PEO Digital
Technical Director

Modern Service Delivery
Service Groups

Version 2.6
April 29, 2022

Prepared By:
Technical Director, PEO Digital

DISTRIBUTION A. Approved for public release: distribution unlimited. (29 April 2022)

Version History

Version	Date	Changes
1.0	08 July 2019	Completed first version release
1.1	11 September 2019	Updated for Public Release
1.2	16 October 2019	New title, references, and PEO EIS Graphic
2.0	29 May 2020	Updated scope from PEO EIS to DON, adjusted to latest service group names
2.1	05 October 2020	Updated graphics
2.2	29 October 2020	Formatting updates
2.3	04 January 2021	Addressed CRM from formal USMC review
2.4	03 March 2021	Added new DON CIO graphics & resiliency to MSD
2.5	1 March 2022	Updated figures, End User and Workplace Automation
2.6	20 Aril 2022	Administrative Updates

Table of Contents

Contents

List of Figures

Chapter 1 Overview

The Department of the Navy (DON) is implementing shared Information Technology (IT) services as a fundamental shift in how the organization designs, consumes, and delivers services to support mission objectives and the DON Information Superiority Vision. *Modern Service Delivery Detail* provides and explains frameworks governing decision-making for design and development of services consumed or managed by the DON and explains design concepts and requirements applying to all DON Information Technology (DON IT) services. *Modern Service Delivery Detail* addresses the relevance of and background leading to Modern Service Delivery (MSD). Different views of the DON portfolio exist, including Program View, Services View, and Technical Focus Areas View.

FIGURE 1: STRATEGY TO EXECUTION

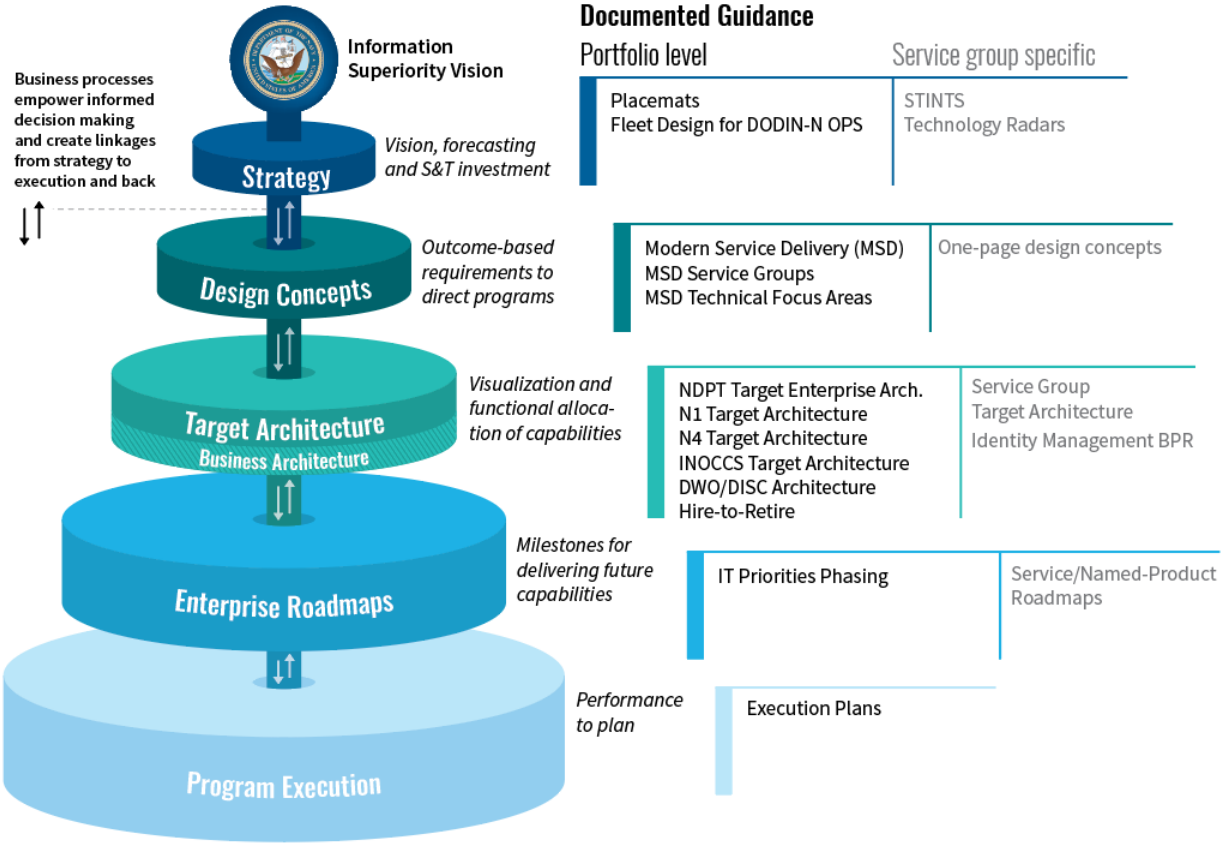
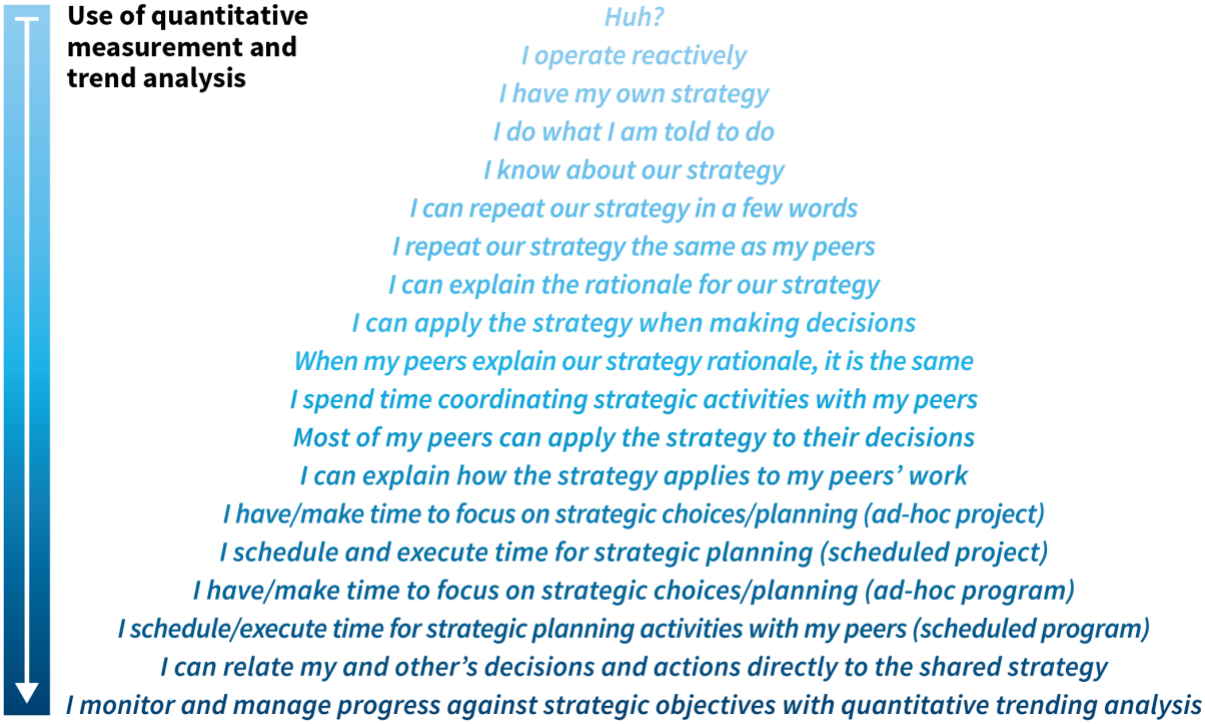


Figure 1 identifies the alignment and increasing levels of detail from the DON CIO strategy, which includes modernize, innovate, and defend pillars. The design concepts and requirements detail support all three pillars of the DON CIO strategy, but most closely align to the modernize pillar, which includes specific lines of effort for cloud, network, and identity. *Modern Service Delivery Details* translates the strategic intent into a limited number of high-level requirements for all services to align Naval IT efforts in the development of a ubiquitous digital platform of integrated networks and services. *Modern Service Delivery – Service Groups* provides additional design concepts and requirements for similar services (e.g. Compute & Store).

Modern Service Delivery – Technical Focus Areas provides additional design concepts and requirements for services related to subject areas of relevance (e.g. cloud). *Modern Service Delivery Details* requirements apply to all services. Requirements in *Modern Service Delivery – Service Groups* and *Modern Service Delivery – Technical Focus Areas* are not mutually exclusive or exclusive to that group alone, so requirements managers should review all requirements to determine which are relevant to the solution in development. This is particularly true as there is a bi-directional relationship between all services and Management & Security services, as each must be designed to integrate.

The purpose of this *Modern Service Delivery - Service Groups* document is twofold. The first is to provide a list of objectives and requirements related to each of the Service Groups. The second purpose is to help the audience and organization improve Strategic Operations Maturity, as depicted in Figure 2. Requirements definition and explanation empowers program managers and requirements officers with strategic intent that may have never been translated into concrete requirements.

FIGURE 2: STRATEGIC OPERATIONS MATURITY



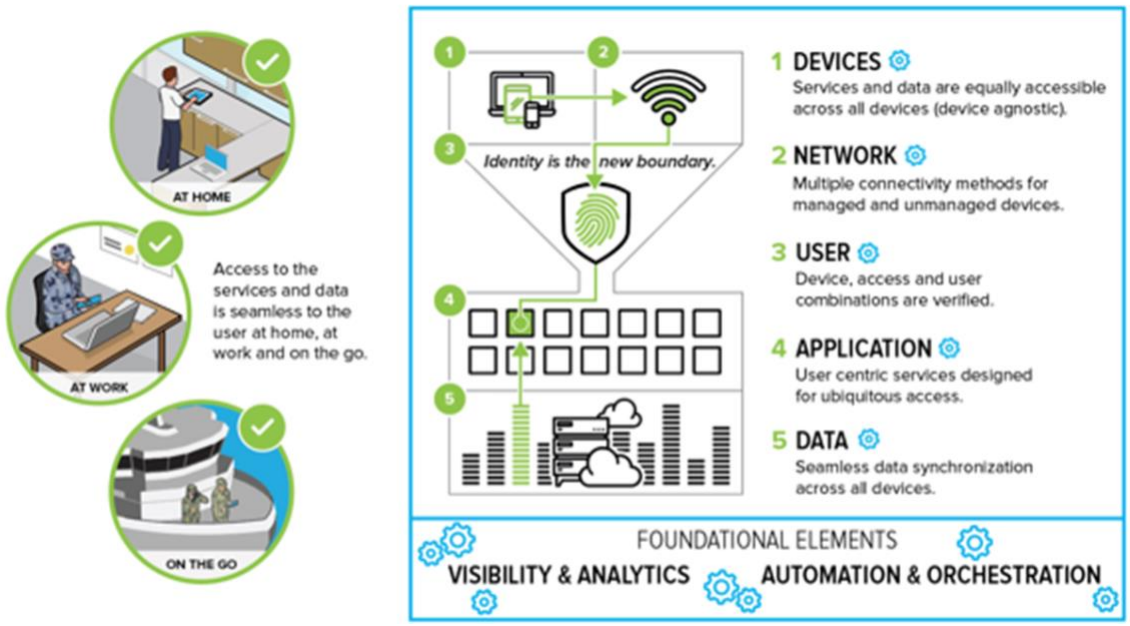
1.1 Modern Service Delivery Design Concepts

The sum of design concepts applying to all DON IT services is called Modern Service Delivery, depicted in Figure 3. The use of Modern Service Delivery Design Concepts for all services will ensure strategic alignment, interoperability, and integration across the DON and the Department of Defense (DoD). Modern Service Delivery design concepts are user-centric and customer-first, prioritizing the ease of consumption of services to free Sailors and Marines to execute their

mission instead of fighting to get the IT services they need. Services designed with mobility in mind supporting disconnected operations will mean they are designed for deployment.

FIGURE 3: MODERN SERVICE DELIVERY

Design Concepts adoption by DON will drive interoperability across Warfighting, Readiness, and Business Pillars using industry standards.



Modern Service Delivery Design Requirements

- Buy instead of build commodity technologies (As-a-Service preferred)
- Maximize use of commercial cloud services
- Create an Application Program Interface (API) economy – design for integration, data sharing and reusable interfaces
- Use Representational State Transfer (RESTful) architecture standards – focused on caching and layering for disconnected uses
- Design to enable the National Institute of Standards and Technology (NIST) attributes of cloud for both on and off-premise consumers
- Design loosely coupled services to operate across network and security boundaries (build once, use often)
- Adopt Zero Trust principles as the basis for security and user experience
- Acquire integrated suites of capabilities instead of integrating many best of breed products
- Enable self-service provisioning in development and production environments
- Design for mobile access
- Ruthlessly automate everything
- Ensure RESTful APIs support service calls from Integrated Navy Operations Command and Control System (INOCCS) manager of managers, ensuring the ability to provision, operate, protect, and defend the service at scale
- Design for resiliency

1.2 Non-technical Ramifications

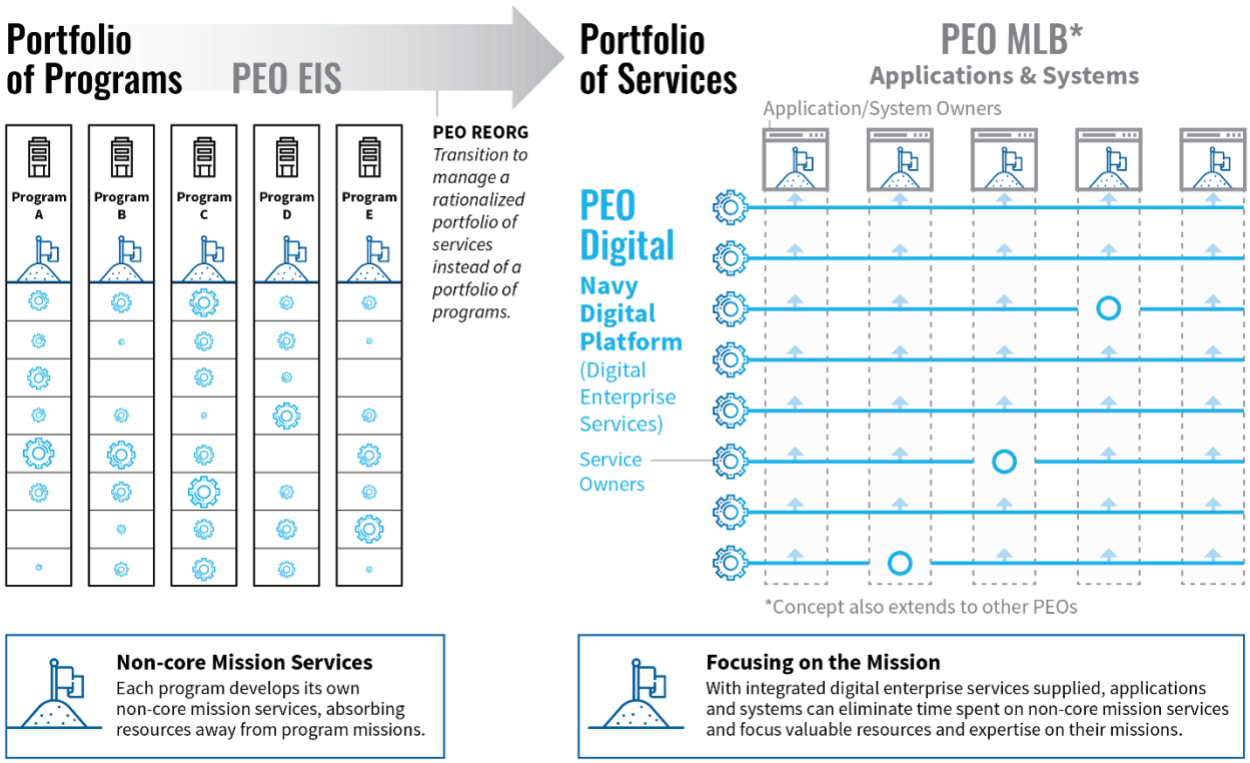
For the DON to execute these design concepts effectively, several non-technical aspects will need to change. Some of the most notable aspects that must change are as follows:

- Manage rationalized portfolios of services instead of portfolios of programs
- Organize resources to mirror desired service orientation
- Develop and publish service catalogs and roadmaps
- Identify organizations that provide new services
- Deliver shared Digital and Enterprise Services (DES) across all Naval security and network domains
- Enable Continuous Integration/Continuous Deployment (CICD) across all environments
- Adjust acquisition, cyberspace operations, and authorization processes

1.3 Service Groups Explanation

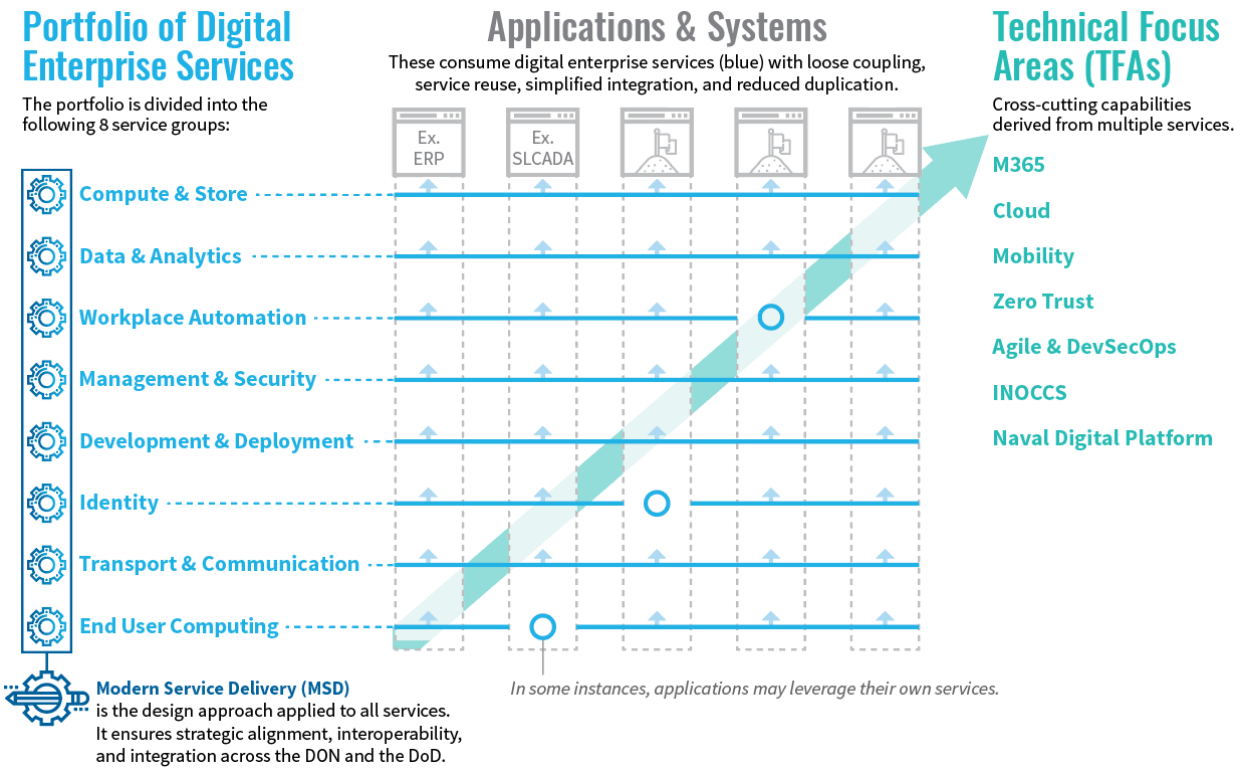
Part of the non-technical aspects of the technical services strategy is to rationalize as a portfolio of services and subdivision of that portfolio into non-overlapping groups of similar services - Service Groups. Figures 4 and 5 identify the relationships between different ways to view the DON portfolio. The first is the traditional view of DON as a portfolio of programs, each delivering its own services. The program view shows each program developing its own non-core mission services, such as identity services, which it needs to fulfill its core mission. The second is viewing DON as a portfolio of services independent of the programs. These shared services represent opportunities for optimization if designed to be a loosely coupled service; operating across multiple network and security boundaries; and configured and consumed by programs rather than developed by programs.

FIGURE 4: PEO EIS REORG - THE TRANSITION TO MODERN SERVICE DELIVERY



The third view of the portfolio, Figure 5, is based on technical focus areas which can affect multiple programs from the program view, and multiple services from the service view.

FIGURE 5: DON PORTFOLIO VIEW



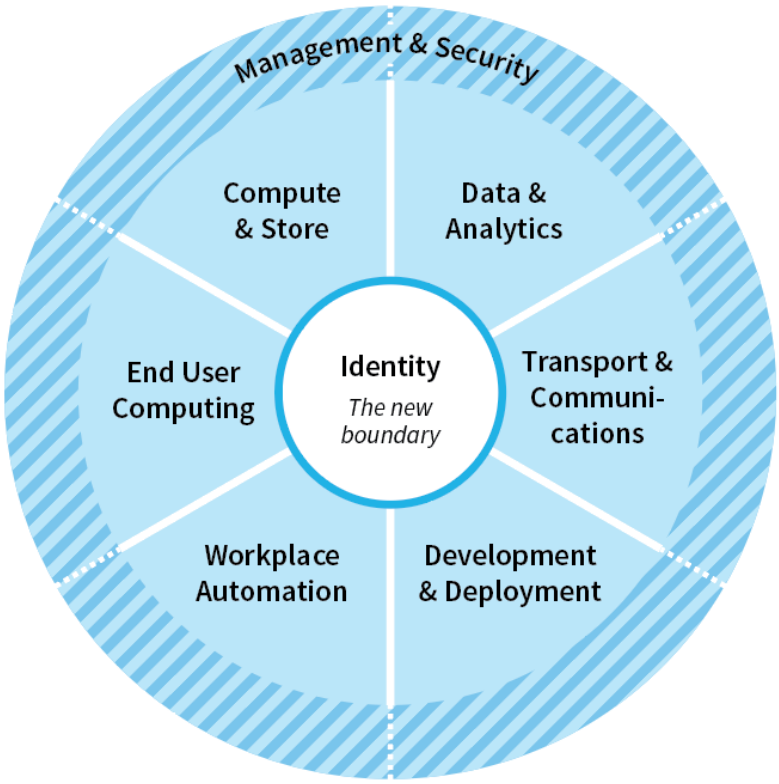
The *Modern Service Delivery Detail* document provides design concepts for all services. This document, *Modern Service Delivery - Service Groups*, provides design concepts specific to each of the service groups listed on the left in Figure 5. *Modern Service Delivery Technical - Focus Areas* provides design concepts specific to each of the named technical focus areas, listed to the right on Figure 5. In addition to the underlying shared services from Program Executive Office (PEO) Digital; PEO Manpower, Logistics, and Business (MLB) provides specific end user applications. When the DON consolidates on shares services in the future, a similar organizational model will be applied to other DON PEOs to support consolidation at shares services and differentiation on end user applications. Technical Focus Areas will continue to increase, but the list of Service Groups will remain static.

Chapter 2 DON Service Groups

The DON Portfolio of Digital Enterprise Services is composed of the Service Groups represented in Figure 6. All eight Service Groups cover the full scope of Digital Enterprise Services, including all IT services detailed in the Marine Corps Information Environment Enterprise (MCIEE) Blueprint. Service Groups are a set of related services organized together for portfolio management purposes. Service relatedness is primarily based on service similarity, not its relationship to IT Service Management (ITSM) functions or processes. For example, the management and security functions and processes will not be completed exclusively with services from the Management & Security Service Group. *The Service Group does not equate directly to the function or process.* Organic management and security processes within each service group is represented as a shared function (hatch marking in Figure 6) with the Management and Security Services Group. Chapter 2 provides a general operational definition

for each of the DON Service Groups, explains in scope and out of scope services, and provides a general approach and requirements for the services in that Service Group. Due to overlap in functionality between groups, overlap in product and product suite capabilities, and changes in industry, the definition serves as a general guideline and cannot provide a black and white delineation. Additional insight can be obtained by reviewing the latest version of the draft or production service catalog. The final determination for functionality, product, and service assignment to a service group is the decision of the Naval Digital and Enterprise Services Portfolio Executive, not the Service Group owner. This prevents duplication between Service Groups when multiple group owners believe their scope includes the service or creation of gaps when no group owner believes their scope includes the service.

FIGURE 6: DIGITAL ENTERPRISE SERVICES



2.1 Compute & Store Services Service Group

Short definition: Compute & Store are services which provide generic compute and structured and unstructured data storage services primarily aligned to Infrastructure as a Service (IaaS) cloud service model.

In scope: Compute & Store scope includes generic compute and storage services. The hosting model (on-premises or externally hosted) does not matter as long as the service has all the National Institute of Standards and Technology (NIST) attributes of cloud computing. The scope includes all instances of servers and storage offered under the Infrastructure as a Service (IaaS) cloud service model. Scope also includes serverless compute and store capabilities including in-

memory services not necessarily considered IaaS. Compute & Store includes capabilities such as:

- Generic virtual servers (Windows, Linux, Unix, etc.)
- Preconfigured/managed Operating System (OS) images
- All generic Compute Function as a Service (FaaS) not part of the scope of other service groups
- Default unconfigured container services
- Data storage and compute infrastructure, including Denied, Disconnected, Intermittent, Low-bandwidth (DDIL)
- Spinning disk, flash, and in-memory storage delivered as a service
- Content delivery
- Structured and unstructured data storage not part of other service groups
- Block, Binary Large OBject (BLOB), and File storage
- Archive files storage

Out of scope: There are several types of services which generically might be considered Compute & Store but are excluded from this service group because they are more aligned with design concepts and requirements of other service groups. Services such as pre-configured secure containers provided as a Managed Service Offering are part of the Management & Security Service group because they are designed and implemented to provide standardized security services. Server computing is part of Compute & Store, but virtual desktop and browser virtualization are part of End User Device services. Services which provide data and analytics services aligned more with the Software, Software as a Service, or Platform as a Service model (such as Data Warehousing, Hadoop, Splunk, etc.) are better aligned with the Data & Analytics services group. Final determination will be made by the service portfolio owner. *The function of storing or processing data is not the only criteria for categorizing the service.*

General approach explanation: The purpose of Compute & Store services is to abstract the consumer from the need to manage compute & store infrastructure and to automate High Availability (HA), Disaster Recovery (DR), backup, restore, failover, and cost/service optimization. Compute & Store services should be self-provisioned, configurable, standardized infrastructure as a service. Consumers of these services, whether they are standard users for storage or administrative users for storage and compute, should have the control to set thresholds for the services so automation, rather than administrators, can provision and deprovision the service scale and tiers. On-premise delivery of services should be seamless and equivalent to cloud-hosted services and should support delivery from heterogenous commercial commodity hardware.

Compute & Store Services Design Requirements

1. Develop services that operate in hybrid multi-cloud as a single logical environment
2. Develop services providing policy-based automated optimization of compute and storage service tiers

3. Develop services providing the consumer automated policy-based capacity and scaling adjustments
4. Develop with automated service resiliency instead of relying on legacy High Availability (HA) and Disaster Recovery (DR) architectures and processes
5. Develop compute and store capabilities abstracted to the logical level to the greatest extent possible.

2.2 Development & Deployment Services Service Group

Short definition: Development & Deployment are services used for the purpose of development, integration and testing (in development), authorization, and deployment of new capabilities primarily aligned to Platform as a Service (PaaS) cloud service model.

In scope: As a general rule, the Development & Deployment service group is comprised of the services used to create (in development) and distribute (in production) new capabilities. Development & Deployment primarily fit within the Platform as a Service cloud service model. Development & Deployment includes capabilities such as:

- Low-code/no-code tools and platforms
- Any capability unique to the development environment only, such as static and dynamic code analysis software
- Trusted code repositories
- Software container registries
- Software deployment tools
- Configuration Management databases
- Development factory front-end
- Pre-configured development pipelines delivered as a managed service
- API management platforms
- Software queuing and notification services
- Application analysis & migration tools
- Automated workflow and Business Process Re-engineering (BPR) platforms
- Internet of Things (IOT) platform hubs
- Software code programs and software development kits

Out of scope: It is difficult to categorize services between Development & Deployment and Management & Security services. A review of the draft or production service catalog helps to develop mental categorization models. It is important to remember **the Service Group does not equate directly to the function or process**. Security compliance tools that operate in both development and production environments, such as Assured Compliance Assessment Solution (ACAS) or Xacta are security services, and any manager of manager service is part of Management & Security services. *Management and security activities will heavily rely on deployment services to achieve the control aspects of command and control objectives.*

General approach explanation: The purpose of Development & Deployment services is to set the condition where the DON can achieve fully integrated and automated Continuous Integration and Continuous Development (CICD) end state in a hybrid multi-cloud environment including Denied, Disconnected, Intermittent, Low-bandwidth (DDIL) operations. Integrated development and deployment services following MSD concepts will enable the Naval enterprise to fail fast and learn quickly as opposed to long duration waterfall development efforts. Secure development is supported through secure code repositories, shared standardized services, and an Application Program Interface (API)-based economy. The development environment is comprised of development factories and development pipelines. Development factories are the virtual location (storefront) where services are provisioned. Development pipelines are specific sets of services intended to serve a particular purpose, such as provide a representative target environment or tools unique to a development approach. Factories and pipelines will include self-provisioned baselined services and data available in the production environments, but the services may be from other service groups (e.g. Identity services). The development environment supports both application code development and functional capability development through integration and configuration of existing Commercial Off-the-Shelf (COTS), custom developed, and cloud native capabilities.

Development & Deployment Services Design Requirements

1. Reduce tools sprawl by identifying Development & Deployment services designed to support development and deployment and management and security functions as part of the INOCCS framework to the greatest extent possible (build once, use often).
2. Automate tools to ensure zero configuration drift between the development environment and the production environment
3. Develop self-service provisionable CICD pipeline environment baselines for target production environments
4. Adopt industry-proven development tools/services that support agile development methods
5. Consolidate software development factories and allow for differentiation of software pipelines
6. Develop pipelines and services enabling citizen developers to create functionality by combining already approved services in new ways
7. Universally adopt the same deployment tools across environments to ensure fully automated continuous monitoring and configuration drift remediation via the native deployment tools capabilities

2.3 Management & Security Services Service Group

Short definition: Management & Security are services implemented exclusively to operate and defend the entirety of the IT portfolio by enabling enterprise-wide visibility, command, and control to administrators or directly to other applications and networks that do not fit into the description of the other service groups.

In scope: Management & Security Services are those which primarily enable global operate and defend functions. Tools and services which serve the purpose of automating manual management and security activities and processes such as Enterprise Mission Assurance Support Service (eMASS) are also within scope. Management & Security includes services solely for the purpose of continuous monitoring as part of Cyber Security Service Provider (CSSP) and non-CSSP Operations functionality. Security containers and security sidecars are within scope. Services such as firewalls are Management & Security services because they prevent the bits and bytes from going from one endpoint to another. Any service that manages or orchestrates services from multiple Service Groups (like a cloud computing management portal for a CSSP) is within scope. Management & Security includes capabilities such as:

- Global (not service specific) command and control capabilities
- Manager of managers including marketplace ordering portals and multi-cloud orchestration
- Services implemented exclusively to manage a process but not necessary for development and deployment function or processes (per se), such as (eMASS)
- Assured Compliance Assessment Solution (ACAS)
- Continuous security risk assessment and compliance automation and management (e.g. Xacta)
- Hardware security module functionality and encryption
- Tools used exclusively for visibility such as network monitoring and mapping
- Application performance monitoring
- Log management & log analytics software
- Security communications hubs
- Stand-alone Data Loss Prevention (DLP) and Digital Rights Management (DRM)
- Device management software such as Mobile Device Management (MDM)
- Automated security monitoring such as Cloud Access Security Brokers
- Host Based Security System (HBSS)
- Pre-configured secure containers delivered as a Managed Service Offering
- Firewalls (because they prevent the bits and bytes from going from one place to another, they are security services, not transport services)

Out of scope: Most services have a native management function and capabilities supporting the secure configuration of the service. These management capabilities are tied so closely to the service that they cannot be abstracted, so the accompanying native tool is part of the respective service group, and thus out of scope for the Management & Security service group, unless the service is used as a manager of managers. *Just because it can be used to manage the service or create a secure configuration does not make it part of the Management & Security services group.*

General approach explanation: The purpose of Management & Security services is to enable visibility, command, and control to administrators or directly to other applications and networks from a DON Enterprise-wide perspective. This is accomplished through integrated capabilities to identify anomalous behavior, integrated and automated policy enforcement points to trigger

remediation, and implementation of manager of managers and managers of orchestrators to automatically respond to anomalous behavior and configuration drift across multiple network and security boundaries. Management & Security services provide enterprise-wide visibility and command functions, and automates the control functions through API integration with services from other service groups. Figure 7 represents the operational complexity of executing command and control functions across multiple independent networks. Application of the Modern Service Delivery design requirements from all service groups, and in particular, Management & Security Services design requirements will support better unified operations of the Naval IT battlespace as represented in Figure 8.

Management & Security Services Design Requirements

1. Rely on the fully automated capabilities of other service group services as the foundation of the control part of visibility, command, and control functions by using a manager of managers approach.
2. Follow Continuous Adaptive Risk and Trust Assessment (CARTA) and Zero Trust (ZT) principles for managing security and user experience to achieve an Enterprise Digital Rights Management (EDRM) end state
3. Adopt commercial modern real-time network monitoring and security capabilities
4. Implement Management & Security services that integrate through APIs with software-defined perimeter, application micro segmentation, and modern identity services
5. Automate monitoring and response using policy enforcement points and risk thresholds
6. Use the power of cloud computing, Artificial Intelligence (AI), and Machine Learning (ML) to identify allowable but anomalous behavior and to automate response
7. Reduce tools sprawl and government integration efforts through use of pre-integrated product suites instead of multiple best of breed point solutions
8. Rely on Data & Analytics services extensively to make aggregated data available for Management & Security Services rather than developing vertical stovepipes
9. Isolate non-business Internet browsing services from the network and endpoints

FIGURE 7: AS-IS NAVAL CYBERSPACE OPERATIONAL COMPLEXITY

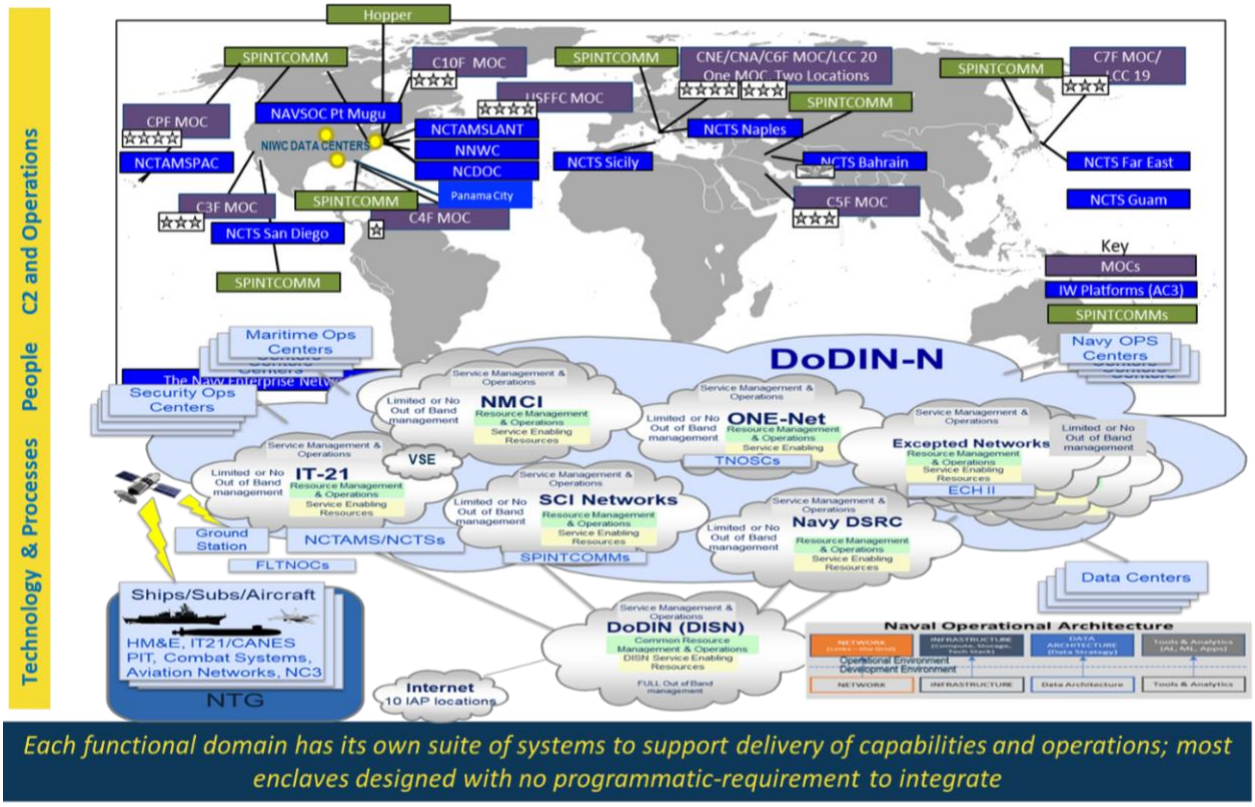
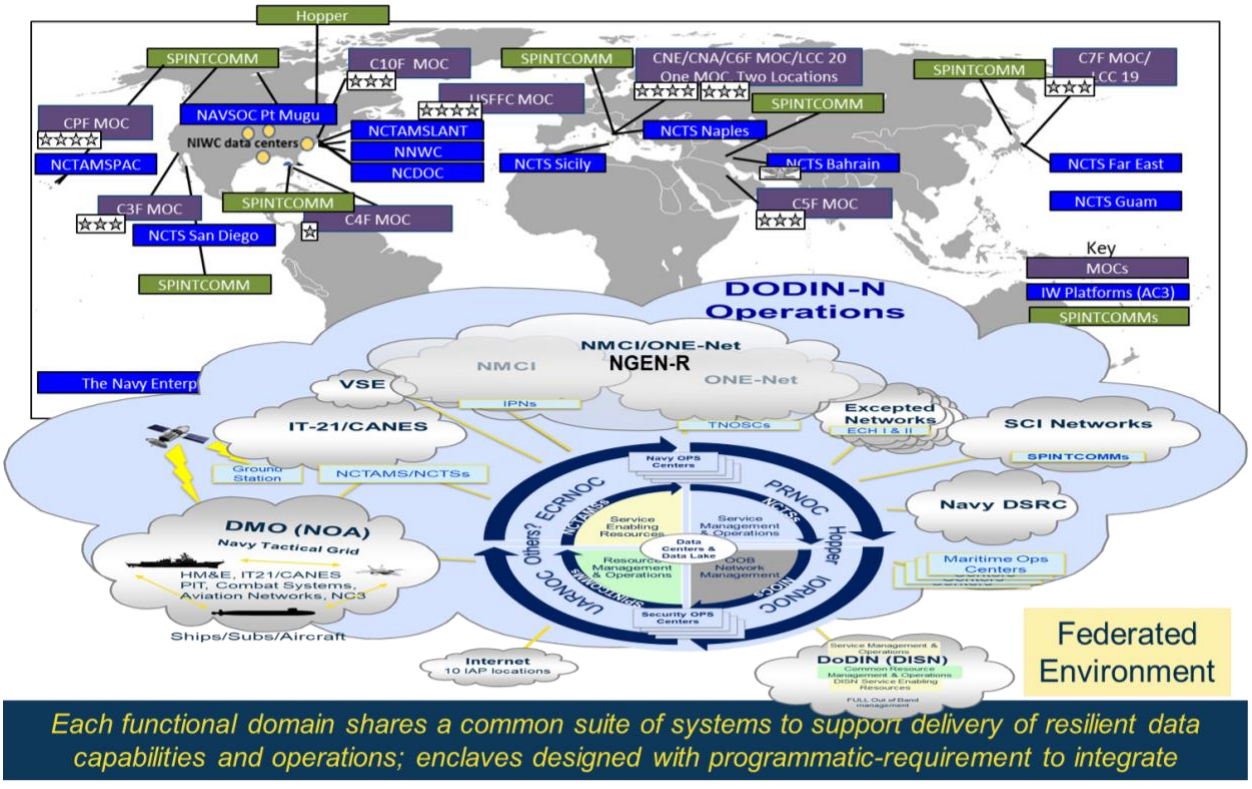


FIGURE 8: FUTURE UNIFIED OPERATIONS ENVIRONMENT



2.4 Workplace Automation Services Service Group

Short definition: Workplace Automation are services consumed directly by end users to optimize technology, increase productivity, and to enable user output primarily aligned to Software and Software as a Service (SaaS) cloud service model.

In scope: Workplace Automation scope covers applications that provide functionality directly to typical end users. End users here are defined as those excluding administrators and traditional developers. Workplace Automation includes capabilities such as:

- End user productivity services including Microsoft Office 365 exchange, office rich client, office online, and OneDrive
- Video teleconferencing
- Telephone voice services
- Robotics process automation
- Instant messaging
- Mapping such as ArcGIS and online map server services
- Collaboration tools such as Slack and Trello

Out of scope: The scope does not include supporting services which are transparent and not directly used to optimize technology, increase productivity and utility, and to enable user output, such as authentication or single sign-on services (Identity services), Virtual Private Network (VPN) (Transport & Communications services), or any service exclusively available to administrators, traditional developers, or data scientists. Applications and services supporting individual Lines of Business or Functional Areas will not be considered under Workplace Automation as they do not meet the definition of a Digital and Enterprise Service. Desktop clients, applications, and core builds are not aligned with WorkPlace Automation, as they are explicitly included in End User Computing Services. *Just because it is automated does not make it a Workplace Automation Service.*

General approach explanation: The purpose of Workplace Automation services is to provide direct user productivity and utility, enable user output, and remove technical administrative burned from the warfighter. The approach uses evergreen SaaS or COTS services and change business processes rather than customizing software around current processes. The approach also includes improving parity between industry and government in terms of functionality and mobility.

Workplace Automation Services Design Requirements

1. Acquire workplace automation as high up the stack as is feasible, avoiding custom development or customization
2. Make Workplace Automation services available from anywhere on any device, including Bring Your Own Device (BYOD)
3. Move business Workplace Automation services off the DOD Information Network – Navy (DODIN-N) and allow direct internet connection

4. Maximize use of server and web application services, and minimize the use of endpoint applications
5. Make all Workplace Automation services self-service provisioned
6. Standardize user experience across device types
7. Ensure workplace automation can be delivered to and synchronized for DDIL environments

2.5 Transport & Communications Services Service Group

Short definition: Transport & Communications are all the services that make the bits and bytes move from one endpoint to another.

In scope: Transport & Communications Service group is exclusively limited to the wired and wireless connectivity services. This includes services exclusively used to transport signal and data to enable access to information and services via assured end-to-end connectivity across environments, including all data route, switch, and distribution functions. Transport & Communications includes all services that specifically create digital connectivity from one endpoint to another. Transport & Communications includes capabilities such as:

- Network as a Service
- Physical and virtual routers
- Physical and virtual switches
- Wi-Fi and 5g
- Software Defined Networking (SDN)
- Application microsegmentation
- Domain Name Services (DNS)
- Virtual Private Network (VPN) software
- Satellite communications

Out of scope: The scope of Transport & Communications does not include any services used to otherwise monitor, read, secure, or use the data (which excludes many of the services typically part of the military Communications definition). Services which exclusively monitor transport services are not part of Transport & Communications services because the monitoring capability does not make the bits and bytes move from one endpoint to another. The scope of the Transport & Communications does not include the full end-to-end vertically integrated capability satisfying all Naval communications objectives. Firewalls, for example, are a Management & Security service because they prevent bits and bytes from moving from one endpoint to another. Video Teleconferencing services, traditionally considered part of communications scope, are now part of Workplace Automation services, but they rely on connectivity between endpoints provided by the Transport & Communications services. *In other words, the objective of the communications function and processes are not satisfied exclusively through the Transport & Communications services group.*

General approach explanation: The purpose of Transport & Communications services is to provide the connectivity between endpoints allowing data transmission across ashore and Denied, Disconnected, Intermittent, Low-bandwidth (DDIL) environments including land,

underwater and/or air battlefields. Satisfying the objectives of Naval communications across persistent ashore and constantly shifting DDIL environments will require automated interoperability between multiple services from multiple service groups. Management & Security services will sense anomalous network activity, traffic pattern and performance issues, and application performance threshold exceptions and trigger fully automated traffic management response through Transport & Communications services. Transport connectivity will be automatically and dynamically routed across government and commercial carriers based on the context (user, data classification, authentication mechanism, current performance, best route, etc.). This approach, based on the concepts of Zero-trust enforce the principle of "protect the content, not the box", and place the security responsibility primarily in the Management & Security services group instead of the Transport & Communications services group.

Transport & Communications Services Design Requirements

1. Add commercial carrier transport services as a service for WAN, BAN, and LAN for resiliency and efficiency
2. For business systems, change to use DoDIN as backup/failover instead of primary WAN backbone
3. Use commercial carrier connections to each other to create multi-cloud connections
4. Change service delivery and ordering to bypass middleman connection services
5. Focus on reducing latency to improve performance and user experience
6. Enable internet connection through the CSPs IAPs for business use cases
7. Optimize transport to off-premises commercial cloud
8. Enable full automation, response, and Software Defined Networking (SDN)
9. Flatten the network to optimize routing for distributed computing, storage, and security
10. Implement application micro segmentation to reduce reliance on perimeter defense

2.6 Identity Services Service Group

Short definition: Identity Services are all services that provide and manage Identity, Credential, Access, Authentication, and authorization for humans and systems.

In scope: Identity scope includes all services which provide capabilities related to identity, credential, and access management. The importance of identity services and the distinctness of the requirements for those services are the basis for treating it as a unique group of services. Identity services includes capabilities such as:

- Identity source services such as Active Directory servers
- Identity Management (IdM) (self-service password mgmt., registration, identity creation, approvals and workflows, role definition)
- Identity Access Management (IAM) (web access management, single sign-on, identity federation, authentication, authorization)
- Identity Governance, Audit Role & Compliance (IGA) (centralized audit, logging and monitoring, access certification, reporting)
- Identity synchronization and replication

- Virtual identity directory
- Multi-factor authentication services
- Credential management services

Out of scope: Any Management & Security service not directly related to handling the in-scope listed services. For example, User and Entity Based Analytics (UEBA) that comes as part of a product suite for identity management is part of the Identity services group, but stand-alone UEBA for security purposes, such as those provided by a Cloud Access Security Broker product would be part of Management & Security services.

General approach explanation: The purpose of Identity services is to serve as the foundation of secure operations in a Naval multi-domain hybrid multi-cloud environment, including DDIL, as represented in Figure 10. Current Identity services in Figure 9 do not enable such integration. Adoption of API based integrated modern identity capabilities is the start of the journey toward Zero Trust and modern methods focused on contextual security of the data. Modern methods will enable the DON to automate identity creation, authorization controls, and definitively know who has access to what data regardless of account, network, or security domain. Data security will be achieved by focusing on identity and authorization as opposed to focus on securing all data the same way through network perimeter security and universal high-bar authentication. Overreliance on network perimeter security has been demonstrated to no longer be successful and prevents access to data by those who need it in many cases.

Identity Services Design Requirements

1. Enable context-aware or identity-aware security by providing identity as input to a policy decision point
2. Integrate with AI and ML to support Continuous Adaptive Risk and Trust Assessment (CARTA)
3. Dynamically assign entitlements based on user role, Role-Based Access Controls (RBAC) and/or attributes, Attribute-Based Access Controls (ABAC)
4. Self-Service for domain and app owners to maintain control of their identities and authorizations
5. Resource owners can link entitlements to any identity from any domain
6. Multiple personas can be linked and tracked to a single individual or entity
7. Identity services integrate with Data Loss Prevention and security services to ensure data level security
8. Identity federation and synchronization without Active Directory federation
9. Resolve afloat/ashore disparity using identity information synchronization
10. Expand identity services to achieve commercial identity services parity
11. Federate disparate sources of identity information and aggregate them for consumption
12. Enable identity services for non DoDIN-N users and Bring Your Own Device (BYOD)
13. Enhance user experience through non-CAC authentication, single sign-on, and self-service
14. Enable fully automated Federal Information System Controls Manual (FISCAM) compliance

15. Adopt alternative multi-factor authentication approaches based on use case

FIGURE 9: IDENTITY SERVICES AS-IS

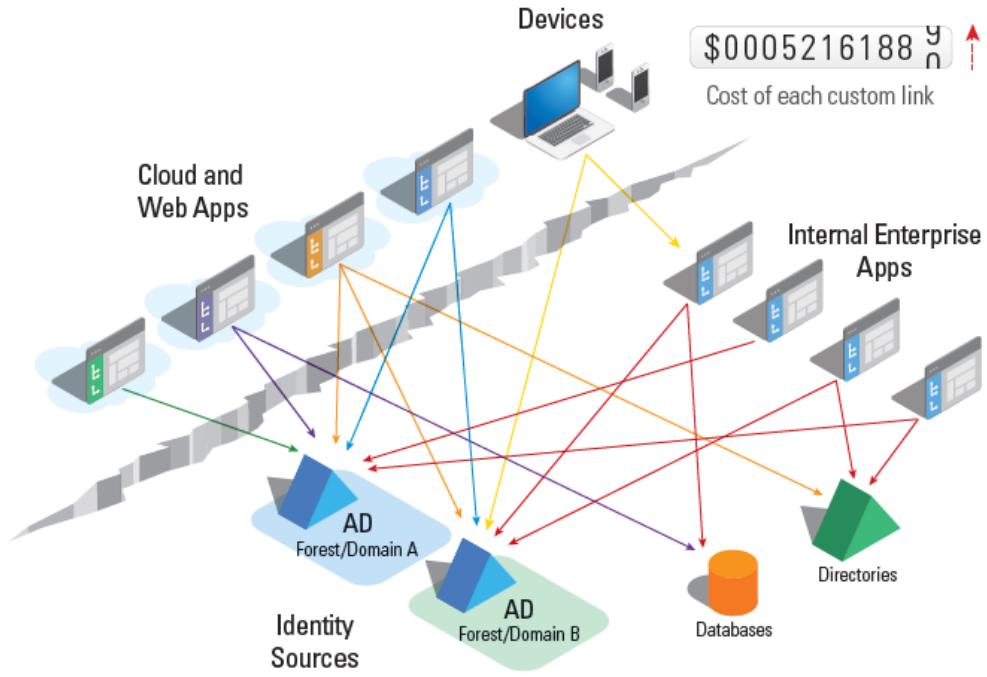
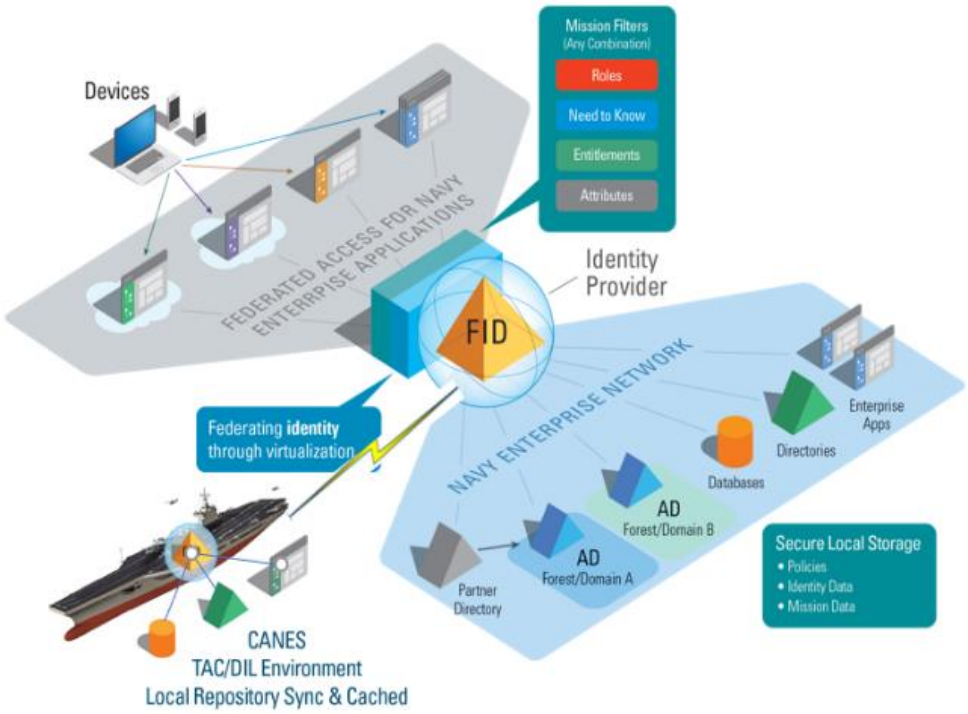


FIGURE 10: IDENTITY SERVICES TO-BE



2.7 End User Computing Services Service Group

Short definition: End User Computing is the physical and virtual device endpoints, core build, desktop applications, and the front end/stand-alone desktop parts that end users and administrators use to access digital data, voice, and video services, and increase endpoint utility. End User aligns to Software and Software as a Service (SaaS) cloud service and evergreen devices as a service.

In scope: End User Computing scope includes all user end-point devices and desktop applications. End User Computing can be either physical (desktop, laptop, cell phone, printer), virtual (virtual desktop, virtual browser), and desktop hosted applications. Scope includes bastion host virtual machines used by administrators. Scope also includes all special video teleconferencing hardware as well as computer and cell phone peripherals. End User Computing includes capabilities such as:

- Laptops
- Desktops
- Virtual desktop (on-premise or cloud hosted)
- Web browser virtualization
- Printers
- Non-windows OS mobile devices
- Desktop applications like zip, Adobe Acrobat, Autocad

Out of scope: End User Computing includes the device itself (physical or virtual), but not the aspects of producing, managing, or delivering the service. The one exception to this rule is for virtual devices. Most of the services related to End User Computing Services that are out of scope are part of Management & Security services. Examples include Mobile Device Management (MDM), Mobile Application Management (MAM), print servers, image production, Host-Based Security Services (HBSS), or antivirus software. Services supporting the delivery of devices such as device ordering and provisioning services and asset management or configuration management systems are also not part of the scope of End User Computing. Other than the device used and desktop applications, video teleconferencing services are not part of this service group.

General approach explanation: The purpose of End User Device services is to provide the front end/stand-alone desktop components and devices that users to interact with DON IT services. The approach is to follow the increasing trend to acquire and provide industry standard commercially available devices. This trend includes obtaining the device as a service from the vendor and the standard applications. Increasing the availability and use of virtual devices and browsers as a service better supports broader access, creates consistent user experience across device types, increases data security, and supports BYOD for personal computer or mobile cell phone based operating systems and form factors.

End User Computing Services Design Requirements

1. Obtain physical device separate from the device management service

2. Acquire devices as an evergreen service from the vendor/reseller to the greatest extent possible
3. Acquire industry standard commercially available devices and applications for desktops, laptops, cell phone, and printers
4. Expand device options available to achieve commercial device parity
5. Proactively plan for device obsolescence
6. Develop acquisition constraints automatically stopping distribution of devices greater than two versions older than the most recent version (e.g. as of version 11 release date, version 8 is no longer orderable)
7. Develop acquisition constraints that automatically update device specifications and performance tiers as technology changes, either based on projections or actual product specifications at a particular time (e.g. the CPU requirement is not the same on day one as it is year four of a contract)
8. Expand the use and availability of desktop and browser virtualization focused specifically on externally hosted virtual desktops and browsers
9. Fully automate self-service device ordering and provisioning

2.8 Data & Analytics Services Service Group

Short definition: Data & Analytics are generally stand-alone (independent of the data) used to aggregate, replicate, analyze, normalize, control, and provide virtual access to data hosted across the enterprise, or analytics-heavy that also contain a storage component. Data & Analytics services are primarily aligned to Software, SaaS, PaaS, and Function as a service delivery models.

In scope: The scope generally applies to stand-alone data management, manipulation, and analytics tools used to manage and share data and to gain business insights. Depending on how the portfolio owner classifies the service, Data & Analytics services scope may also include some data processing Function as a Service (FaaS). Data and analytics services align most closely with the Software as a Service, Software, and Platform as a Service models than the Infrastructure as a service model. Every other service group includes an aspect of data and analytics services, so identifying the attributes unique to Data & Analytics services is difficult. The primary attribute is Data & Analytics Services are stand-alone services that are independent of the data itself. Analytics and visualization services available to privileged users such as data stewards and data scientists fall under Data & Analytics services group. The service model is a particularly important distinguishing factor when determining the difference when categorizing between Compute & Store services versus Data & Analytics services. Data & Analytics includes capabilities such as:

- Stand-alone AI and ML
- Data visualization
- Cognitive search functions
- Stand-alone indexing and translation services
- Stand-alone data synchronization and distribution services
- Data aggregation

- Data analytics software such as Informatica
- Data mediation
- Sematic data modeling software
- Any data storage capability not part of Compute & Store services
- Data warehousing
- Big data storage/analytics services such as Hadoop and Splunk

Out of scope: Services primarily providing storage, aligned more closely to Infrastructure as a Service are part of Compute & Store services. Data analysis and visualization services available to standard end-users are Workplace Automation services. Services that store data or provide analytics as part of a SaaS or application are part of the service group the SaaS or application is categorized (e.g. just because an application stores data does not make it a Data & Analytics service). Content Distribution services handle distribution of static content, not data specifically, and are therefore part of Compute & Store services. *Analytics or data manipulation is not the only criteria for alignment to the Data & Analytics service group.*

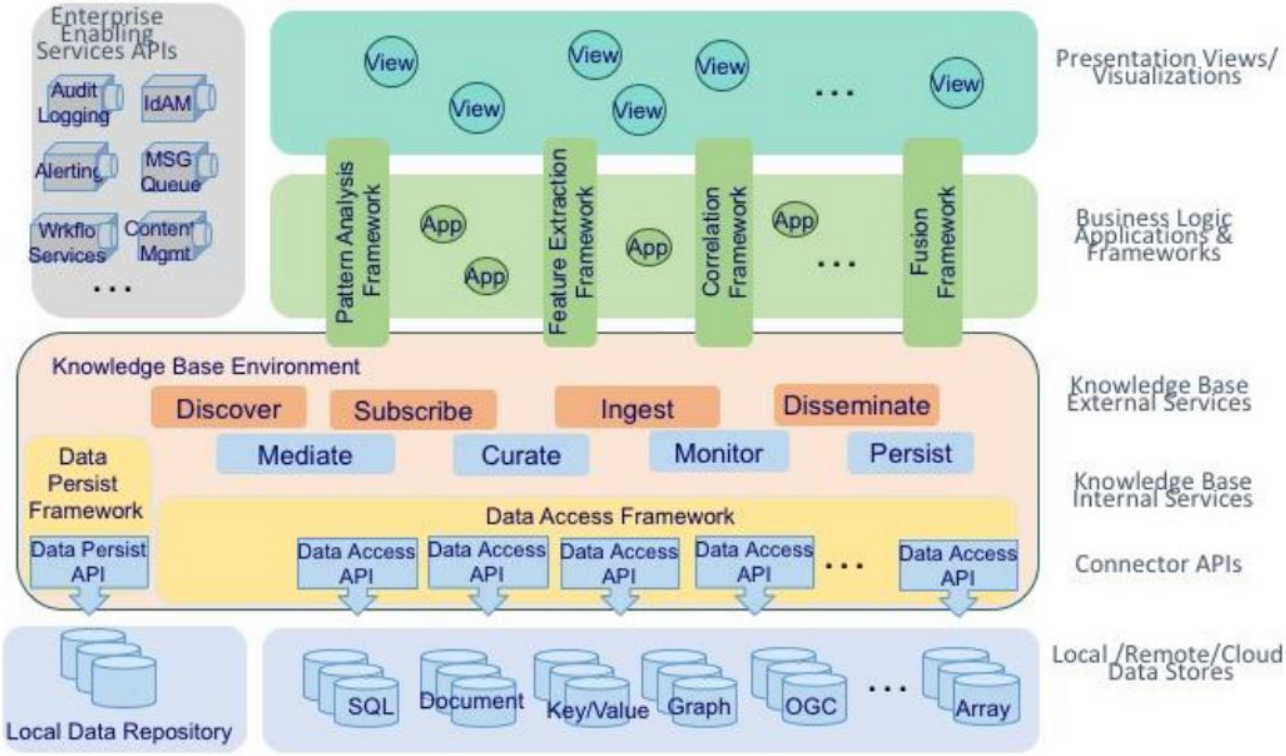
General approach explanation: The purpose of Data & Analytics services is to enable data sharing and providing insight to integrated DON data across multiple functional, system, network, ands security boundaries. Current capabilities are generally limited to identifying anecdotal and point-in-time data instead of continuous trend analysis and predictive analytics. The speed and detail possible through these capabilities will enable the DON to weaponize its data by providing trustworthy, contextual information supporting timely data-drive decision-making to win the Naval fight. Data and analytics services should automate data integration rather than forcing the warfighter to manually integrate data across systems. Data & Analytics services designs must support making the Data & Analytics service reusable across multiple network and security domains for multiple processes, and to enable access to data across many data domains to increase the ability to gain business and operational insight. This is primarily achieved by following the MSD concept of loosely coupled services. This is fundamentally different than how data and analytics services are designed today, which is stove-piped to single network or security domains or available only as part of a fully integrated activity support tool for one data domain. Following the new design concepts will ensure the DON can seamlessly architect data and services together in the future in ways not yet imagined, specified, or required now.

Data Services Design Requirements

1. Develop data services named in the Naval Data Sharing standard, Figure 11
2. Provide all the services in the Naval Data Sharing standard as a packaged Naval Data Sharing standard data environment (operationalize the reference architecture into a standard managed service)
3. Create services that fully automate production data availability to development pipelines
4. Enable automated data classification, data tagging, and content management capabilities at the data layer, not just the file layer.
5. Take advantage of AI and ML as part of data analysis services

6. Develop multi-level and cross-domain data solutions
7. Minimize data replication by enabling consumption of data from the authoritative source to the greatest extent possible
8. Design to support data level security as a baseline practice as a part of Zero Trust
9. Develop all services processing data to support central and federated policy-based RBAC and ABAC control of the data by the Naval Chief Data Officer (CDO), designated Data Stewards, and the data owner/producer

FIGURE 11: NAVAL DATA SHARING FRAMEWORK



Chapter 3 Refinement and Update

This document provides initial concepts and requirements provided early enough to influence behavior in order to mature the organization's strategic operations maturity represented in Figure 2, and better inform and align operational activities as soon as possible. New design concepts are drastically different from the past. The DON will provide updates annually to this document at a minimum as information is refined. Please check frequently for the latest version at the following public web address https://www.navwar.navy.mil/peo-digital-home/