PEO Digital
Technical Director

Modern Service Delivery
Technical Focus Areas

Version 2.6
April 29, 2022

Prepared By:
Technical Director, PEO Digital

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	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	23 February 2022	Added INOCCS TFA. Added NDP. Removed RPA and SDx. Updated Images. Updated cover page.
2.6	22 April 2022	Moved NDP to a TFA

Table of Contents

Contents

List of Figures

Chapter 1

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 – Technical Focus Areas* is an addendum to *Modern Service Delivery Detail. Modern Service Delivery Detail* provides and explains frameworks governing decision-making for design and development of services managed by the DON and explains design concepts applying to all DON technical services. *Modern Service Delivery Detail* addresses the relevance of and background leading to Modern Service Delivery. Different views of the DON portfolio exist, including Program View, Services View and Technical Focus Areas View.

FIGURE 1: STRATEGY TO EXECUTION

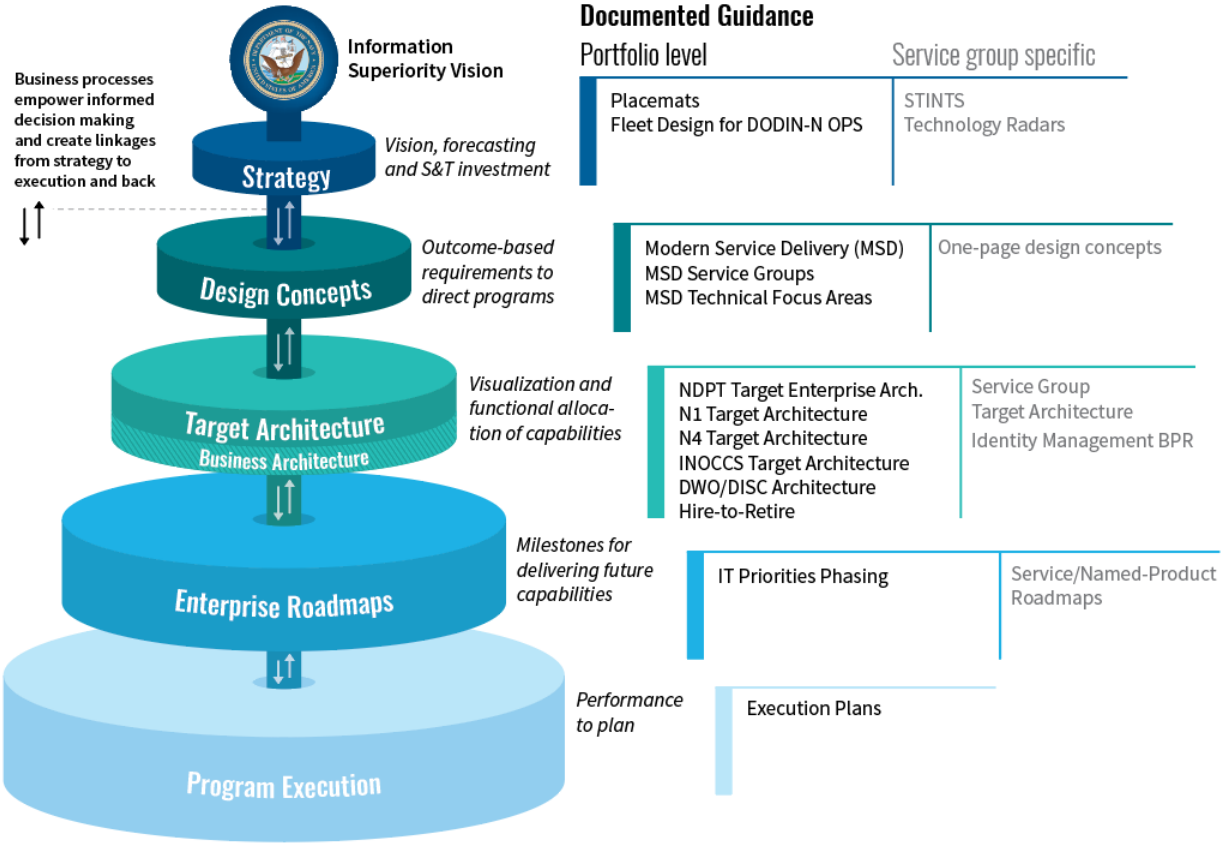
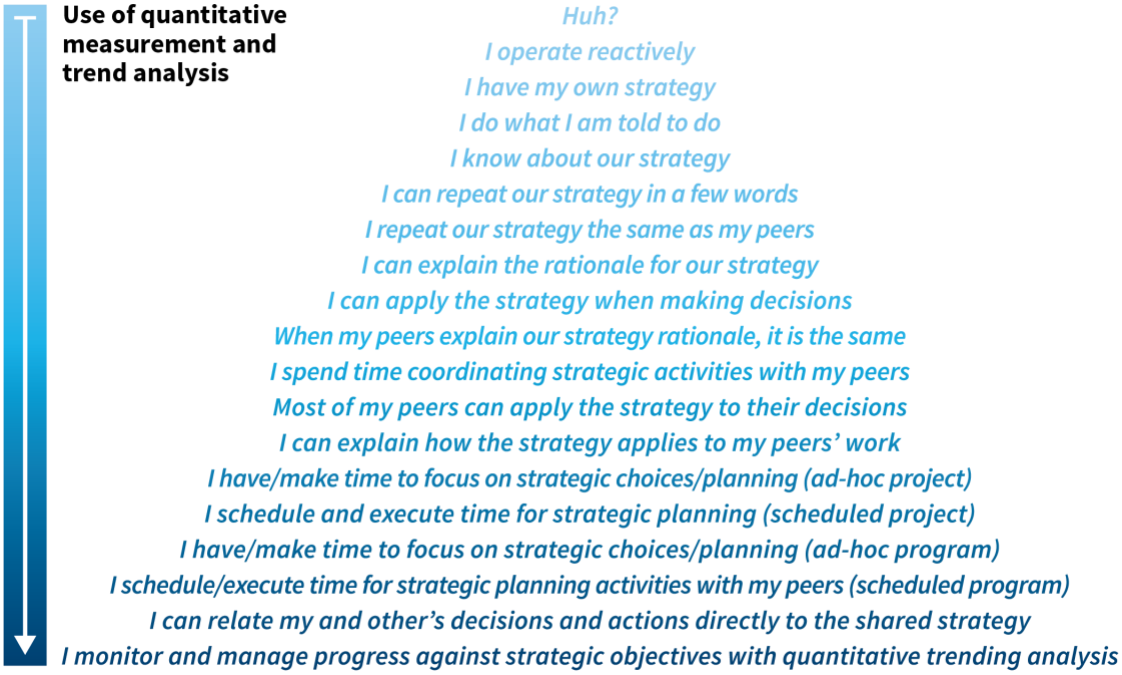


Figure 1identifies the alignment and increasing levels of detail from the DON CIO strategy, which includes modernize, innovate, and defend pillars. The design concepts and requirements detail supports all three pillars of the DON CIO strategy, but most closely align to the modernize pillar, which includes 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 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.

This *Modern Service Delivery Technical Focus Areas* document further elaborates on some specific strategic areas in support of the DON mission, vision and strategy. The purpose of this document is twofold. First is to help the audience and organization to improve Strategic Operations Maturity as depicted in Figure 2. The second and perhaps more important purpose, is to provide a list of design concepts and specific requirements related to strategically important technical focus areas, which are to be applied during service or system development or replacement.

FIGURE 2: STRATEGIC OPERATIONS MATURITY



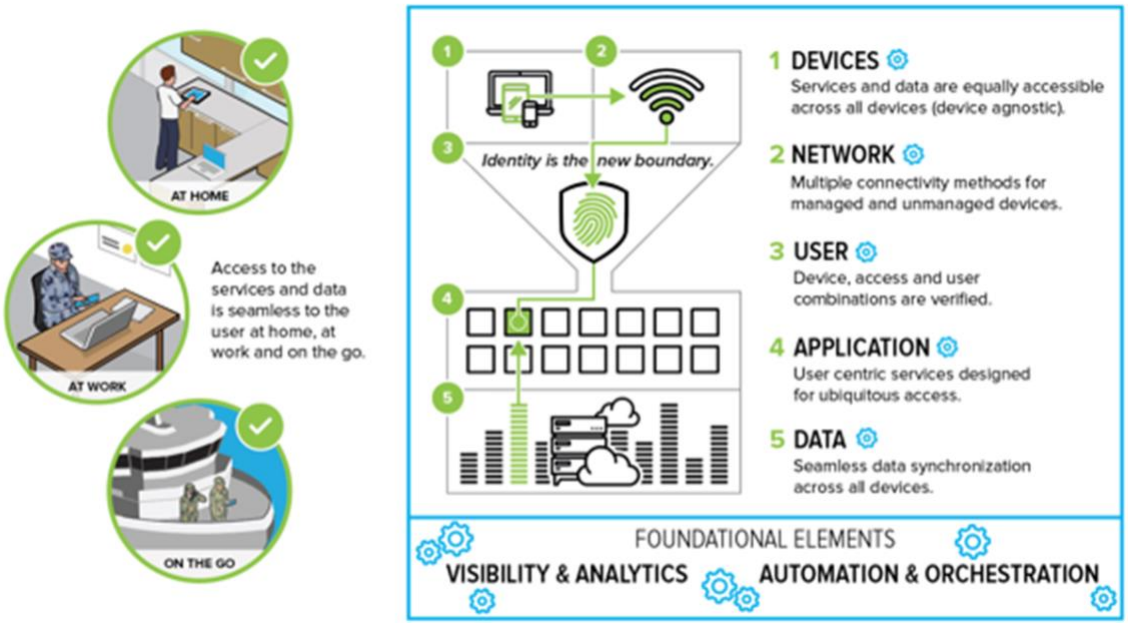
1.1 Modern Service Delivery Design Concepts

The sum of design concepts applying to all DON technical services is called Modern Service Delivery, represented in Figure 3. 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).

- 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 re-usable 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 3: MODERN SERVICE DELIVERY



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

1.2 Non-technical Ramifications

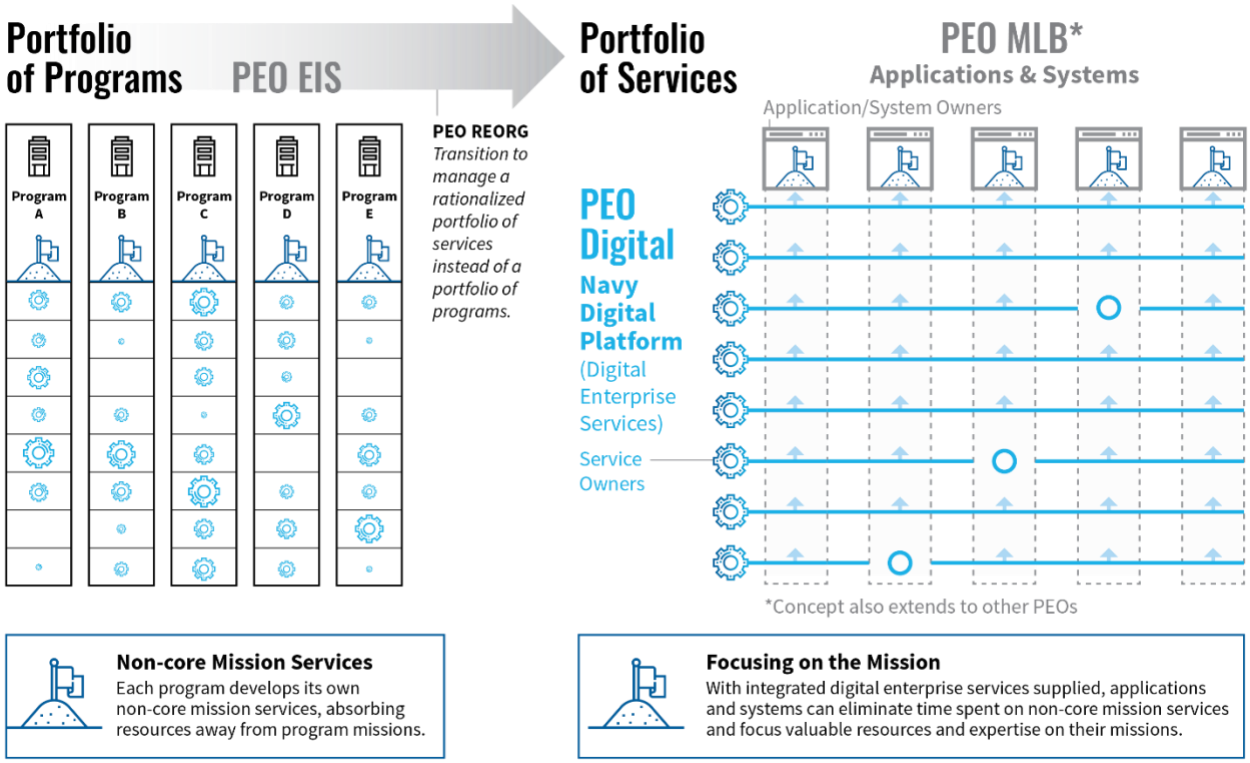
For the DON to execute these design concepts effectively, several non-technical aspects must be addressed. Some of the most notable aspects are as follows:

- 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 organization for new services
- Centrally deliver Digital Enterprise Services across security and network domains
- Enable Continuous Integration/Continuous Deployment (CICD) across all environments
- Adjust acquisition, cybersecurity operations, and certification and accreditation processes

1.3 Technical Focus Area 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. Figure 4 identifies the relationship 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



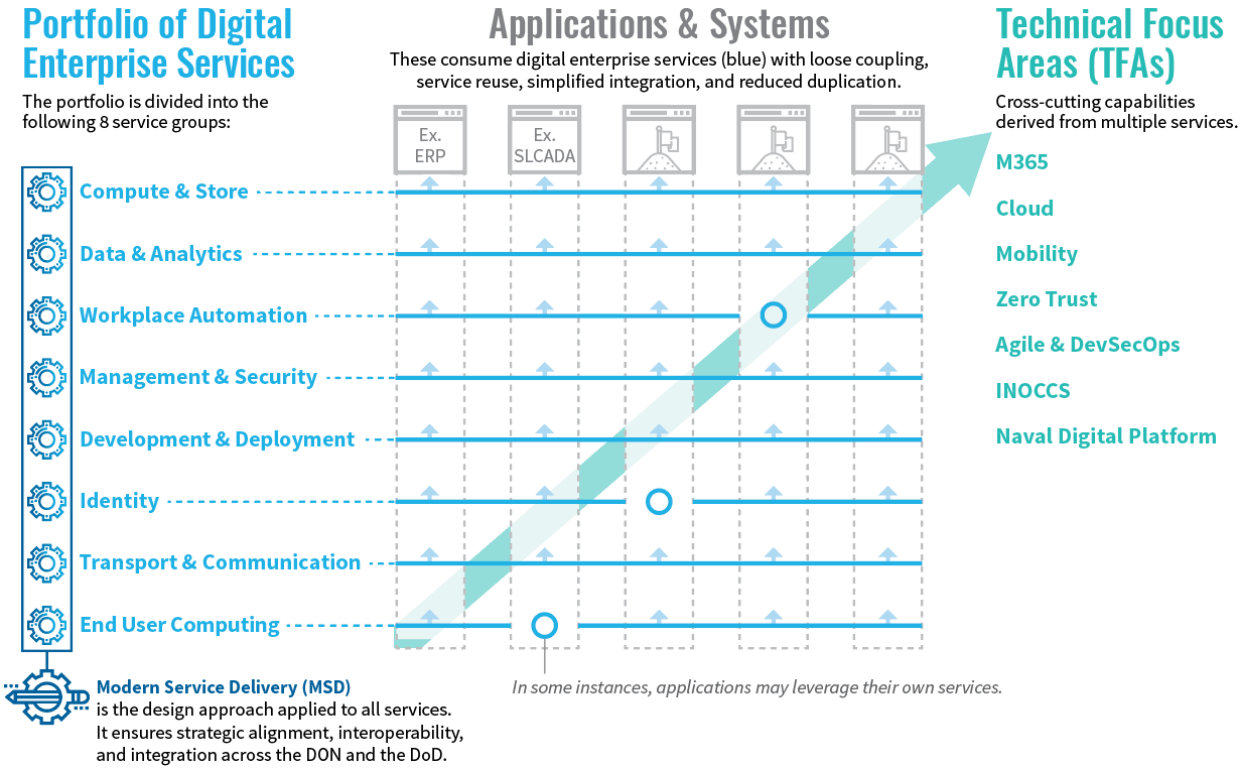
The third view of the portfolio is based on technical focus areas (a specific approach to a subject), which can affect multiple programs from the program view, and multiple services from the service view.

The *Modern Service Delivery Detail* document provides design concepts for all services. *Modern Service Delivery - Service Groups*, provides design concepts specific to each of the service groups listed on the left in Figure 5. This document, *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 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 Technical Focus Areas

Technical focus areas are groupings of technologies and concepts around a specific technology subject area. The services combine to provide capabilities related to a technical focus area are derived from more than one of the Service Groups identified in the previous chapter. Figure 5 identifies the relationships between Service Groups and Technical Focus Areas. Service Groups are grouping of *similar* services, Technical Focus Areas are groupings of *related* services.

FIGURE 5: DON PORTFOLIO VIEW



2.1 Cloud Computing Technical Focus Area

Cloud Computing Technical Focus Area scope includes all services that have the five attributes of the NIST definition of Cloud (on demand self-service, broad network access, resource pooling, rapid elasticity, measured service), including all service models (IaaS, PaaS, SaaS) and all deployment models (Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud). Services hosted on dynamically allocated resources that do not have all the attributes of cloud computing are NOT CONSIDERED TO BE CLOUD COMPUTING BY THE DON. Navy Cloud Brokers (NCB) or Navy Technical Agents (NTA) manually provisioning services for a customer on externally hosted cloud is not considered successful delivery of cloud to consumers. This is because cloud computing provides the maximum inherent value through the availability of all the NIST attributes of cloud to the end user. The hosting location or model alone provides only partial value.

Cloud Computing Design Requirements
1. Consume as high up the stack as possible (order of precedence SaaS, PaaS, IaaS)
2. Develop Navy Cloud Brokers capability to deliver self-service commercial cloud services
3. Proactively identify and make commercial cloud services available through coordination of Navy Cloud Broker and Digital Enterprise Services service portfolios
4. Move to a hybrid multi-cloud deployment model
5. Replace on premise infrastructure with evergreen on premise cloud service
6. Make a virtual development environment available as a self-provisioned service
7. Standardize between on-premise and off-premise security approaches

FIGURE 6: CLOUD COMPUTING AS-IS

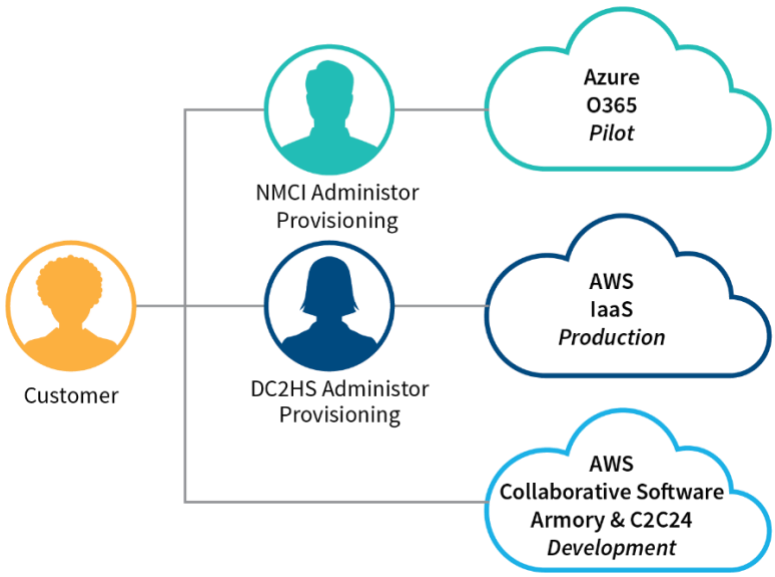
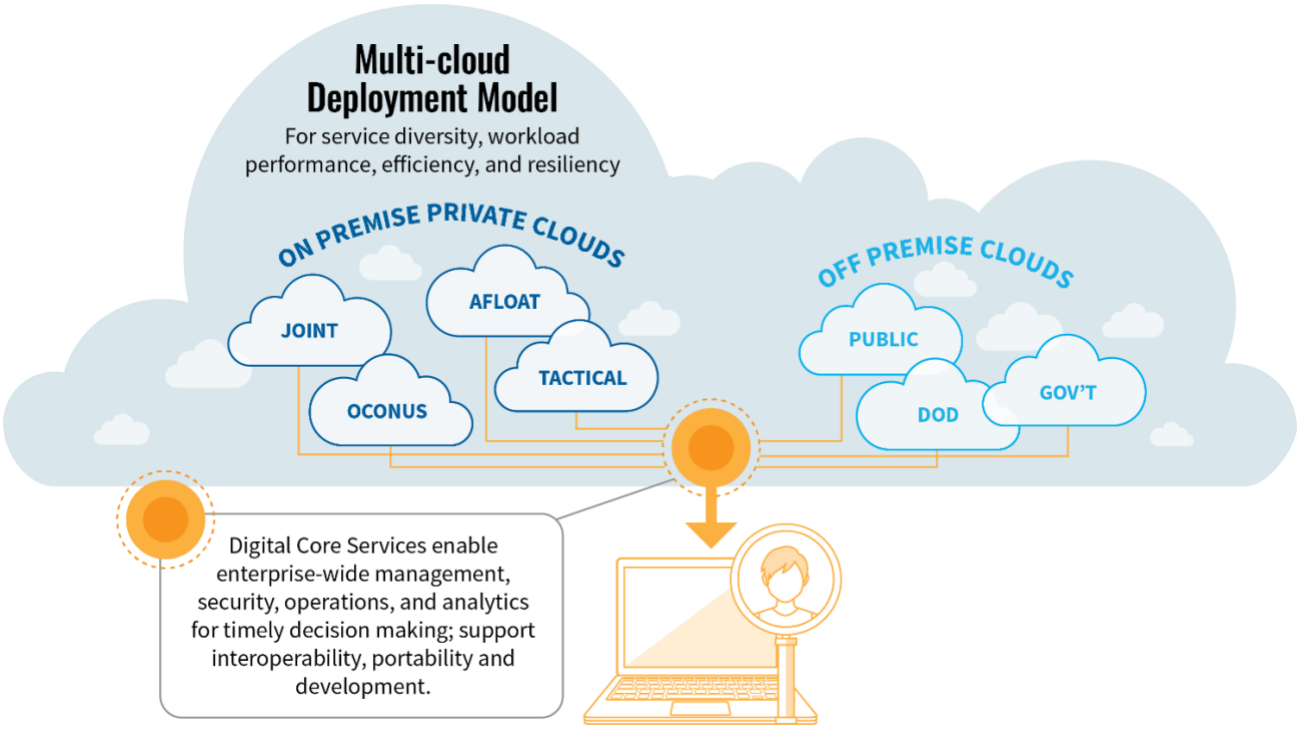


FIGURE 7: CLOUD COMPUTING TO-BE



2.2 Mobility Technical Focus Area

Mobility Technical Focus Area scope includes all services enabling a mobile workforce access to data and applications from anywhere on any device. The scope is intentionally broader than commercial mobile devices and mobile applications. The scope includes web application design, virtual desktop, wireless networking, and other services enabling a more mobile workforce. While mobility is considered a technical focus area, it will apply as a design concept to all services, changing from a named Technical Focus Area to simply the way we work. Mobility services are historically treated as distinct solutions to support a mobile workforce. In accordance with Modern Service Delivery design requirements, all services should be designed to be inherently support a mobile workforce. The Mobility design requirements below are derived from the MSD requirement "Design for mobile access" that applies to all services. As a result, the graphical representation of mobility to-be, Figure 9, is the same as the MSD graphical representation showing all services inherently designed to support mobile access.

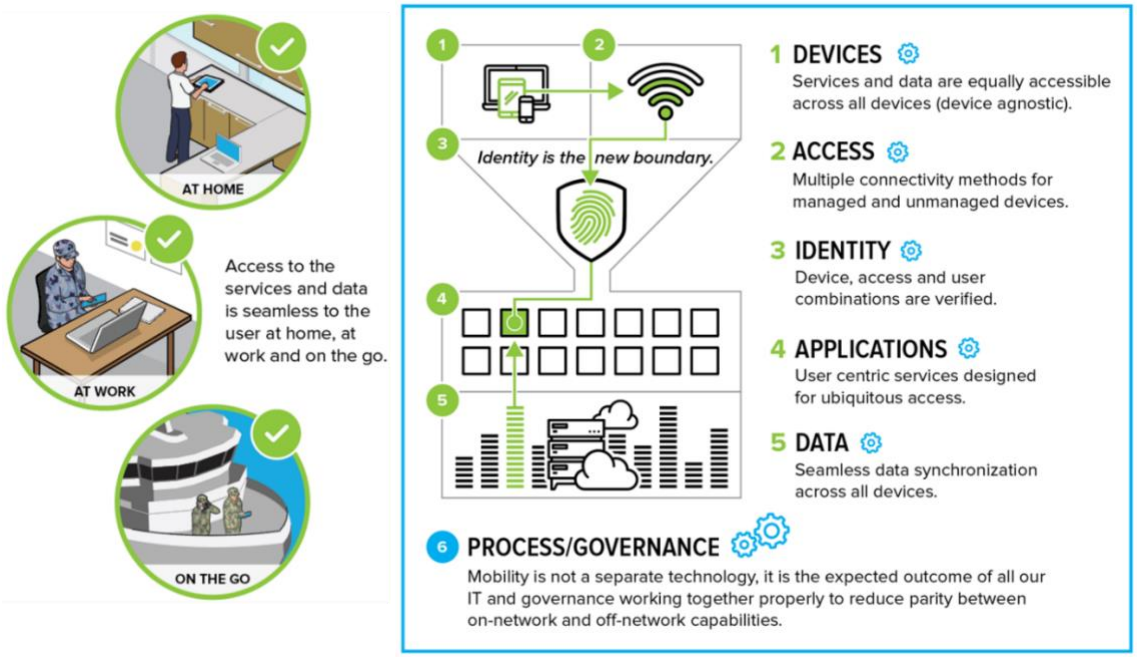
Mobility Design Requirements

1. Make services and data equally accessible across all devices
2. Provide multiple connectivity methods supporting managed and unmanaged devices
3. Verify device, network, user, and authentication method combination to provide appropriate access
4. Develop user centric services designed for ubiquitous access
5. Provide seamless data synchronization across all devices
6. Expand availability of services which do not place data on the end user device

7. Design services with the intent to integrate/collaborate with coalition partners and the Defense Industrial Base (DIB)
8. Improve parity between user experience on different devices and between on-network and off-network capabilities

FIGURE 8: MOBILITY AS-IS

FIGURE 9: MOBILITY TO-BE (MODERN SERVICE DELIVERY)

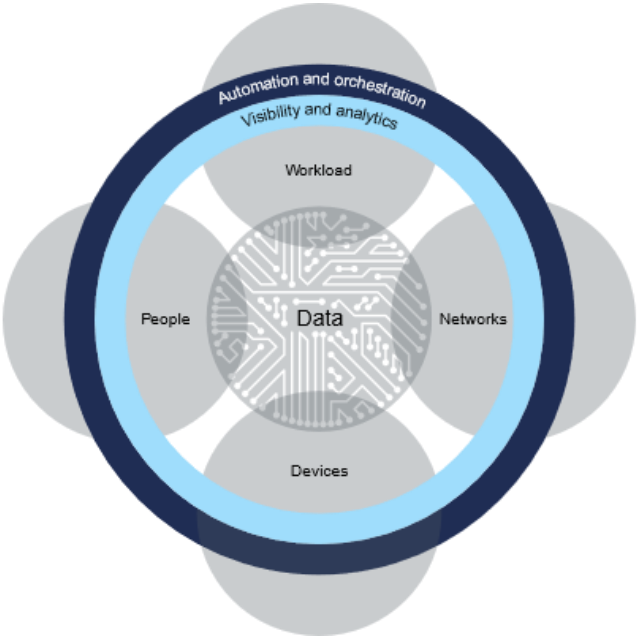


2.3 Zero Trust Technical Focus Area

Zero Trust Technical Focus Area scope includes all services supporting progress toward a Zero Trust security approach. Application of the design concepts in this Technical Focus Area will span a significant portion of the DON service portfolio. Zero Trust is an information security design approach using a set of intertwined and interdependent adaptive processes, capabilities, and controls with data-driven feedback loops based on risk/trust levels.

There are many models for Zero Trust, most notably Forrester Zero Trust Networking, Forrester Zero Trust Extended, Gartner's Continuous Adaptive Risk and Threat Assessment (CARTA), and Google's BeyondCORP as examples.

FIGURE 10: FORRESTER ZERO TRUST

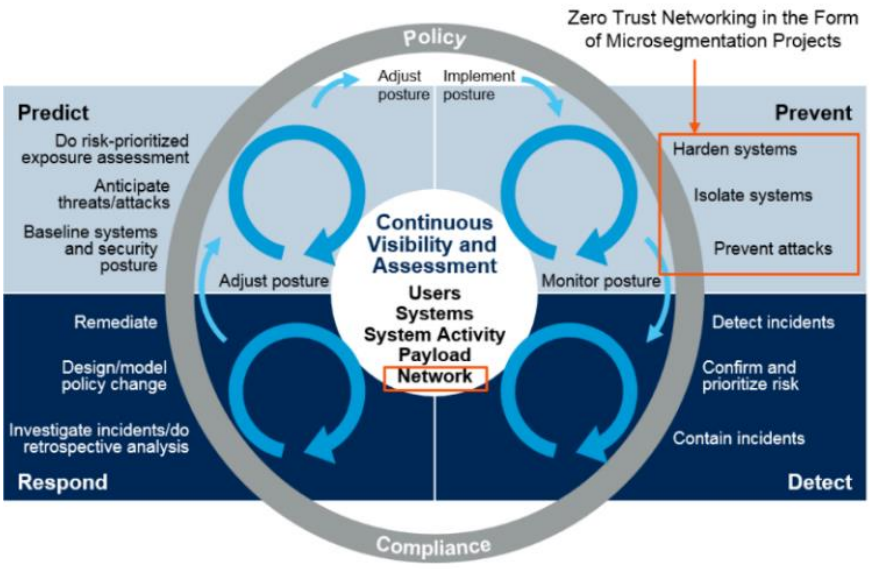


https://go.forrester.com/government-solutions/

FIGURE 11: GARTNER CARTA

Zero Trust is an initial step on the roadmap to Continuous Adaptive Risk and Trust Assessment (CARTA)

Adaptive Attack Protection Architecture

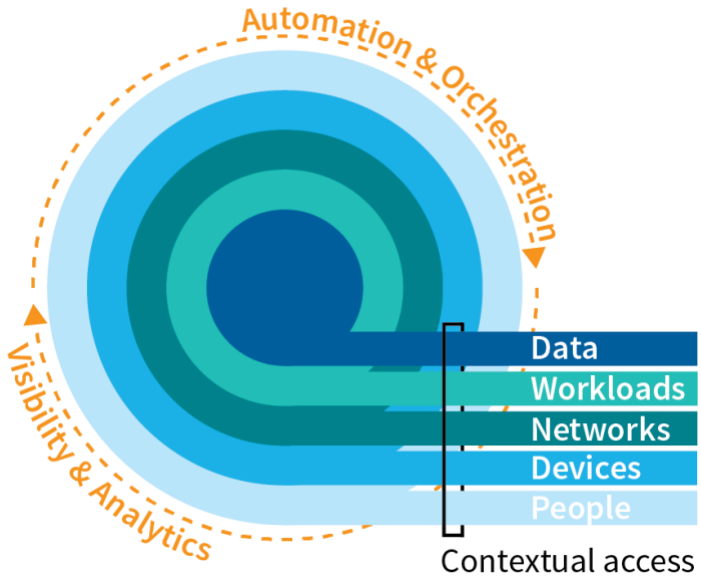


Published: 10 December 2018: ID: G00377791

While the industry models differ, they each share the same general principles:

- Trust traffic inside the perimeter no more than external traffic
- Authenticate, validate, and verify every request for resource access; authorize only on need to know
- Inspect, log, and continuously monitor all traffic throughout sessions for anomalous behavior
- Authorize access based on risk profile (adaptive authorization)

FIGURE 12: ZERO TRUST



In the development of services supporting Zero Trust, the DON will use the following *Zero Trust Design Requirements*:

1. Fully automate user provisioning and monitoring
2. Use multifactor authentication
3. Eliminate automatic trust for users or machines
4. Build context aware access
5. Encrypt all traffic at rest and in transit
6. Instrument for comprehensive, full-stack visibility
7. Separate protections for network, applications, and data
8. Perform Continual Adaptive Risk and Threat Assessment
9. Augment detection and response using automated AI, ML, & orchestration
10. Continuously discover, monitor, assess and prioritize risk and trust
11. Use micro segmentation to create granular perimeter security zones
12. Match security zone policies around context; do not treat all data and workloads the same
13. Put continuous risk visibility, decisions and ownership into business units and product owners

2.4 Agile & DevSecOps Technical Focus Area

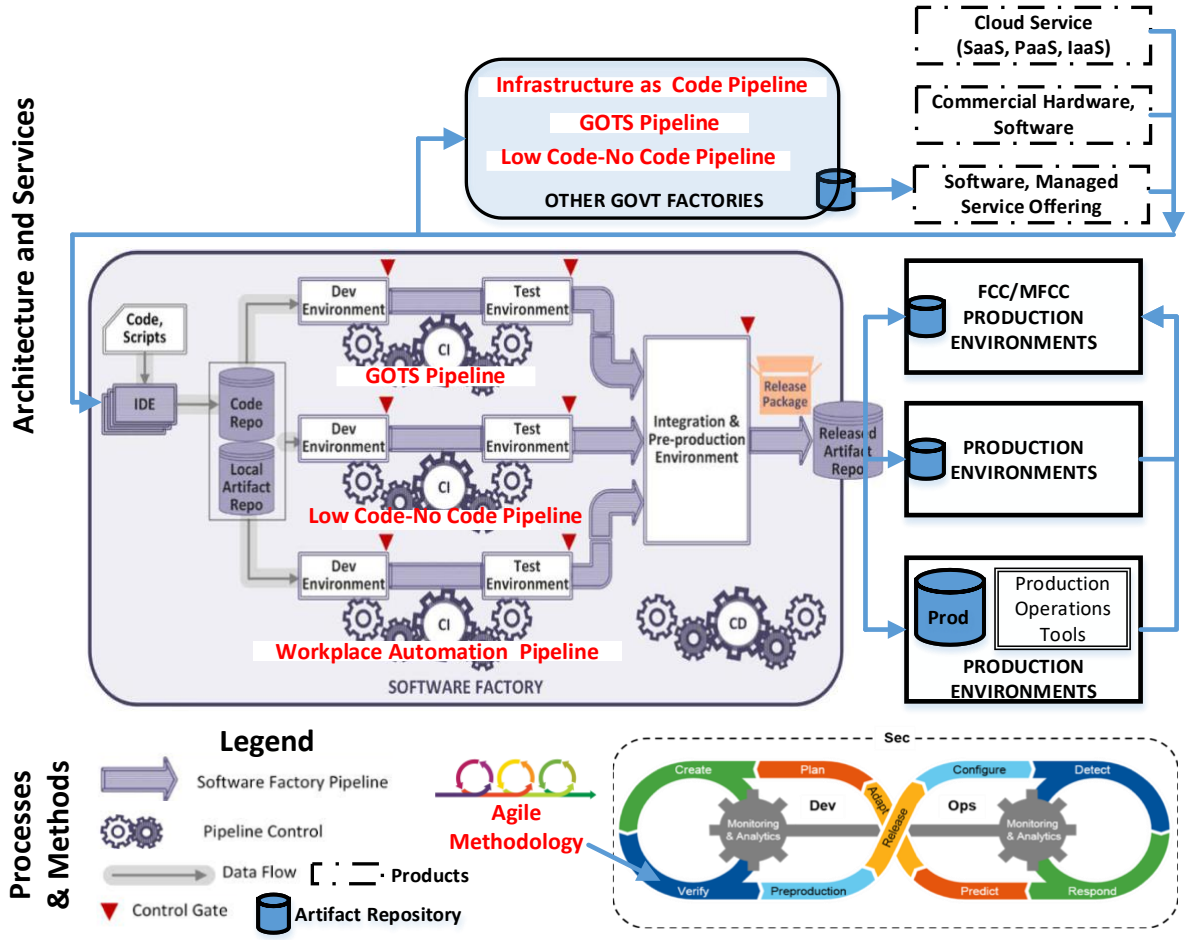
Agile & DevSecOps Technical Focus Area scope includes three intertwined subjects: Agile development; Development & Operations (DevOps); and Development, Security, and Operations (DevSecOps).

"Agile software development is more than frameworks such as Scrum, Extreme Programming or Feature-Driven Development (FDD).Agile software development is more than practices such as pair programming, test-driven development, stand-ups, planning sessions and sprints. Agile software development is an umbrella term for a set of frameworks and practices based on the values and principles expressed in the Manifesto for Agile Software Development and the twelve Principles behind it." (https://www.agilealliance.org/agile101/).

"DevOps is the practice of operations and development engineers participating together in the entire service lifecycle, from design through the development process to production support. DevOps is also characterized by operations staff making use many of the same techniques as developers for their systems work." (https://theagileadmin.com/what-is-devops/). DevSecOps is an extension of the DevOps that also includes security design and operations in the entire service lifecycle.

There is currently a low level of maturity for Agile and DevSecOps across the DON. Despite several anecdotal examples of progress[1], few of the development efforts in the DON satisfy the criteria identified in Detecting Agile BS[2]. Some notable progress in the Development area of DevOps exists in the DON and some inclusion of security and automated testing for some development and deployment models has been made, but progress has been slow to make its way to fully integrated Development and Operations. Of all the technical focus areas, Agile and DevSecOps hold the promise of having the most dramatic impact on the DON and mission success through responsive IT delivery and increased security through automation. However, Agile and DevSecOps requires as much organizational and cultural change as it does technology change, complicating adoption.

FIGURE 13: AGILE & DEVSECOPS TO-BE



Agile & DevSecOps Design Requirements

1. Rent before buy, buy before build: only develop custom capabilities unique to the DON mission
2. Deliver and consume DevSecOps capabilities as self-service provisioned Digital Enterprise Services
3. Create pipelines and continuous A&A for each capability development and delivery model
4. Consolidate factories, tool networks, and enable differentiation and local control of pipelines
5. Align with DOD Enterprise DevSecOps Reference Design[3] for containerized and GOTS use cases
6. Enable Fleet Cyber Command visibility and control of continuous delivery and target environments by using the same tools for development and operations
7. Institute cultural change to enable Agile development, not Agile BS[2]
8. Create cross-factory interoperability and promote re-usability

9. Integrate feedback loops and enable self-service access to production data and baselines in Dev
10. Automate all aspects including functional testing
11. Treat all items as Infrastructure as Code

References
[1] Compile-to-Combat in 24 Hours Implementation Standard V1.
[2] DIB Guide: Detecting Agile BS; Oct 9, 2018
[3] DOD Enterprise DevSecOps Reference Design V1.0; August 12, 2019

2.5 Microsoft 365 (M365) Technical Focus Area

Microsoft 365 (M365) Technical Focus Area includes all services necessary for all users to access M365 services from anywhere on any device and network. M365 Services implement a Zero Trust strategy to ensure ubiquitous and secure access to Office and collaboration tools.
The M365 implementation effort followed a legacy project management approach through Operation Flank Speed. The project demonstrated great success but requires realignment of capabilities to meet Modern Service Delivery. The project must be dissected into the associated services, services mapped to their appropriate service groups, and delivered as products by the Portfolio Managers of those service groups. Realignment of the capabilities from M365 to the Digital Enterprise Services portfolios prevents duplication of services, enables organizational flexibility, and supports the Zero Trust journey. Identity, endpoint security, application security and digital rights management services in Azure are used for M365 services today, but those capabilities are available for consumption independently of M365. Realignment of services to the portfolios requires intentional intervention by the Portfolio Managers and project leaders to increase parity between the private sector and the DON.

M365 Technical Focus Area Design Requirements

1. Transition service delivery of M365 capabilities to the Portfolio Managers
2. Make services and data equally accessible across all devices
3. Provide multiple connectivity methods supporting managed and unmanaged devices
4. Verify device, network, user, and authentication method combination to provide appropriate access
5. Develop user centric services designed for ubiquitous access
6. Provide seamless data synchronization across all devices
7. Improve parity between user experience on different devices and between on-network and off-network capabilities
8. Implement Apply Zero Trust design requirements

2.6 Integrated Navy Operations Command & Control System Technical Focus Area

Integrated Navy Operations Command and Control System (INOCCS) is a secure operations framework delivered as a collection of services operating as a manager of managers enabling significantly automated and modern command and control of naval cyberspace operations. The INOCCS framework enables the operational community to provision, operate, protect, and defend the cyberspace elements and capabilities supporting the warfighter mission. INOCCS is a security and management-related function relying on people, processes, and services. The INOCCS framework represents the most critical cross-service-group relationship within the entire IT portfolio because it must rely on services from multiple service groups to satisfy the CONOPS. The visibility aspects of INOCCS are primarily enabled through security and configuration monitoring tools as part of Management & Security services. These monitoring tools then trigger manager of manager services in the Management & Security service group that either directly provide an automated response or indirectly make the changes through services from other service groups such as Identity Services or Development & Deployment services. This coordinated interaction is enabled through loosely coupled API integration of services as required by Modern Service Delivery, supporting the execution of the INOCCS framework through a combination of people, functions, processes, and loosely coupled replaceable services. Figures 14, 15, and 16 are copied from the latest INOCCS documentation, which does not graphically represent specific USMC elements for C2, so the graphics should be considered representational (rather than complete and exhaustive) of C2 with multiple networks, locations, and domains. The important item to note is that the individual services comprising the INOCCS system of systems are designed as loosely coupled services that operate across multiple network and security boundaries. As a result, Successful C2 does not have a dependency on active directory or network singularity.

FIGURE 14: INTEGRATED NAVAL OPERATIONS COMMAND AND CONTROL FRAMEWORK

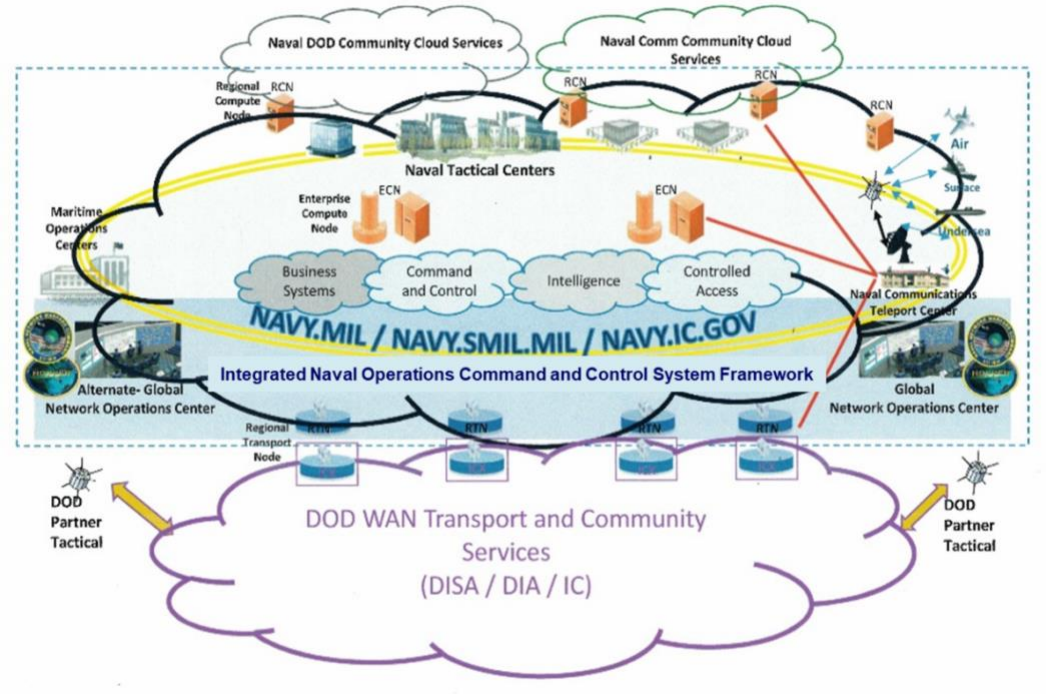
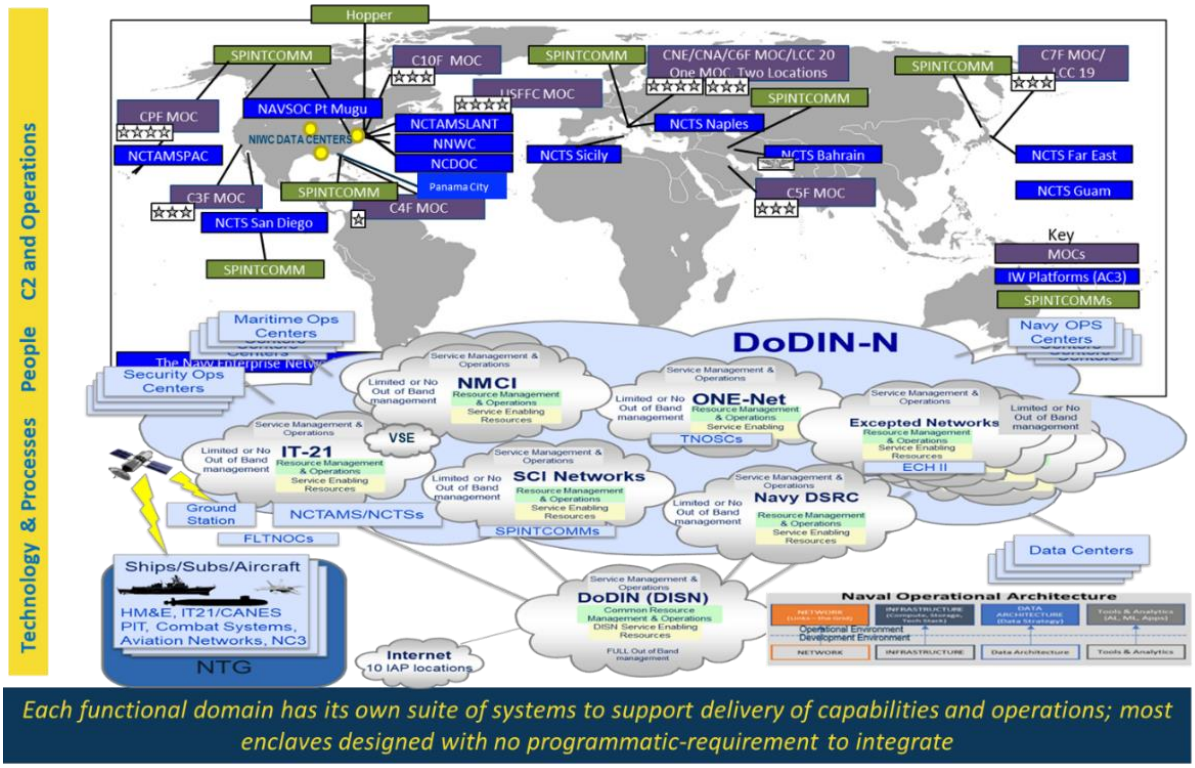
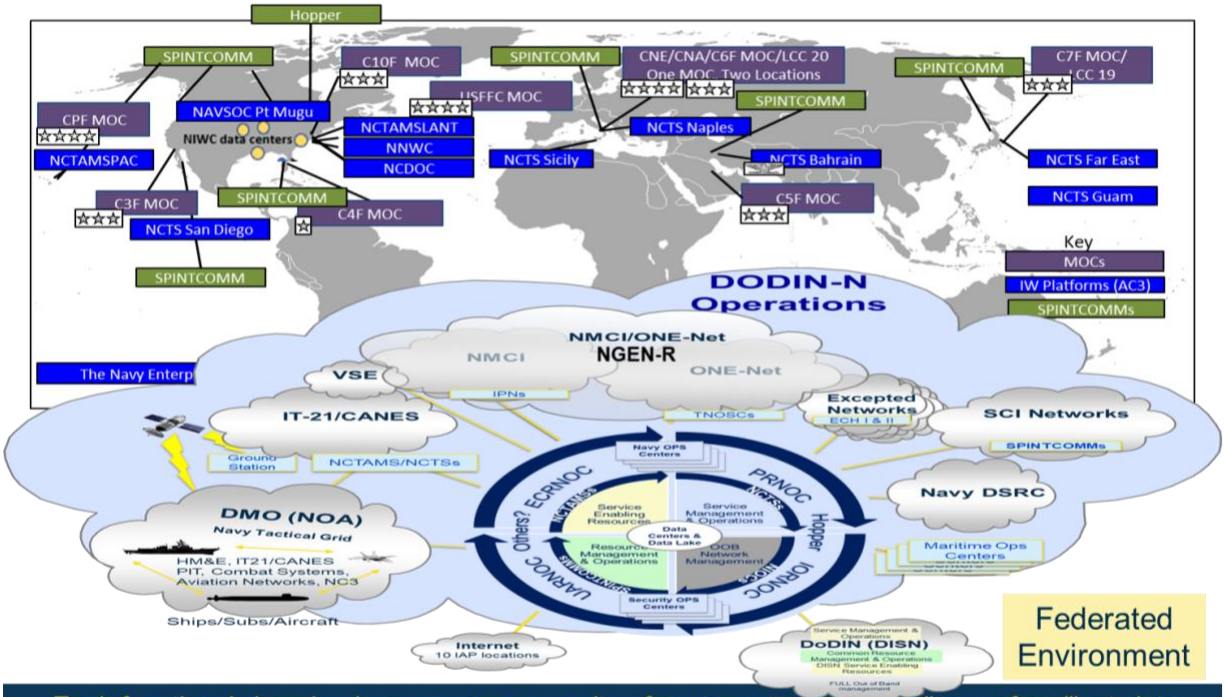


FIGURE 15: AS-IS NAVAL CYBERSPACE OPERATIONAL COMPLEXITY



Each functional domain has its own suite of systems to support delivery of capabilities and operations; most enclaves designed with no programmatic-requirement to integrate

FIGURE 16: FUTURE UNIFIED OPERATIONS ENVIRONMENT



Each functional domain shares a common suite of systems to support delivery of resilient data capabilities and operations; enclaves designed with programmatic-requirement to integrate

INOCCS Design Requirements

1. Deliver enterprise services from multiple Services Groups to support the Integrated Navy Operations Command and Control System Initial Target Architecture[1]
2. Enable Fleet Cyber Command visibility and control of continuous delivery and target environments by using the same tools for development and operations
3. Adopt Zero Trust principles as the basis for security and user experience
4. Apply Zero Trust design requirements
5. Design for reusability of capabilities for consumption outside of FLTCYBERCOM
6. Ruthlessly automate everything
7. 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
8. Design for resiliency

References
[1] DON Integrated Navy Operations Command and Control System Initial Target Architecture.

2.7 Naval Digital Platform (NDP) Technical Focus Area

Naval Digital Platform is an approach to realize part of the Modern Service Delivery (MSD) vision. Six Epics shape NDP, and they reach across the PEO Digital service groups. Portfolio managers deliver the capabilities from their respective service groups to enable NDP. NDPs Six Epics include (1) MS365 Acceleration Flank Speed, (2) Core Infrastructure & WAN Transport, (3) Naval Identity Services, (4) Hosted Application Services Migration to Hybrid Cloud, (5) Endpoint Image Redesign, and (6) Commercial Solutions for Classified Program. The specifics of the NDP epics are a constant work in progress as portfolios deliver capabilities using SAFe Agile principles."

NDP is NOT: A project, a program, a portfolio, a formal reference architecture, an enterprise service, or a comprehensive view of all Digital Enterprise Services. A single acquisition strategy should not enable NDP, and the epic capabilities will be decomposed and delivered by the portfolios.

Naval Digital Platform Design Requirements

1. Deliver all NDP capabilities through the portfolios
2. Buy instead of build commodity technologies (As-a-Service preferred)
3. Leverage an Application Program Interface (API) economy
4. Enforce Representational State Transfer (RESTful) architecture standards – focused on caching and layering for disconnected uses
5. Enable the National Institute of Standards and Technology (NIST) attributes of cloud for both on and off-premise consumers
6. Adopt Zero Trust principles as the basis for security and user experience

7. Enable self-service provisioning in development and production environments
8. Design for mobility
9. Ruthlessly automate everything
10. Support Integrated Navy Operations Command and Control System (INOCCS) Requirements

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. This is primarily because the new design concepts are drastically different from the past. DON will provide regular updates of this document, as information is refined. Updates are expected on an annual frequency. Drastic changes to the concepts represented in this document are not expected. Please check with the DON Chief Architect frequently for the latest version.

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