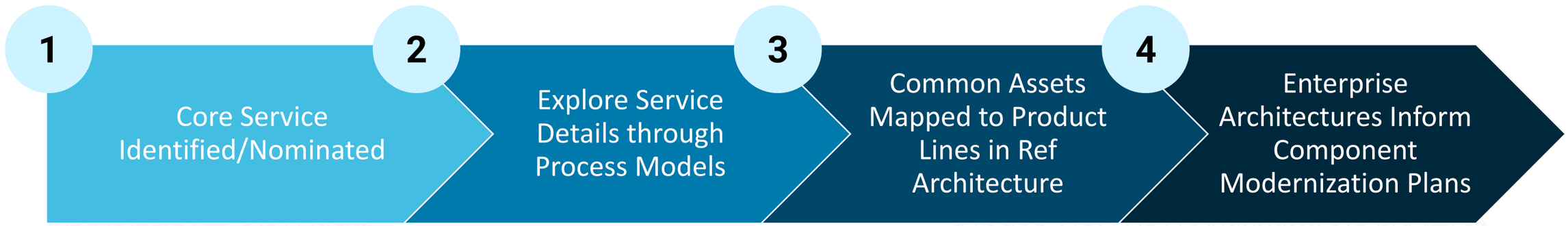
Lines of Interaction: Identify the relationship between actions, actors, and assets

TECHNICAL EXCHANGE MEETINGS

UTILIZING TECHNICAL EXCHANGE MEETINGS TO MODEL ENTERPRISE ARCHITECTURE, SERVICES & PROCESSES

In support of the Navy Blueprint for a Modern Enterprise Information Ecosystem, each Navy command that has responsibility for the operations, sustainment, and modernization of network environments will capture their current state through the lens of tools and frameworks provided in the Navy Service Blueprint in partnership with the OPNAV N2N6 staff.

Enterprise Core Services focused working groups will hold Technical Exchange Meetings (TEM) to build consensus and commonality among shared services.



MILESTONES FOR MODERNIZATION

A CALL TO ACTION FOR NAVY COMMANDS:

PHASE 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 timeline for network segment assessment
- **Deliverables:** Network assessment plans to support Target Enterprise Architecture (TEA) assessment tools

COMPLETED BY Q4 FY24

PHASE 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 Integrated Modeling Environment (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

PHASE 3:
EXECUTION

- **Objective:** Complete the movement of applications and data to cloud, consolidation of on-prep infrastructure, and demonstrate divestment of redundant systems
- **Model Development:** Adjust 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

NAVY BLUEPRINT GLOSSARY

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 Tea
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 Perameter
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	SOURCE
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	SOURCE
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	SOURCE
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	SOURCE
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	SOURCE
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	SOURCE
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)	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. 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. 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. 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)	

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	SOURCE
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.	
Artifact Software Artifact	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 scripts, test results, security scan results, configuration scripts, 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. 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.	
Artifact Repository	An artifact repository is a system for storage, retrieval, and management of artifacts and their associated metadata. 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	
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. 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	SOURCE
Build Tools	Used to retrieve software source code, build software, and generate artifacts	
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." https://www.cncf.io	
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	SOURCE
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	SOURCE
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/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.	

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. 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.	*Department of Defense Data Management Lexicon Memo (June 15, 2020)* *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 2nd Edition (Loshin, 2008)*
Metadata	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.	*The Intelligence Community Data Management Lexicon, Office of the Director of National Intelligence, dated January 2020*
	Information describing the characteristics of data; data or information about data; or descriptive information about an entity’s data, data activities, systems, and holdings.	*DoD Metadata Guidance Memorandum (March 2023)*
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.	*Department of Defense Data Management Lexicon Memo (June 15, 2020)*
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	*https://dbpedia.org/page/5ESS_Switching_System*
Base Level Information Infrastructure (BLII)		*Google*
Base Modernization (USN Phase 2)	"On-base" (interior) base infrastructure and changing end points (phones, alarm systems, etc.)	*OPNAV (Charlie)*
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 NETWORX Contract	*PMW790*
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	*OPNAV (Charlie)*
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.	*DISA/NAVIFOR/NCMO*
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.	*Google*
Defense Information Systems Network (DISN)	The United States Department of Defense's enterprise telecommunications network for providing data, video, and voice services.	*Google*
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.	*Google*

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.	*Google*
DoD365 Integrated Phone Service (DIPS)	An integrated Microsoft's M365 (Teams) product offering for in and outbound phone call processing	*OPNAV (Charlie)*
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.	*Google*
Global Network Services(GNS) OCONUS	Contract through DISA with industry partners to provide IP external circuit to and from USN installations.	*DISA/NAVIFOR*
GSA's Enterprise Infrastructure Solutions(EIS)	Contract through DISA with industry partners to provide IP external circuit to and from USN installations.	*DISA/NAVIFOR*
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	*DISA/NAVIFOR*
Inquiry/Qoute/Order(IQO)	Competitive lease contract through DISA with industry partners to provide IP external circuit to and from USN installations.	*DISA/NAVIFOR*
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)	*OPNAV (Charlie)*
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	*PMW790*
Low Speed TDM (LSTDM)	T-1 and below circuits connected to EOL(2017) Promina devices.	*PMW790*

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 sensoring 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
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 (Vl.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)".	*DoD CIO FAQ Page*	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.	*DoDI 8115.02; IT PFM Implementation*	DoDI 8115.02 - IT PfM Implementation.pdf
BEA (DoD)	**Business Enterprise Architechture** 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.	*Defense Business Systems Investment Management Guidance, V4.1, June 2018*	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)