PEO Digital
Technical Director

Modern Service Delivery Detail

Version 2.6
April 29, 2022

Prepared By:
Technical Director, PEO Digital

Version History

Version	Date	Changes
1.0	08 August 2019	Completed first publicly releasable version
1.1	16 October 2019	Updated name, references, and PEO EIS Graphic
2.0	10 April 2020	Changed scope from PEO EIS to DON
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	01 March 2022	Updated title page and figures
2.6	20 April 2022	Administrative Updates

Table of Contents

Contents

List of Figures

Addenda

(The following addenda, provided as an external document, contain more detail about design concepts and requirements per service group and technical focus area as part of Modern Service Delivery)

Chapter 1 Overview

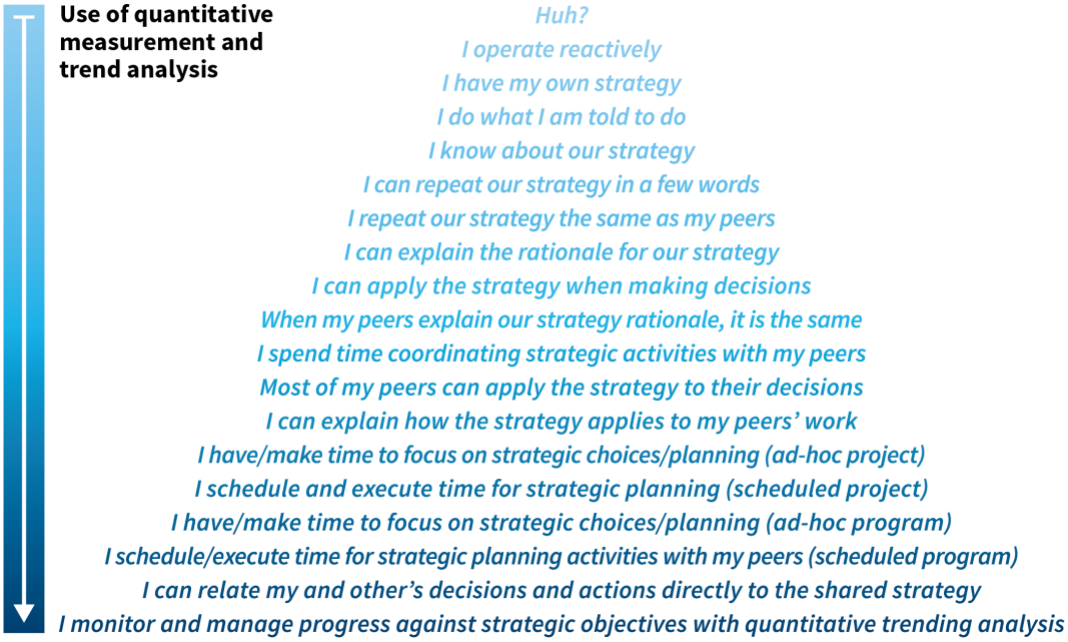
The Department of the Navy (DON) is implementing shared Information Technology (IT) services as a fundamental shift in how the organization designs, consumes and delivers services to support mission objectives and the DON Information Superiority Vision. The DON is also transforming services to better align with industry standards for service delivery. Accordingly, the design concepts for the DON portfolio of services are called Modern Service Delivery, which are generally universal decision-making guidelines aligning efforts related to a scope of work. This *Modern Service Delivery Detail* document explains the following aspects related to Modern Service Delivery:

1. Relevance of Modern Service Delivery to strategic operations
2. Background leading to Modern Service Delivery Design Concepts
3. Different views of the DON portfolio
4. Modern Service Delivery Design Concepts
5. Critical efforts enabling Modern Service Delivery

1.1 Achieving Strategic Operations Maturity

The ideal state of operations in any organization exists when tactical and strategic decisions of each employee or work unit are aligned. Strategic Operations Maturity is the level of any organization in achieving this alignment. Alignment is achieved through the creation of universal decision-making guidelines as opposed to unique considerations for each decision. Figure 1 identifies varying levels of individual and organizational knowledge and actions enabling operations alignment with strategy.

FIGURE 1: STRATEGIC OPERATIONS MATURITY



The DON strategy addresses business and technical aspects of strategic alignment at a high level. The *Modern Service Delivery Detail* document provides generally universal decision-making guidelines for the DON portfolio of technical services. The document also provides additional detail beyond the Modern Service Delivery Design Concepts and requirements to support more informed decision-making. The DON provides non-technical services to its customers as well. The *Modern Service Delivery Detail* document provides some input to those services by identifying linkages between the technical services of the portfolio and non-technical efforts necessary to enable Modern Service Delivery. In this way, employees focused on business aspects, and technical employees can align their efforts and decisions, enabling strategic operations maturity.

1.2 Background

In general, the DON lags behind industry IT capabilities by 10 years or more. This situation exists for several major reasons, including acquisition constraints in contracting information technology, limited funding, maturing of industry capabilities to meet DoD security compliance, the complexity of aligning lifecycle updates with technology improvement planning, and challenges matching direct and indirect requirements with the mission needs and technologies. This lagging trend means the DON should now plan to experience the fundamental computing transformation experienced by the private sector during the previous 5-10 years. Cloud computing drove this fundamental shift, including the change in the design pattern for use of Commercial Off the Shelf (COTS), agile development, and service management. The benefit of being a lagging adopter is the ability to leverage lessons learned from the experience of early adopters.

As a major driver for IT technology development, cloud computing is anything that has the attributes of cloud; not simply externally hosted. According to the National Institute of Standards and Technology (NIST) Special Publication 800-145, cloud computing has the following attributes: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. These attributes are relevant whether the computing is on premise or off premise, connected to the Internet or not, operating in an enclosed environment or not, including the entire IT delivery stack or not. These attributes have driven application development to focus on service development and consumption; service development to focus on agile development methods; and the service consumption to be enabled by loose coupling of services, applications, and data using standards-based Application Programming Interfaces (APIs).

Most legacy DoD and DON systems today are just beginning to follow the cloud, service consumption, agile development, and open standards path. Attempts were made across the DoD to adopt earlier iterations of similar methodologies, such as Service-Oriented Architecture (SOA), which were unsuccessful because of the inability to identify and adopt internal standardization for custom interfaces and data formatting. SOA adoption also required unfunded reprogramming of legacy Government Off the Shelf (GOTS) system interfaces in order to

publish and subscribe to services, which DoD and the DON could not afford. There are four new driving forces now addressing these issues.

The first driving force is the industry change to using loosely coupled services versus tightly coupled services. In computing and systems design, a loosely coupled system is one in which each of its components has, or makes use of, little or no knowledge of the definitions of other separate components. Components in a loosely coupled system can be replaced with alternative implementations that provide the same services. Components in a loosely coupled system are less constrained to the same platform, language, operating system, or build environment. For decades, commercial, DoD, and the DON approach for security and interoperability has been the use of tightly coupled services. These tightly coupled services have typically been part of a single network domain, managed by a single service provider. The integration between domains is expensive, time consuming, inflexible, and increases security vulnerabilities. While manageable at a small scale, DON efforts demonstrate managing this complexity by a single provider is not always possible, agile, nor straightforward. The tight coupling means component replacement is not a simple task, and there are significant downstream technological and contractual dependencies to component replacement or update. Due to lack of product interchangeability in a system of systems, dependency software or hardware updates in a tightly coupled configuration often results in a multi-year effort of sequential tasks. Loose coupling is an intentional design choice for integrated use of services across multiple networks, network domains, and services, supporting easy replacement with alternative implementations that provide the same services. System of systems components become independent and easily replaceable. Cloud-computing services follow the loose coupling design pattern, which is one of the reasons for their significant value and success.

There are many additional external business and technical drivers, strategies, mandates, and requirements influencing adoption of a loosely coupled services strategy. These influences include data interoperability, service interoperability and integration, movement to the cloud, Joint Information Environment (JIE), Federal Information System Controls Audit Manual (FISCAM), Modernizing Government Technology (MGT) Act, Department of Defense (DoD) Digital Modernization Strategy, DISA Software Defined Enterprise (SDE) implementation plan, Navy Business Operations Plan 2019-2021 (BOP), and a host of technical guidelines developed by NAVWAR. Modern Service Delivery Design Concepts reflect design patterns for commercially available software and services and recognizes the need to integrate with afloat platforms. The design choice focusing on loosely coupled COTS services is the critical linchpin in fulfilling these mandates and effectively supporting the National Defense Strategy.

The second driving force is the strategy, policy, and approach from Federal, DoD, and DON to purchase COTS software to the greatest extent possible, instead of custom developing software. As a result, the DON must plan and fund system re-platforming or system retirement of GOTS and customized COTS. While this requires adjusting the business processes, industry efforts have demonstrated the benefits of transferring the risk of interface integration and development, as well as product lifecycle costs from the Government to the product vendor. For example, even simple application software today maintains standards-based system interfaces as part of the software package. This approach overcomes the problem of ongoing and new GOTS interface lifecycle management costs experienced in the past.

The third driving force is industry transformation to develop and maintain standards-based APIs a part of its software or service. During prior decades, software vendors intentionally used custom, proprietary interfaces to force vertical integration with their product and service stacks. As commercial consumers started to adopt cloud and agile development methodologies, the vendors with custom and proprietary interfaces changed their approach to remain competitive. The industry development and adoption of loose coupling, API standardization, and vendor-provided product agnostic APIs dramatically improves application interoperability. Furthermore, aligning to external standards enhances the possibility of standardization within the DON and across the DoD. The Government's business decision to use COTS is a recognition of the value of this fundamental change.

The fourth driving force is the maturity of automation and industry standardized open-source API-based development. This can be referred to as an API economy. Industry use of open standards for vendor-provided inter-application APIs and middleware, such as API Gateway software, eliminates the tight coupling of applications and services. This loose coupling enables significant advantages. The first advantage is the easy replacement of system components without the significant redesign efforts of the past. The second advantage is that APIs can integrate other systems into the system of systems without interface redesign or data standardization at the database level. Cybersecurity systems can easily integrate and monitor Identity and Access Management systems, for example, using the default vendor provided APIs. The extensive use of automation also means that systems can be relied upon for previously manual activity, enabling secure management of increasing levels of complexity. Automation enables the organizations to redirect most resources from manual IT operations to higher-level activities or the execution of core business functions.

These driving forces support and enable a design construct of loosely coupled services. There are many advantages to the design choice of loose coupling of services. The result is the ability to provide any service, on any device, from any location. While this may appear to be a mobility focused approach, it is not. It is a fundamental change to the way the Sailors and Marines work. Mobility is not a solution; it is a design criterion for all services – enabling a mobile workforce. A second significant advantage of loosely coupled services is that it enables a transformation from legacy to new IT technology without breaking legacy operations. This transformation improves customer satisfaction, increases security, and enables the dynamic response to changing mission needs and changes in business processes. Loosely coupled services enable the DON to configure rather than customize or develop and integrate using COTS API tools rather than hard coding point-to-point interfaces. Business processes can be automated using Business Process Management software and APIs rather than coding the process into the applications themselves, enabling dynamic capability creation or adjustment in days rather than years. This dynamic ability enabled by an API economy and loosely coupled services can be applied to any perspective used to view the DON portfolio.

1.3 DON Portfolio Views

The DON portfolio and its relationship within the DoD portfolio is extraordinarily complex. One perspective of the DON portfolio is to view it as a stand-alone portfolio. Alternatively, it can be viewed as a subset of DoD's other portfolios. Each perspective of the portfolio can be valid and accurate, but unless each of the different perspectives are understood, making the most appropriate decisions,and effectively evaluating trade space and determining priorities may not be possible.

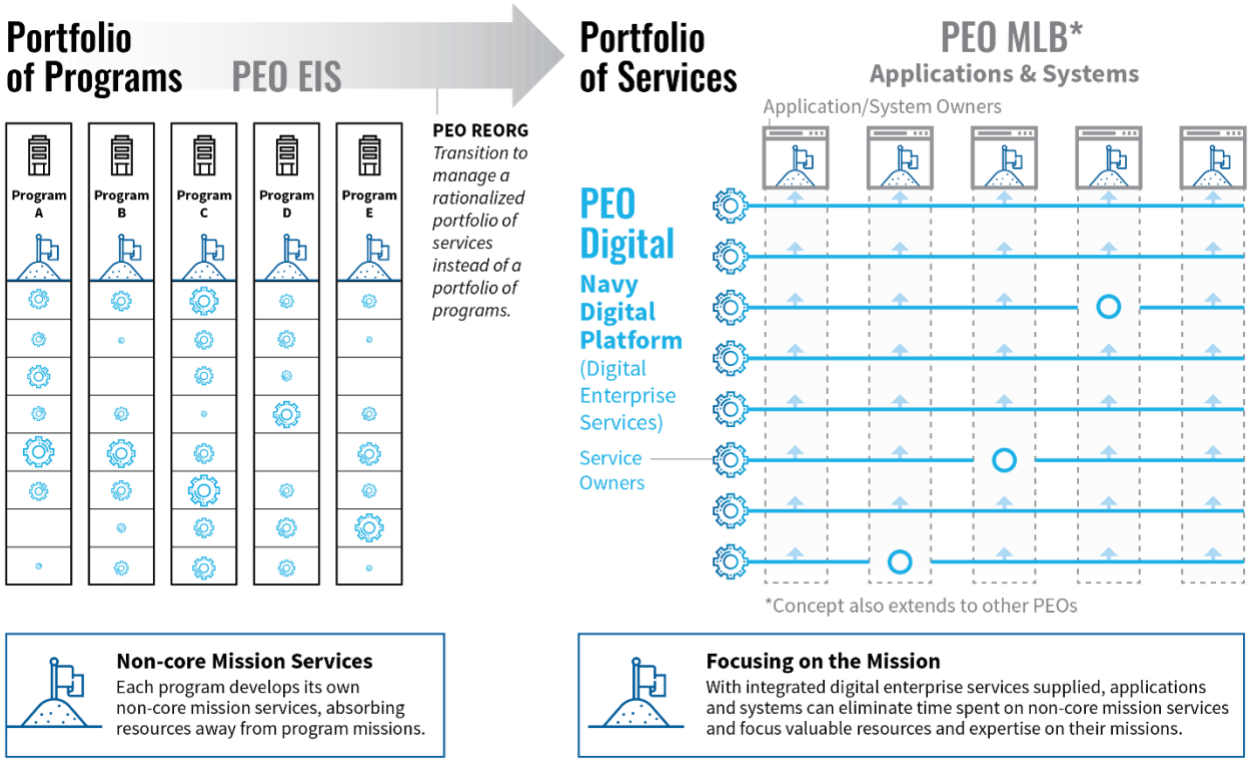
1.3.1 Stand-alone Portfolio

Within the perspective of a stand-alone portfolio, DON can be viewed as a collection of programs, services, or technical focus areas.

1.3.1.1 Program View

DON as a portfolio of programs is represented by the "Portfolio of Programs" view in Figure 2. In the Program View, each program delivers the majority of its own IT services in support of achieving its mission. Following the Program View, program independence is optimized at the cost of duplication of effort and wasted resources. A program whose mission is to deliver Human Resources (HR) functionality must deliver identity functionality, helpdesk functionality, data storage functionality, etc. Delivering IT functionality beyond HR is not part of the program's mission, but it must still be delivered by the program. The result is multiple independent programs, each with their own solutions and their own independent experts in identity, helpdesk, data storage, etc. The experts usually have multiple roles, so their specialization and expertise are limited because they operate multiple technical areas. Detailed program strategies and roadmaps should be developed but executing them results in lack of cross-program integration. The program view is the current approach used to organize and manage the DON IT portfolio.

FIGURE 2: PEO EIS REORG - THE TRANSITION TO MODERN SERVICE DELIVERY



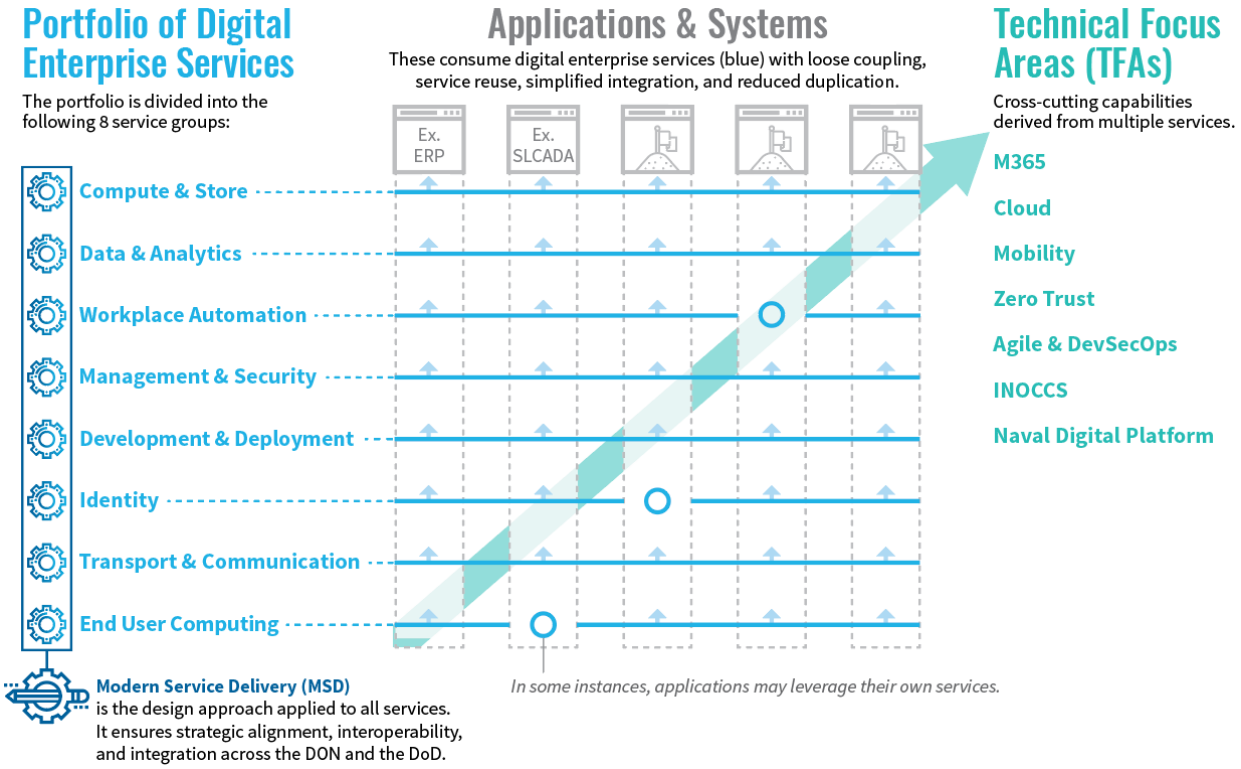
1.3.1.2 Services View

Another view of the DON portfolio is a set of independent services, represented by the "Portfolio of Services" view in Figure 2. The graphic shows PEO EIS but is representative of the DON as well. The Services View represents opportunities for resource and performance optimization. If services are designed as loosely coupled services, they can operate across multiple network and security boundaries. Instead of being delivered by programs, they are configured and consumed by programs. In the services view, one organization can optimize its use of resources to deliver identity services, for example, to all programs. Following the services view, optimizes performance and use of DON resources at the cost of program independence. However, optimization of a shared service may not result in optimal alignment for a Technical Focus Area. Development and optimization using the Services View is the desired state, and efforts are underway by the DON to start organizing and managing shared IT services in alignment with the Services View. Detailed design concepts for each of the identified service groups are addressed in the addendum *Modern Service Delivery - Service Groups* document.

1.3.1.3 Technical Focus Areas View

A third view of the DON portfolio is based on "Technical Focus Areas" as shown in Figure 3 (a specific approach to a subject), which can affect multiple programs, and multiple service groups. Technical Focus Areas are subject areas that are neither a service view or a program view. Detailed design concepts for each of the identified strategic technical focus areas are addressed in the addendum *Modern Service Delivery - Technical Focus Areas* document. Individual one-page executive summaries for each technical focus area are available or in development.

FIGURE 3: DON PORTFOLIO VIEW



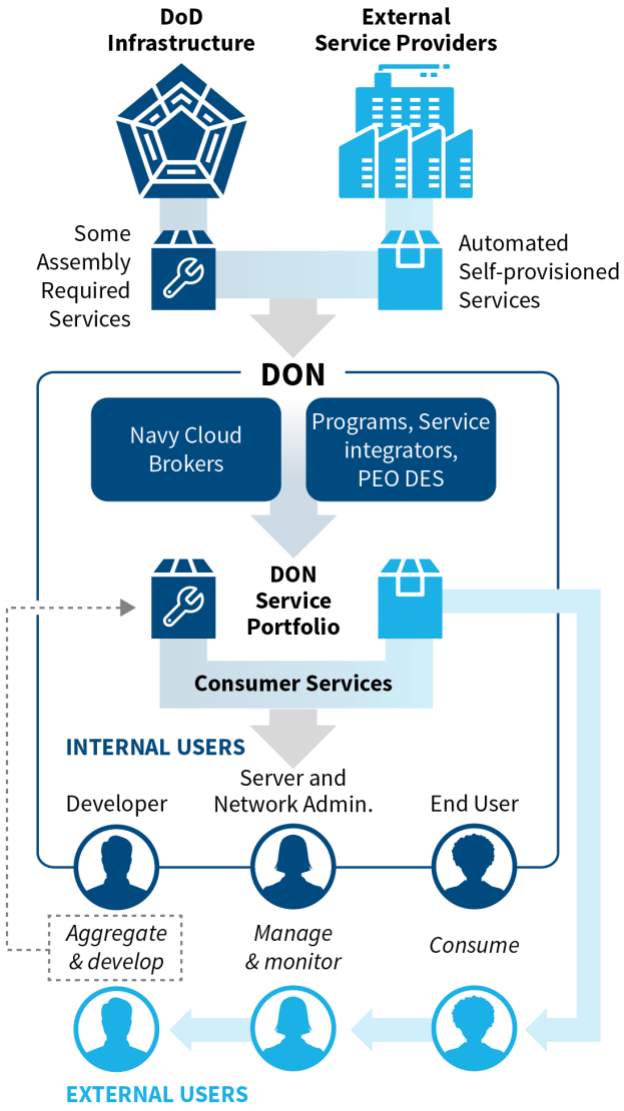
1.3.2 DoD and DON Portfolios

Another perspective of the DON portfolio is part of a larger commercial and DoD portfolios. When viewed in this context, service provider and service consumer roles change, and a provider, such as DON can be both a provider and a consumer of the same service. Organizations such as commercial cloud service providers, DISA, or any other DoD organization can be an "External Service Provider." This services consumer and provider relationship is depicted in Figure 4.

The DON provides services internally and externally to multiple customer types through the service catalog (covered in Chapter 3). Customer/Provider relationships are an important consideration for service development, prioritization, and portfolio gap analysis. When performing portfolio management and portfolio rationalization, the DON must deliberately decide if each program, or DON at large, should be a consumer or a provider of a service. Rationalization leads to the conclusion of developing or consuming services for use by multiple programs. Those services are shared services, and when delivered by across multiple network or security boundaries are called Digital Enterprise Services.

FIGURE 4: CONSUMER/PROVIDER VIEWS

1. DON is a Service Consumer and a Service Provider
2. DON is a Service Provider for Internal and External Customers
3. Services can be Automated, Self-Provisioned, or Some Assembly Required



1.3.2.1 Shared Services

Shared services are individual named services that are consumed by more than one program in the DON portfolio. Loosely coupled shared services enable service reuse, simplifies integration, and reduces program duplication of effort. When services are shared across the DON portfolio, they are represented as the "Portfolio of Services" in Figure 2. As a result of consuming shared services, each program can focus its financial and human capital resources on its core mission.

Shared services can be grouped with like services, as depicted in the DON Portfolio view, Figure 3. Detailed design concepts for each of the service groups is addressed in the addendum *Modern Service Delivery – Service Groups* document as a summary, and individual one-page executive summaries for each service group are available or in development.

1.3.2.2 Digital Enterprise Services

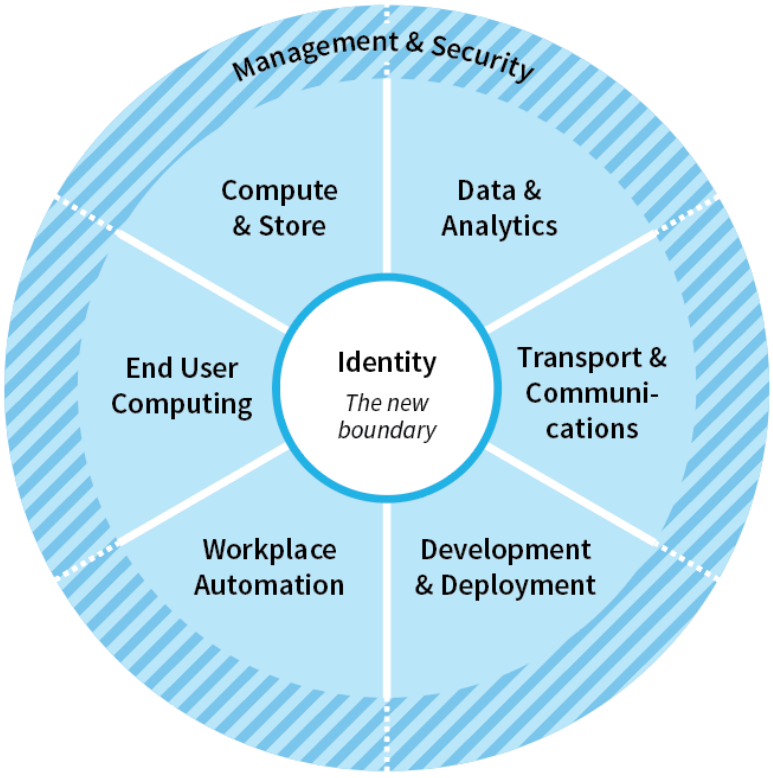
Expanding the scope of service providers and consumers means any organization can provide or consume shared services. When shared services are designed as loosely coupled services that operate across multiple network and security boundaries, they become Digital Enterprise

Services (DES). The DON has identified eight groups of similar services. The eight Digital Enterprise Service Groups are identified in Figure 5. Each Service Group has its own set of design concepts and requirements, identified in the addendum *Modern Service Delivery – Service Groups*. When viewing shared services as Digital Enterprise Services, the DON can perform portfolio rationalization and decide to stop being a provider of a service, and instead become a consumer of a Digital Enterprise Service provided by an external organization, such as a Navy Cloud Broker, or DISA. At the same time, organizations other than DON can decide to become consumers of DON shared services, making the DON service a Digital Enterprise Service.

This approach results in the need to simultaneously rationalize services inside and outside of the DON portfolio. The DON is collaborating internally and externally to standardize service groups, service group definitions, and identify Digital Enterprise Services for development, and alignment efforts are still underway. The addendum *Modern Service Delivery – Service Groups* document describes the DON design concepts and requirements for services based on service groups. The addendum *Modern Service Delivery – Technical Focus Areas* document has a section with service design concepts for Digital Enterprise Services, which is the internal and external service overlap.

Regardless of the view applied, the DON Modern Service Delivery design concepts will apply to all services under the control of the DON. The DON is working for adoption of Modern Service Delivery design concepts as a requirement for all future cross-agency and inter-organizational collaborative service development efforts to ensure flexibility and interoperability.

FIGURE 5: DIGITAL ENTERPRISE SERVICES

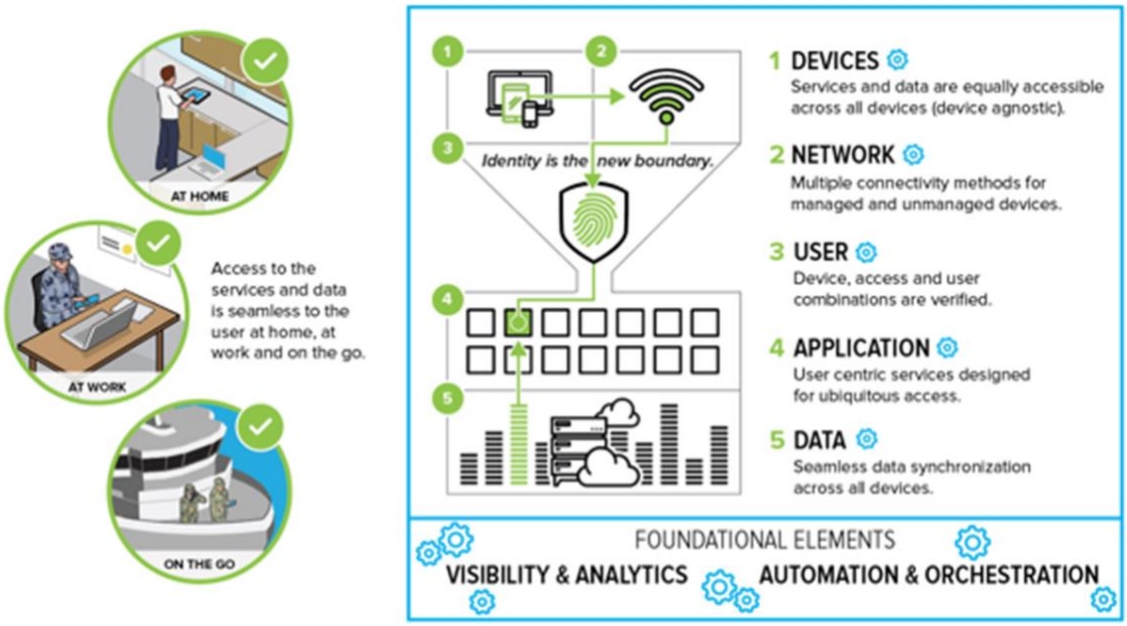


Chapter 2 Modern Service Delivery

The design concepts applying to all DON Technical services are called Modern Service Delivery. 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. The Modern Service Delivery Design Requirements are as follows:

- 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

FIGURE 6: MODERN SERVICE DELIVERY



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

Chapter 3 Modern Service Delivery Enablement

Execution of Modern Service Delivery, and alignment to the Modern Service Delivery Design Concepts will require the coordination of many enabling technical, business, and organizational efforts. When viewing the DON portfolio as part of a larger DoD portfolio, it is not important whether or not the efforts in this section are wholly owned, managed, or delivered any particular organization. With the exception of those identified specifically for the DON, efforts included below are not intended to infer that the DON plans on leading or owning the effort. It is only significant and important that the effort is taken on behalf of, and to affect the consumers of DON services. Some of the most notable efforts 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 providing organizations for new services
- Deliver shared (Digital Enterprise Services) across all Naval security and network domains
- Enable Continuous Integration/Continuous Deployment (CICD) across all environments
- Adjust acquisition, Cybersecurity Operations, and Certification and Accreditation processes

Technical Efforts – the DON will transform the design approach for all services and applications from tightly coupled to loosely coupled COTS services and applications aligned with industry capabilities to the greatest extent possible.

Business Efforts - The Enterprise Service Provider(s), Navy Cloud Brokers (NCB), and Navy Technical Agents (NTA) will focus business activity on delivering services through self-service automation. Enterprise Service Providers are organizations that deliver any of the Digital Enterprise Services. NCBs are specific Enterprise Service Providers that deliver cloud-hosted services. Self-Service automation is the full automation of all steps between service request to provisioning and delivery to the end user. Self-service provisioning completely eliminates human interaction between the requestor and the service delivery. The move to consumption of services will enable the DON to focus more effort on the acquisition and orchestration of services. The DON will identify, subdivide, and coordinate the delivery of DON provided Digital Enterprise Services by Enterprise Service Provider(s) and NCBs.

Organizational Efforts – the DON will develop organizational management and governance structures to guide the development and orchestration of services from the Digital Enterprise Service Providers and NCBs. Reorganization around common shared Digital Enterprise Services will affect what programs such as Navy Marine Corps Intranet and NCBs deliver and consume. Organizations inside or outside of DON might deliver the Digital Enterprise Services to the DON, making the DON a consumer of a service as opposed to a provider.

Using the approach of shared services and Digital Enterprise Services, Enterprise Service Provider and NCBs' primary business function will be the delivery of underlying shared IT services. PEO Digital Enterprise Services (PEO DES) will coordinate the delivery of the underlying shared IT services, delivering some services and front-ending other services delivered by other organizations. PEO Manpower, Logistics, and Business (PEO MLB) primary business function will be the delivery of end-user consumed manpower, logistics, and business applications. Logistics, etc. Applications managed by PEO MLB will consume the loosely coupled Digital Enterprise Services to enable their primary business function, reducing the redundancy of individual programs managing capabilities not directly related to their primary business function. Across the DoD and DON, this will reduce duplication of similar work and enable data and functional interoperability. Enabling the use of the Digital Enterprise Services to programs outside of the DON will extend this business value of reduced duplication of work and increased interoperability.

3.1 Enabling Actions

Many actions are necessary to efficiently enable Modern Service Delivery and consumption. Several of the more notable actions are detailed in this section.

The DON will develop a DON level Service Catalog and roadmap identifying individual and common services. The DON is responsible for the acquisition of IT services. The foundation of any IT service organization is its service catalog. The service catalog identifies the

services available for consumption. The service roadmap will identify the new/updated services, time phased based on planned future availability. The service catalog provides a single source of consistent information on all services to ensure services are widely available to authorized consumers. From the business aspect, the service catalog is the primary tool to manage changes to services, service delivery models, and service delivery organizations. The DON will deliberately prioritize service development in support of planned service improvement using the service catalog and service roadmap as a tool.

The DON will subdivide the service catalog into service groupings to enable alignment of contracts, service providers, acquisitions, organization, and best practice implementation. Organizations operate, manage, and acquire services along similar lines of service for simplicity. The DON organizes services today organically under a program management organizational construct, but each program provides its own underlying shared IT services. The service-oriented organization represented by the "Services View" in Figure 2 represents an opportunity to optimize the DON organization by standardizing and delivering shared IT services across multiple programs. The current approach forces organizations to design, build, and deliver non-core mission services in order to fulfill their core mission. This leads to duplication of work, waste of resources, and suboptimal performance across the programs. This approach resulted in the creation of monolithic enterprise service providers, which has created challenges. In particular, tightly coupled services from monolithic service providers resulted in a lack of flexibility, responsiveness to customer needs, and an inability to integrate data or capability across multiple service providers and multiple network and security domains.

The subdivision and then integration of service groupings also results in new boundaries of security by forcing interaction across the service groups to enable an integrated user capability. Today, the DON relies heavily on external network boundary and perimeter defense. When services are loosely coupled, bad actors must gain control of services from more than one service grouping to obtain access to applications and data. This subdivision leads to two centrally significant changes. The first change is moving from a perimeter defense heavy model to a Zero-Trust rust model. The second change is that rather than monitoring the entire operation of all services, security can focus on continuous monitoring the interaction between services. This transformation is critical to support the adoption of cloud computing. In particular, the consumption of Software as a Service (SaaS) means the DON will not have the traditional in-depth control of the delivery of the service, but it can maintain visibility and control of the interaction between that service and others.

The DON will make a self-provisioned Continuous Integration Continuous Development (CICD) pipelines as a service available. As identified in Figure 4, a severely unserved customer base is internal and external developers. These developers require consistent, self-provisioned baseline services to perform application development and integration. Compile to Combat in 24 hours (C2C24) is a currently well-recognized effort to realize the value of full CICD pipeline implementation for a particular network segment in the DON, and there are other similar efforts across the DON for other networks. The DON has many target environments, each with its own constraints. The DON will consolidate development factories and differentiate pipelines for different target environments and mission/development needs. The Factory is the provision and development portal. Creation of a single factory will support efficient use of

contracting resources, licensing costs, consumption management, and reuse of baselines and content from one pipeline to another. This model supporting development and operations provides unquestionable value, and CICD is an industry standard as a result.

In order to achieve automated Development, Security, Operations (DEVSECOPS), all NCBs and Digital Enterprise Service providers will make development and production versions of their services available through self-provisioned CICD pipelines. The DON can benefit from the value demonstrated by the C2C24 Implementation Standard and other similar efforts. Benefits include reduced lifecycle cost for development work, increased cybersecurity, and overall a dramatic acceleration of technology adoption. The ability to provide a trusted self-service CICD pipeline as a service as government furnished equipment for application developers and service providers will fill a critical existing gap in DON services. The trusted CICD pipeline is also the foundational enabling component of the new Zero-Trust approach to cybersecurity.

The DON will create and distribute roadmaps and strategic requirements to the program offices. Historically, the DON roadmaps were an aggregation of the program roadmaps. The bottom-up approach results in a suboptimal use of DON resources and reduces alignment between strategy and execution. Creation of a centrally managed roadmap based on strategic priorities enables the coordination of resources across multiple programs and improves customer experience by setting customer expectations for service changes. Developing a roadmap that reflects DON strategic priorities is necessary to optimize digital transformation efforts.

The DON will develop shared services as loosely coupled COTS-based services, aligned with industry capabilities, and designed to operate in a hybrid multi-cloud, multi-network environment. Loose coupling of services is a design pattern currently used in industry because of technology evolution. This design pattern enables the consumption of services across networks, directories, security boundaries, and infrastructures. As the DON moves to operate in a hybrid multi-cloud environment, this design change is critical to overcome the constraints of current tight coupling under single security and network boundaries. Loose coupling and the ability to integrate services across boundaries will also increase security. Integrated security services using APIs enable cyber security to analyze data across multiple domains and network boundaries for greater visibility and control. Use of machine logic and Artificial Intelligence (AI) as a part of continuous monitoring will identify threats and automate mitigation.

The DON will collaborate with internal and external cybersecurity stakeholders to change how the cybersecurity mission is accomplished. The existing cybersecurity environment relies heavily on people, processes, and boundary protection. Cybersecurity functions are therefore difficult to manage, resource heavy to accomplish, and time consuming to complete. Industry has made the fundamental change from this approach to one of automation and evaluation of the process as well as the products. The three fundamentals of this approach are to, 1) Develop a trusted development process, 2) Accept the output of the process and product analysis, and 3) Continuous monitoring of the operational environment against trusted baselines. As long as the process is trusted, the output can be trusted, and continuous monitoring can identify and mitigate configuration drift. This approach goes for software development as well as transport/network

itself. Industry has automated these processes to such a significant success that it can operate and secure data centers serving millions of customers globally using only a handful of people. The change to how the cybersecurity mission is accomplished is so fundamentally different from how the DON operates today, it will require cultural, organization, process, and product changes.

The DON will provide a Community of Practice (COP) support to programs. While the Federal, DoD, and DON strategy for applications direct the use of COTS software and capabilities by default, the DON's progress in cloud adoption is dependent on developing an organization mature in the acquisition and use of cloud computing technology. In order to support the development, creation, and adoption of Digital Enterprise Services using on premise and off-premise hosted cloud computing services, the DON needs a cadre of staff with detailed knowledge and expertise in contracting, engineering, and executing such services in the DON. This Community of Practice will be a source of information and expertise that will evolve and mature until all programs in DON have organic knowledge and experience. For the small case of custom application development, such applications or custom integration will consume DON Digital Enterprise Services. This design constraint maintains the value created by developing reusable Digital Enterprise Services and reduces further service development sprawl and lifecycle management costs not directly related to program core business function. Over time, this will result in the retirement of legacy systems and adoption of commercial products, services, and design patterns and pervasive organic capability in each program.

The DON will ruthlessly automate everything. Capabilities for automation have evolved in industry, but the DON relies on relatively few automation capabilities. Industry developed automation capabilities in response to cloud computing, IT complexity, and the need for improvements in performance and cost. Automation improves user satisfaction, performance, and reduces costs by providing self-service provisioning for simple to extraordinarily complex services. Automation eliminates manual work, human error, and time delays by providing real-time network mapping and monitoring. Automation increases security by sensing and remediating configuration drift. Automation enables scaling from 1 to N with a consistent and predictable price. Automation improves performance by sensing and responding to demand. Automation improves security through testing and continuous monitoring. Automation reduces cost and increases security by responding to threats without the need for human interaction. Automation through AI improves security by sensing, flagging, and responding immediately to previously undetectable authorized insider threat actions. Automation can unlock previously undiscoverable data relationships to enhance human decision-making. Automation of every aspect from provisioning to problem resolution will be critical to ensuring DON services deliver and enhanced and positive customer experience, enhance decision-making, and increase agility and affordability.

Please check frequently for the latest version at the following public web address https://www.navwar.navy.mil/peo-digital-home/