US Navy

PEO Digital

OTP ORE

Business Case Analysis

PWS 3.3.32.6

17 April 2023

2 TWELVE Solutions
241 18th Street, Suite 203
Arlington, VA 22202

www.2TWELVEsolutions.com

Table of Contents

Table of Figures

1.0 Executive Summary

The vision of the Department of the Navy (DON) for “digital transformation and optimized program alignment across Navy and Marine Corps enterprise IT capabilities” necessitates the Navy’s infrastructure to be able to keep up with rapidly changing environments, modern services and IT software, security, cost effectiveness, and end user efficiency. The DON is right to understand that this vision requires the resources and expertise to build an enterprise-class digital platform and implement a modern service delivery model with end user centricity in mind which are captured via World Class Alignment Metrics (WAM). To accomplish this, the Navy needs the right tool to integrate and orchestrate all of its networks, data, software, and configurations, etc. while providing independence, ownership, and control of the same so that it can operate at the cutting edge of a rapidly changing, cloud native, hybrid, multi-cloud environment with security, mobility, efficiency, and cost effectiveness. Without such a tool, it will be very challenging for the Navy to achieve the technological capabilities necessary for modern service delivery.

Orchestrating Business processes and ensuring Governance of the IT life cycle to support a Government Owned Contractor Operated network is also critical in ensuring the DON achieves optimal services to the end user but also maintains control of managing these services in a Government Ownership role. With over two decades of outsourcing coupled with the technology paradigm shift, the complexity of Government oversight in managing multiple services from Azure, Amazon, Google Cloud, etc. requires technology that enables security and control over Navy’s distributed multi-cloud environment.

This Business Case Analysis (BCA) evaluates how the Orchestrated Repository for Enterprise (ORE) is the only singular comprehensive solution available and consumable to deliver WAM outcomes that will enable the Navy to meet its objectives in comparison with the insufficiency of current capabilities of Navy infrastructure and that of other alternatives. The Orchestrated Repository for Enterprise will enable the collection and retrieval of data via indexing to enable translating data into outcomes. Furthermore, the ORE enables alignment to the Department of Navy’s goal of providing ubiquitous access to data to the end user through methods of federation and open standard API architectures in a distributed multi-cloud environment so Navy can securely control their environment and maintain operational resiliency.

Figure 1 below illustrates how the ORE provides a central ecosystem that will enable the Navy to bring its IT solutions which are currently siloed, distributed, and owned by outside vendors into alignment with their objectives of government independence, ownership, and control while maintaining security and performance in the modern IT environment. At the current state, the Government lacks sufficient visibility and control of these disjointed IT systems, making effective oversight and governance nearly impossible to execute its Government-Owned model. The ORE uses API driven architecture and automation to orchestrate distributed data, configurations, applications, and other IT systems in any cloud environment from one central location. The result is critical visibility, access control, archival capability, automated processes, and enhanced system performance, without which the Navy cannot meet its objectives for command and control, modern service delivery, and tracking World-class Aligned Metrics (WAM).

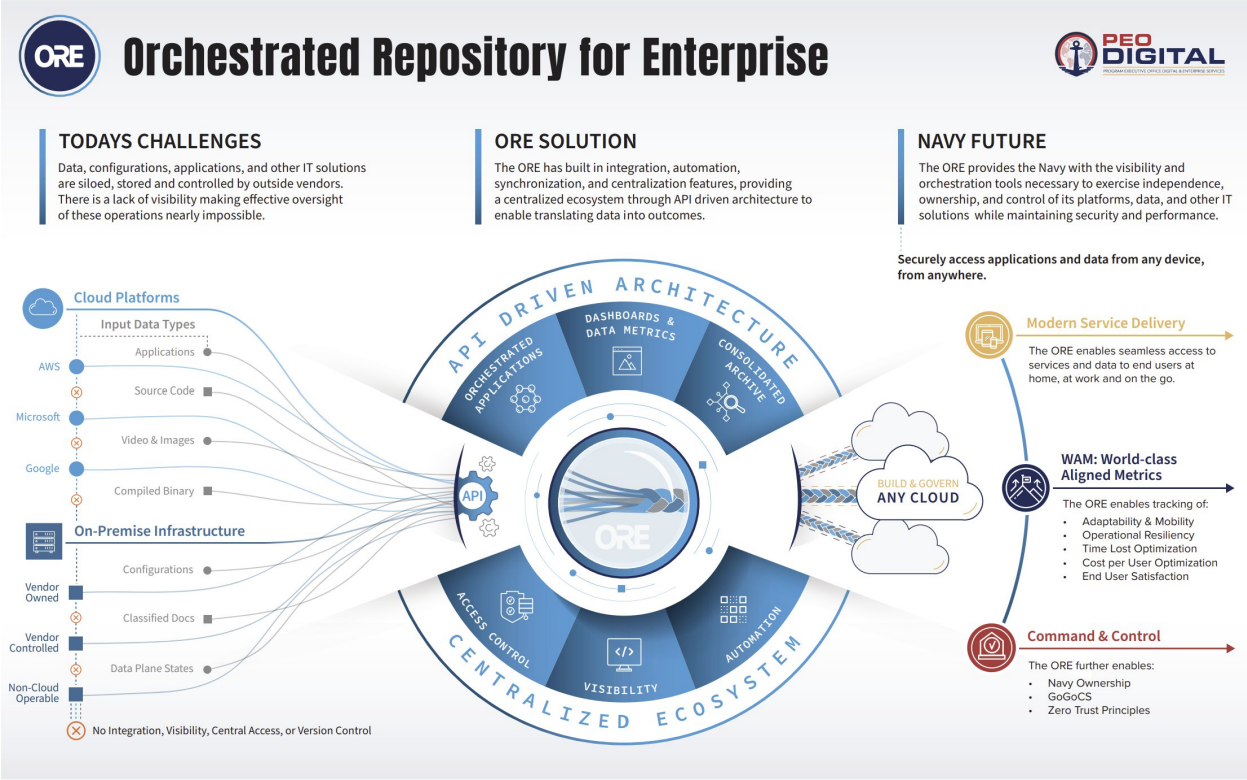

Figure 1: ORE Ecosystem

2.0 Overview

2.1 Purpose

This Business Case Analysis (BCA) analyzes the landscape of the Navy's network and other IT solutions and whether they align with the capabilities necessary for the Navy to effectively achieve its objective of digital transformation and modernization of IT capabilities. It evaluates how the Navy's current solutions are not sufficient to meet its objective and how the Orchestrated Repository for Enterprise (ORE) meets the requirements to deliver these necessary capabilities.

2.2 Problem Statement

The Navy's current network is comprised of a large amount of data and IT solutions that are operating in silos, many of which are owned and controlled by outside vendors. The Navy operates in environments hosted on cloud platforms that are controlled by the major cloud providers (Azure, AWS, Google Cloud Platform (GCP)) or on legacy on-premise infrastructure that cannot operate in a cloud native environment. Data, configurations, applications, and other IT solutions are stored and controlled by outside vendors, and there is a lack of visibility into the software and services owned and operated by vendors making effective oversight of those operations nearly impossible. Therefore, the Navy is unable to independently manage its own storage, security, processes, and configurations, which puts Navy IT solutions in a position of being unable to communicate with each other efficiently or securely, being unable to optimize

poorly performing applications, being unable to integrate and automate technical, operational, or business processes, and being unable to sufficiently control access to information. This lack of visibility also hinders the ability for the Navy to obtain operational resiliency because of lack of control over the services and not being able to reconstitute services in case of outages. Navy IT solutions have become locked in to disadvantageous cost structures and do not have the ability to store, archive, retrieve, and share data necessary for provisioning, sustaining, or decommissioning systems as a part of the plan for digital transformation. These are the technology Outcome Driven Metrics that feed and enable the WAM.

Therefore, the Navy needs a solution that will provide oversight and enable good governance over the entire process of transforming and modernizing its legacy network. To truly achieve its objective of digital transformation, this solution must provide several critical features including;

- A central repository for storing, retrieving, sharing critical documents or artifacts used in designing, building, maintaining, and optimizing the system.
- Quick and secure access to all the different applications used in this process.
- The ability for governing authorities to consolidate and control access to information logically, physically, or temporally.
- Efficient management and communication between the many vendors, contractors, service members, and other stakeholders involved in the process.
- The ability to aggregate information pertaining to feedback, measurement, and evaluation for use in optimization.

Without such features, the Navy will continue having operational difficulties including:

- Critical Knowledge and information is lost, misplaced, or difficult to find and use
- Applications are cumbersome to use and monitor,
- Third parties have diverging standards and sets of data making collaboration more challenging
- There is no way to fully ascertain a detailed and comprehensive perspective on the flaws present in the system.
- Poor performance of software, networks, and other IT solutions
- Barriers to communication,
- Structural fragmentation
- Compromised security and sustainability of software, networks, and other IT solutions

Figure 2 below illustrates the difference between the current state of Navy IT solutions and the transformed state after implementing the ORE. Currently, the Navy's IT solutions (NMCI) are isolated in silos, and therefore they exhibit all the problems just described because they lack the centralization, access, control, communication, automation, and other data/software management capabilities that the ORE provides. And while certain solutions may have more or less robust features which may address certain specific programmatic needs of the Navy, the underlying issues that the ORE resolves are left unaddressed (i.e. different solutions may have a larger or smaller "dot" in the picture, but the dots still cannot communicate, integrate, or coordinate with each other). On the other hand, the transformed state uses the ORE as the central location for IT solutions to be integrated and synchronized with each other and through which Navy leadership would access, control, manage, and coordinate important processes. It would become the single source of truth in which important data, configurations, source code, etc. would be securely archived, retrieved, and shared with appropriate Navy

stakeholders for efficient use and reuse of software utilized in design, maintenance, sustainment, and optimization of Navy IT solutions.

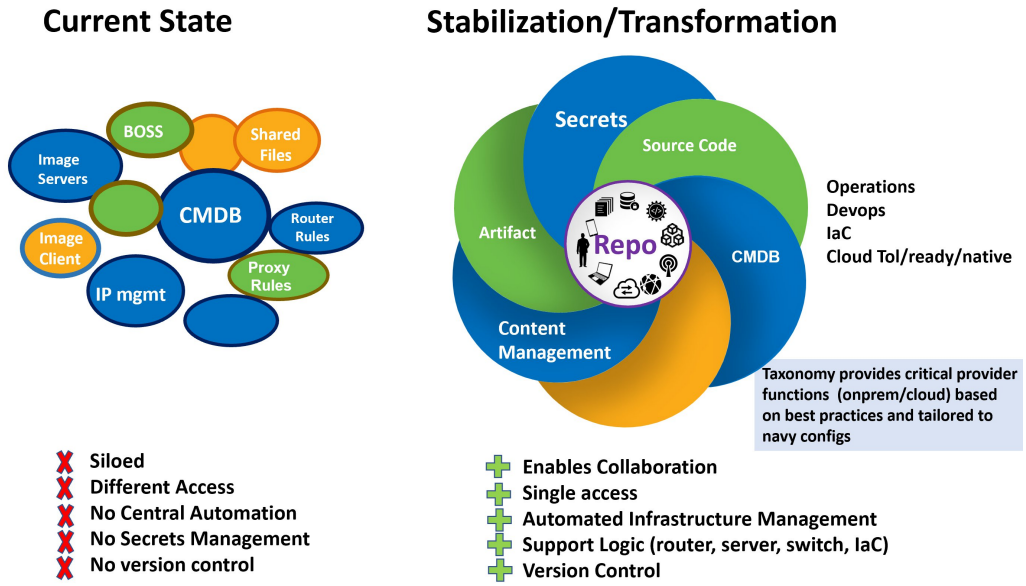

Figure 2: Current State to Transformation State

2.3 Background and Context

The technology design underlying the ORE was originally developed for the US commercial financial sector, but the prototype proved that its capabilities are critical to the Navy's effort to update and modernize its IT systems as a part of its digital transformation strategy, Acquisition re-compete independence, and WAM outcomes. In order to transform its legacy platform into a modern, cloud native platform and to retain ownership and control of its data storage and IT processes, the Navy needs a solution that can integrate and orchestrate its data, applications, configurations, and processes that are currently hosted in different legacy or cloud environments and driven via API's. It needs a tool that is optimized for a hybrid, multi-cloud, cloud native environment that provides visibility, independence, adaptability, and resilience necessary to put in place the right governance structures to provision, operationalize, sustain, and optimize solutions.

The Navy currently lacks any tools that are capable of providing the necessary features to implement the governance structures or the IT solutions for modernization. The ORE has built in integration, automation, synchronization, and centralization features that can orchestrate data and applications from any network or storage location. The Navy's current vendors either lack the expertise to build and implement a modern cloud native network, or they lack the economic incentive to market such a tool because it conflicts with their business model - i.e. their model is naturally opposed to facilitating the Government having control of a solution driven by Government Specification to be consumed on Government owned platforms. This causes vendors to have roadblocks to updating software and solutions, to preventing vendor lock, and to sharing information such as code, configurations, and other intellectual property that should be government owned yet is not under the government's control. This has created an atmosphere of stagnation and rigidity leading to risks and inefficiencies in cost, security, and

performance. Now the Navy has been left with solutions that are incapable of integrating with each other, sharing information with each other, or scaling up to meet the demands of the Navy's mission. Therefore, the ORE was created to resolve these deficiencies and help move the Navy back into the forefront of the into modern cloud native zero trust IT landscape.

2.4 Project Initiative Description and Requirement

This BCA was developed as a part of PEO-Digital Enterprise Services procuring implementation and productionizing services in support of the Operationalizing Modern Enterprise Capabilities as a Service model that was prototyped under, IWRP 19-LANT-0012. The proposed solution provides for seamless provisioning and integration of IT solutions which allows for the unification and orchestration of any data platform portal. The secure orchestration of these solutions will allow the Navy to obtain visibility into hybrid multi-cloud environments to support DON's operational ability to control and maneuver critical environments and support the DON's zero trust digital transformation.

2.5 Scope

The PEO Digital Orchestrated Repository for the Enterprise (ORE) provides a highly secure multimedia Content Management System that enables archival and extremely robust index-able search capabilities – with the ability to index, organize, search and retrieve video, audio, and various 3D images (i.e. CAD and text documents). It also provides a data orchestration system gateway to the modern data repository ecosystem.

The ORE provides the ability to orchestrate any cloud native, API driven IT solutions, including systems of software applications, repositories, databases, as well as cloud networks. The ORE has been deployed on multi-cloud environments and can be deployed on any cloud environment. ORE has been configured to be deployed as configuration as code so it can be re-deployed into any environment Navy chooses as long as foundational IaaS/PaaS core enabling services are available. In addition, the ORE is a cloud native zero trust application designed with zero trust concepts built into it. So, while it does not implement zero trust architecture for the enterprise, it enables and facilitates implementation for the enterprise for all of its zero trust IT solutions.

Figure 3 below illustrates how the ORE takes data and systems that are siloed and unorganized, and provides a centralized ecosystem through API driven architecture that integrates distributed storage and networks on multiple hybrid cloud platforms, synchronizes software and configurations, and orchestrates all the applications and repositories from one central location. This is what enables the efficient management of IT solutions, the IT solution life cycle process, and the alignment of governance and management roles to those solutions. Such a centralized ecosystem is critical to give the Navy the visibility and orchestration tools necessary to exercise independence, ownership, and control of its platforms, data, and other IT solutions while maintaining optimal security and performance in a modern, distributed, cloud native, API driven environment.

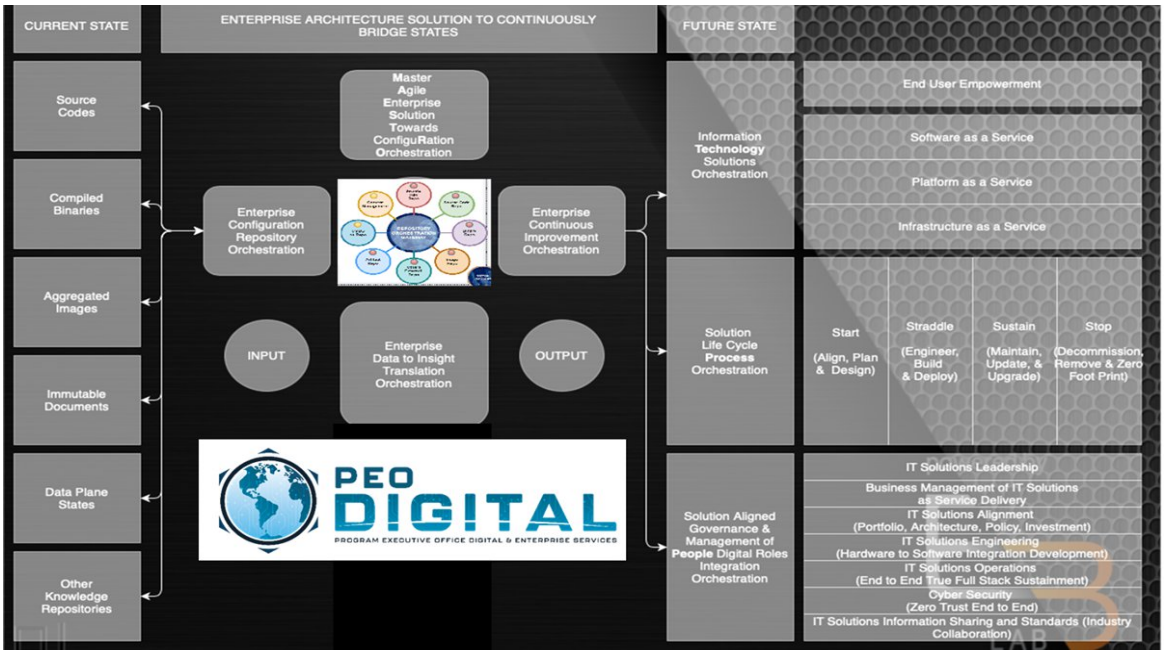

Figure 3: Transformation Target State

2.6 Assumptions and Constraints

The ORE is designed to enable the Enterprise to accelerate cloud native zero trust technology adoption across the Navy. It addresses the host of requirements necessary to ensure the viability of a cloud native environment and API driven architecture. The ORE aims to increase the Navy's accessibility to cloud native architecture based on the following principles:

- Ease-of-use
- Integration of Development and Maintenance
- Increased and Continuous Security
- Streamlining of configuration

The ORE facilitates the implementation of the tenets of zero trust framework through the following principles:

- Standardize data according to open standards
- API driven architecture
- Software driven architecture
- Facilitate machine to machine token automation
- Secure segregation and portability of data
- Seamless integration of IdAM services
- Seamless integration of monitoring services
- Facilitate abstraction of network security to (OSI model) layer 3 and above
- Orchestrate separate verification of user, device, network, application, and data

The following assumptions concern the system, software and its use. These include issues related software or hardware, operating systems, end-user characteristics, and possible and/or probable changes in functionality. The following are assumptions made related to the ORE infrastructure (the list is not exhaustive):

- PEO Digital is the system owner

- The ORE assumes that the Navy has a cloud native platform to host this system, as this modern system requires open standard APIs and compute, networking, and storage fabrics.
- API connections will be configured with varying lead times
- Operations of the ORE are shared responsibility between NEN operators and Navy user organizations
- An ICAM solution with CAC authentication capabilities will be available for the ORE to integrate with as the upstream identity provider.

The following limitations or constraints have a significant impact on the system's design (the list is not exhaustive):

- Security Requirements – Development team will have to continuously design, monitor, and configure the system to adhere to Navy security standards
- Scheduling – Scheduling factors outside of the ORE systems' direct control will impact the platform's development, deployment, and acceptance (i.e. procurement of hosts or existing hosts with storage, compute, and network fabrics, ATO process, etc.)
- Cross-Department Integration – Platform's success is dependent on engaging and integrating with a host of stakeholders across the Navy and ensuring the repository enables secure access to different enclaves.
- Funding – Future maintenance and development will need to be addressed with some type of charge back. The cost savings of provisioning a server image with the appropriate network dependencies to be leveraged in the form of scripts enables cost avoidance which is achieved by minimizing the duplication of provisioning, accreditation etc.
- Standards Compliance – Navy Standards will impact the platform's development, deployment, and operations.

3.0 Major Benefits

Implementing the ORE will provide many features that directly impact the governance, operations, and user performance of the Navy's systems, as well as facilitating digital transformation and modernization. Some of the major benefits are as follows:

Visibility - The orchestration of applications and resources through API integrations enables the automated extraction and aggregation of relevant data from distributed storage and networks to be customized and visually presented in centralized dashboards. The centralized access to each application also enables effective and efficient monitoring, reviewing, and coordinating of all enterprise systems and processes. This visibility is critical for good governance of all Navy operations and aligns to the pillars of zero trust.

Data Metrics **-** Data metrics are a specific form of visibility that can be shown on the dashboards to enhance understanding and control of operations and can be customized according to the needs of the user or group.

Access Control - User role management, user permission controls, management of passwords, and management of access to features and software is all centralized so that those in the correct leadership or management positions have visibility into who is using the system, what they have access to, and what they are doing in the system. They also have the ability to tailor that access to the specific needs of the users and revoke the access when necessary.

Automation - The ORE's features facilitate extensive automation, which is essential for a modern DevSecOps process, for the effective testing and optimization of IT solutions, and for

the effective management of a modern cloud native platform. If the API integration is the “glue” that holds everything together, then automation is the gears that keep everything working smoothly.

Zero Trust Security - The ORE is a cloud native zero trust application designed with zero trust concepts built into it such as API and software driven architecture, Standardization of data and configurations according to open standards, integrations of IdAM and monitoring services, multi-tenant design, secure segregation and portability of data, automated machine secrets management, abstraction of network security to OSI model layer 3 and above, and orchestration of separate verification of user, device, network application, and data. So while it does not implement zero trust architecture for the enterprise, it enables and facilitates implementation for the enterprise for all of its zero trust IT solutions.

Continuity of Operations - The ORE leverages modern API protocols to store configurations in a highly available repository so that systems can be rebuilt to the correct configuration. The ability to efficiently provision, manage and sustain, and decommission resources through centralized extraction, storage, and retrievability of data and configurations optimizes and ensures the continuity of operations at all levels including infrastructure, storage, platform, and software.

Institutional Life Cycle - Similar to the Continuity of Operations, the ability to synchronize and orchestrate data and IT solutions throughout every stage of the IT product life cycle fosters a healthy institutional life cycle for technology and systems that not only includes the design, build, and sustainment phases, but also facilitates continuous optimization and mobility.

Knowledge Management - The combination of features such as the searchability and availability of archived files from distributed or siloed storage, centralized access control, visibility into operations and the institutional life cycle, and automated integration of IT solutions enables the government to control all of its important data throughout the life cycle and archive it in a retrievable format regardless of whether it is from a government operated or vendor operated solution.

Risk Management – All of the previously stated benefits enhance risk management. Whether it is business risk, operational or technical risk, security risk, automated centralization, integration, access control, visibility, etc. are key to managing risk. Some specific examples include:

- Vendor Lock - The ORE mitigates the risk of vendor lock through the API driven integration that enables it to orchestrate the movement of data from any platform or software.
- Cost Overruns - The ORE mitigates the risk of cost overruns through the visibility of data metrics and resource monitoring enabling near real time view of how resources are distributed.
- Roadblocks to Project Execution - The ORE limits roadblocks to project execution by resolving problems with storing, accessing, and sharing information securely.
- Technical Debt/Product Failures - The ORE mitigates the risk of technical debt and product failures by standardizing and storing configurations and source code, as well as providing visibility, control, and agility to the DevSecOps pipeline, so systems can be provisioned and patched quickly and repeatedly as a part of a true CI/CD pipeline with rapid deployment.

- End of Life Support - The ORE mitigates the risk of noncompliance, data and information loss, data retrieval and transfer costs, and time lost when decommissioning software through its central archival, retrieval, visibility, and automated synchronization capability.
- Security Risk - The ORE mitigates security risks through its multi-tenant Zero Trust design that enables secure segregation, aggregation, storage, transfer, and sharing of data with granular access control and integration with Identity services.

World-class Aligned Metrics (WAM) **–**The ORE's centralization, integration, orchestration, automation, and controls are necessary to achieve WAM outcomes.

- Adaptability/Mobility - The visibility and control provided by the ORE, as well as the automation and synchronization features that seamlessly connect distributed storage, networks, and platforms, combined with integrated Agile development and project management principles, makes the ORE a vital part of the Navy's effort to provide mobile, adaptable systems.
- Operational Resiliency - The ORE's ability to synchronize and manage distributed network, compute, and storage resources in hybrid, multi-cloud, cloud native environments, as well as the ability to ingest data from legacy environments in a format that is archivable and retrievable, combined with the security and efficiency that comes with automated work flows that are visible and traceable, make the it essential to the operational resiliency the Navy is trying to achieve.
- Time Lost Optimization **-** When it comes to provisioning, development, allocation, accreditation, authorization, monitoring, updating, and replacing distributed physical, virtual, and human resources, as well as operating the many (currently siloed) IT solutions the Navy needs to utilize to achieve its objective, the centralization, integration, synchronization, and orchestration of storage, applications, configurations, and network resources makes every process and work flow related to these operations and systems more efficient. This eliminates much of the time that is wasted with uncoordinated systems that do not share information.
- Cost per User Optimization - all the same features mentioned in "Time lost Optimization" previously also apply here. Costs per user are optimized when all resources are coordinated, monitored, and updated efficiently. Optimized costs are the natural result of the visibility, adaptability and mobility, and time efficiencies that the ORE provides.
- Customer/End User Satisfaction **-** The visibility, efficiency, mobility, control, and automation of the ORE naturally increase user satisfaction since the IT solutions the users must use on a daily basis, along with the systems, process, and work flows related to them, are made more efficient, more resilient, more manageable, and more aligned with their objectives.

4.0 Shared Services/Multi-Tenancy for Modern Service Delivery

To truly achieve the visibility, control, collaboration, and rapid deployment necessary for modern service delivery, the Navy must have an underlying technical approach that enables a shared services management and cost model. This is a critical capability and it requires the flexibility to provision and manage software solutions for multiple agencies, or tenants, which have varying needs and objectives, without recreating or redesigning the same solutions. A

shared services approach enables you to use the same network, platform, or database configurations for these multiple tenants, while still allowing for separation and isolation of sensitive data and permissions between tenants when desired. This multi-tenant capability is built in to the ORE. The integration and orchestration features of the ORE not only enable centralization and aggregation of data, but they also enable control over the appropriate segregation and storage of data among different systems. Therefore, leadership at multiple levels will be able to both restrict sensitive data to the appropriate users and share data with appropriate users within their respective organizations and across multiple organizations, all while using the same unified infrastructure, platform, and network, and without being subject to roadblocks from vendor-locked solutions. This shared services approach has implications for business and cost decision making in many areas.

The graphics to the right illustrate, first, the unique situation the Navy is in regarding IT solutions, and second, the unique and critical value the multi-tenant/shared services capability of the ORE provides. Figure 4 illustrates that while a normal enterprise has to manage many of the issues discussed in this BCA concerning modern service delivery, the Navy's situation compounds the problems because it is essentially an enterprise of enterprises. Each agency within the Navy has the size, resources, and operational needs and capabilities of an entire enterprise, yet these enterprises must also be managed and coordinated effectively in alignment with the Navy's overall objectives.

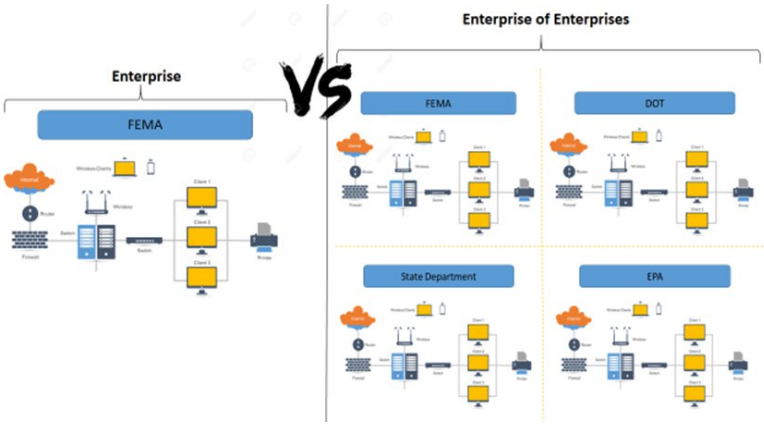

Figure 4: Enterprise of Enterprises

Figure 5 illustrates how the ORE's API driven architecture and automated orchestration enable the Navy to effectively manage all of their agencies even in its unique situation. When using the ORE, the Navy would be able to store its data in any cloud environment it chooses, and then extract the data it chooses to use for visibility and collaboration, and restrict the data it chooses to maintain security and compliance. Considering configurations and software for networks and applications, this means that it's no longer necessary reduplicate efforts to design and build a new system or solution every time a different agency or department needs a new capability. The Navy will be able to utilize the same solutions and configurations across multiple agencies and maintain centralized control

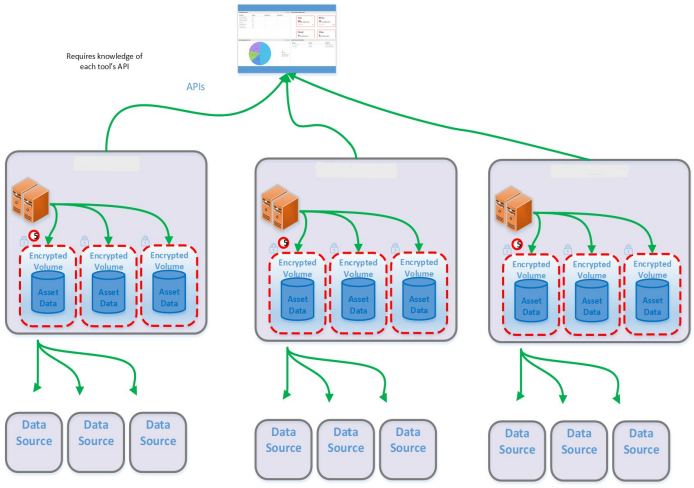

Figure 5: Multi-Tenant Database Design

while still retaining the ability to use separate instances of the same software when necessary. The same is true for storage, namely that the Navy will be able to use the same database with separate and secure data storage for different agencies, or use separate databases for different agencies with the ability to extract, share, and aggregate data when necessary.

4.1 Critical for Modern Service Delivery

The potential cost and operational benefits of this shared services design are extremely significant. Some examples of how this applies to modern service delivery include:

Storage - Storage can be shared and structured according to what is most advantageous for the Navy, optimizing the use of on premise and other cloud storage according the most cost-effective and efficient allocation, without danger of creating data silos or becoming locked in to cost prohibitive cloud storage agreements that become unsustainable as the amount of data increases.

Software - The capability to centrally manage software solutions enables the Navy to consolidate its software requirements across agencies and projects and utilize the economies of scale inherent to such a combined negotiating position to procure advantageous pricing and contract terms for all of its solutions. This is in addition to the operational efficiencies created by decreasing the amount of overhead necessary to securely orchestrate the software solutions from a central repository.

Provisioning through standardized configurations - Whether it is provisioning a new software instance, a new hardware device, or a new network edge or co location, a centralized repository of standard configurations for IT solutions enables the Navy to rapidly deploy IT services for any user or any command center instead of unintentionally proliferating similar but disconnected solutions, logins, administrative tasks, and vendor contracts and adding unnecessary costs and time lost to the process. It ensures that the Navy will have a unified approach to managing solutions that fulfill DON or DoD-wide requirements and be able to scale solutions as necessary to meet the needs of Naval operations.

Data as Asset - The way of the future for any modern enterprise, especially when it comes to modern service delivery, is adopting a mindset of using data as an asset. An enterprise the size of the DON has and will continue to generate massive amounts of data. Currently, much of this data is difficult to use or completely unusable because of the way it’s stored or the lack of IT solutions available to retrieve, organize, and manage it. Also, there is much data being managed and controlled by outside vendors that should be owned by the government, but does not function that way in reality. The ORE is designed to enable and facilitate the data as asset mindset by providing the central ecosystem in a cloud native, hybrid, multi-cloud environment to manage data from on premise storage, hyperscalers, and edge networks in one place. The data is made available and useful through standard configurations and secure synchronization of IT solutions that can aggregate it, segregate it, and format it appropriately for use in visibility metrics, workflows, DevSecOps pipelines, and any other decision-making construct. This capability also enables the DON to fully own and control all of its data and no longer be dependent on outside vendors.

Collaboration - Whether it is a modern CI/CD pipeline, the DevSecOps pipeline, project management, contract management, or any other execution of work, collaboration is key to modern service delivery. You must have a streamlined process in which business, operations, security, and other users are able to interact through a combination of user input and automation in order to provide rapid and ubiquitous availability of services, updates, and fixes that continually sustain and optimize the system. Without the centralized control, automation, and visibility provided by the ORE, the necessary level of collaboration would not be possible. The time, operational, and financial cost of creating manual work-arounds for communication and work flows, of managing the proliferation of accounts on single tenant applications, of intellectual property being stolen because of unsecure practices employed in an attempt to increase efficiency, and of constantly repurchasing software or services from vendors to redo work that has been lost or outsourced would inhibit you from ever reaching anything close to modern delivery of services.

Monitoring and Analysis - Modern service delivery is characterized by certain metrics that relate to user experience such as high availability, efficient performance, quick response time, low latency, and low error rate. For a modern service delivery framework to successfully deliver this experience, the enterprise must have the ability to monitor the services being provided, to analyze the feedback from what is monitored, and give alerts when problems are detected so they can be resolved quickly. Without the centralized, orchestrated, multi-tenant design provided by the ORE, the Navy could not possibly monitor and analyze services on a large scale and could not ensure that these characteristics are being achieved. It may be able to achieve something close to modern performance on certain specific applications, but the moment they are required to interact with or utilize other storage, software, vendors, or network resources, the roadblocks to modern service delivery cause the whole system to break down and your performance will denigrate to that of the least efficient aspect of the system.

End to End control - Successful modern service delivery also requires end to end control of processes in order to properly integrate business and IT functions. The collaboration, efficiency, monitoring, and automation, etc. previously mentioned would be severely inhibited without having ownership of, and visibility into, every aspect of IT processes utilized for delivery of services. Whether it is the multiple development environments in the CI/CD pipeline, the infrastructure, platform, and software services on your cloud native network, or access to sensitive information used in contracting and project management, if you do not have ownership and visibility of each component of the process the operational and financial costs become prohibitive at scale due to dependence on the diverging expertise, policies, and business models controlled by multiple outside vendors.

Cloud as a Service Model - Successfully implementing a modern service delivery framework would enable the Navy to provide the ORE as a service to all the Navy customer commands. This would multiply the benefits of efficiency and cost as the digital assets for the entire Navy could be integrated, orchestrated, and automated according to centralized processes and policies. This visibility and control would give leadership the tools necessary to govern and manage all the IT solutions with the speed and performance necessary to lead in the modern warfare environment.

4.2 Critical for System Optimization and Cost Savings

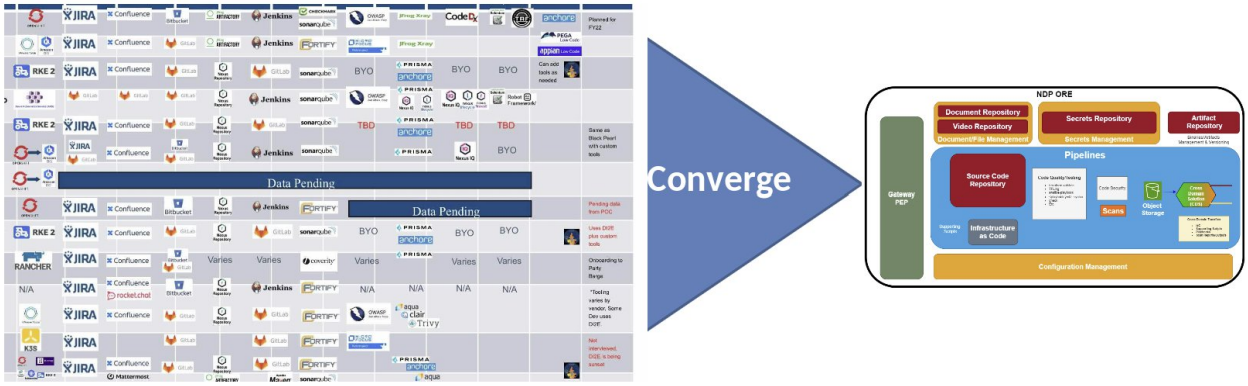

Figure 6: Convergence of Solutions through Shared Services

Figure 6 above illustrates the benefits of the multi-tenant, shared services concept more from a very practical end user perspective. The number of instances of the same software being deployed and managed across Navy organizations shows that there is no sufficient way to mitigate the inefficiencies and costs of the proliferation of software instances and software licenses across agencies in the Navy.

The current state of the proliferation of these IT solutions comes with several significant costs or potential costs including:

- If information needs to be shared with a user from a certain software, right now the information would need to either be downloaded and sent over an unsecure medium, or a new license needs to be purchased to give the user access no matter how rarely the user actually needs to use the software.
- If a different group or agency wishes to use a software that the Navy already uses, but wants to keep their data segregated for security reasons, a new instance of the software needs to be created with new infrastructure, deployment, management, and licensing costs. Then, if information needs to be shared, you are still in the same situation of needing to proliferate licenses.
- In addition, there is still no way for Navy leadership to have visibility into the use or cost of software or to view and share important files without further proliferation of licenses, instances, and management costs.
- And in any case, there is no way for the Navy leadership to automate consolidated data metrics from the software it uses regardless of how the systems are structured because they are not designed for that purpose.
- There is also no way for the Navy to effectively decommission applications because there is no central archive for data, nor is there any efficient way to retrieve, transfer, and store data. Every step in this process (retrieval, transfer, and storage) adds costs of time and money as it will be necessary to pay vendors to perform each task, potentially incurring exorbitant costs. This is especially significant in order to mitigate the risk of noncompliance with regulatory archival requirements for data storage, outputs for application decommissioning, refactorization, etc.

The shared services/multi-tenant design of ORE eliminates the unnecessary proliferation of every one of these costs:

- The ORE provides secure sharing capability across agencies through its built-in archival, searchable, retrievable storage that eliminates the need to proliferate user licenses in order to share information. The only licenses necessary to buy would be for those who use the IT solution extensively. Other sharing can be done securely through the ORE.
- The ORE's multi-tenant design provides secure segmentation of data at the database level, so information is only shared and accessed according to user defined restrictions. Therefore, the Navy will be able to limit the instances of software necessary to deploy. Also, and more importantly, when the Navy does need to deploy separate instances of software, it can use the same infrastructure and configurations for every instance, instead of proliferating new infrastructure, design, and deployment costs for each instance of software. It also consolidates management operations to one central place, thereby significantly reducing ongoing management costs.
- The ORE can orchestrate IT solutions from all Navy agencies in one location, from which leadership can access information with no added licensing or management costs.
- The ORE can be configured to extract data from orchestrated applications across the entire Navy and present the data in central dashboard visuals to enhance governance and decision making. This is currently not achievable without implementing the ORE.
- The ORE's archival, retrieval, and synchronization capabilities, in addition to the multi-tenant segmentation, provide a central location for ongoing storage of sensitive data and an efficient repository for transferring regulated data storage without being dependent on outside vendors, thereby significantly reducing costs of decommissioning applications.

5.0 Use Case Analysis

The following use cases illustrate features in the ORE that meet the capability needs of the Navy as discussed in this BCA.

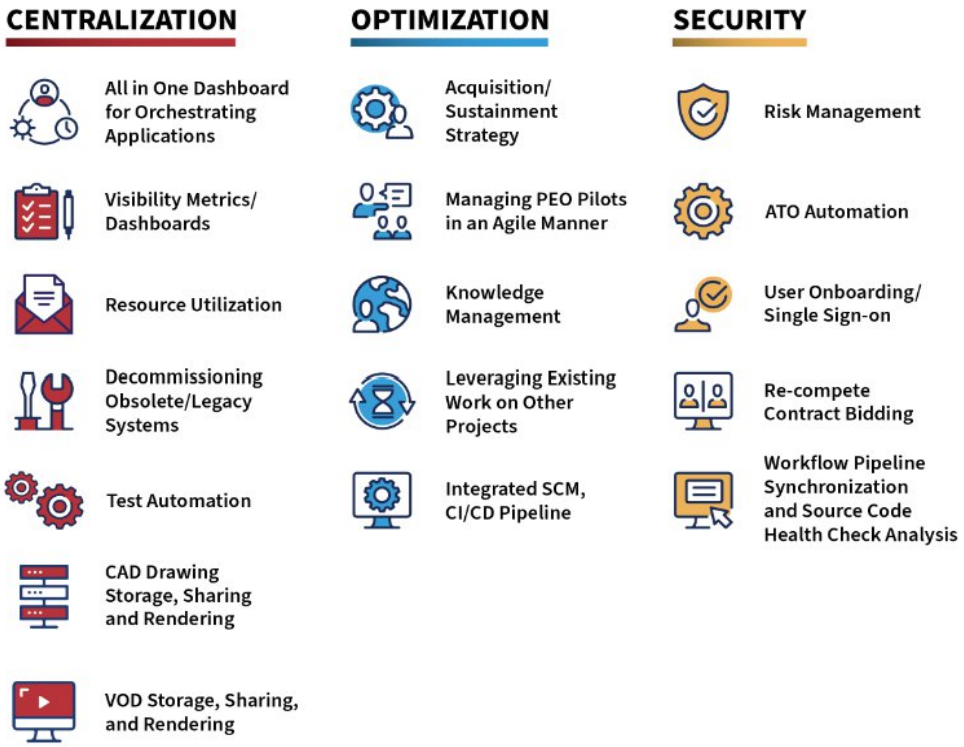

Figure 7: Example Use Cases

5.1 Re-compete Contract Bidding

Overview: In order to design, build, sustain, and optimize Navy networks, infrastructure, hardware, licenses, and other IT assets, PEO Digital needs an optimized process for contract bidding so these assets can be acquired quickly, securely, and efficiently. The optimal process would include the ability to distribute sensitive data to vendors while keeping control over who is able to access and view the information, how long they are able to access and view the information, and while restricting those with access from stealing the information. This requires coherent visibility of who has access and when, control over what capabilities the end user has to manipulate the data, and the ability to revoke access without leaving data behind.

Status Quo: Currently, there is no way to share secure or sensitive information with vendors during the contract bidding process without using a solution that lacks any mechanism to enforce any level of security and control. Either sensitive information must be downloaded to a local drive and sent through a non-secure method like email, or it must be uploaded to a physical hard drive and the drive sent to the vendor. In either case, once the information is sent, all control, visibility, and security is forfeited, no matter what regulations are placed on the data.

ORE Feature/Process Alignment: This use case is an example of the capability of secure and controlled temporary sharing of files (documents, videos, and configurations) in the ORE. The ORE enables the user to control access to files by sharing information with outside users through a temporary and secure viewing room, in which the outside user is able to view the file but not download, print, or otherwise manipulate it. The granted access can be set for a defined period of time and can be revoked at any time. By using this feature, instead of sending out proprietary information through an non-secure channel, like email or a hard drive, and having no control over what the vendor does with the information, the Navy will be able to control who has access and when, to have visibility into who has access, and to mitigate the risk of giving out otherwise proprietary information.

So for re-compete contracts, instead of sending hard drives or some other non-secure solution, you can just give vendors access to the temporary viewing room for any information they need and thereby exert control over the access and manipulation of that data throughout the entire process.

5.2 All in One Dashboard for Orchestrating Applications

Overview: In order for the Navy to operate efficiently and govern effectively in a software driven, cloud native working environment, end users need to have quick, simple, yet secure access to all the applications that are relevant to them. This enables the users to maximize efficiency since they are not spending unreasonable amounts of time searching for the correct software applications, troubleshooting accreditation issues, and managing passwords that are easily forgotten. The optimal solution would include a centralized dashboard where all relevant applications can be accessed from one location, the ability to customize that dashboard so that only the applications relevant to each particular user are available both for efficiency and security, and an automated ID management system that integrates the source of authority and the IDP with the relevant applications as well as providing single sign on capability.

Status Quo: Currently, there may be certain solutions that offer consolidated dashboard and single sign on capability, but only on products that belong to one particular vendor. For example, Microsoft 365 offers consolidated and single sign on access to the Microsoft suite of

products. However, the DON does not have any solution that offers this capability for products from different vendors. Practically, that means that there is no way to integrate software products outside of the Microsoft Suite or Google Suite, nor can these integrate with each other. These major vendors do not offer this capability because it is against their business model. Therefore, whatever capabilities are available from a certain vendor, the problem of siloed and unorchestrated applications, data, access, and processes remains.

ORE Feature/Process Alignment: The Orchestrated Applications feature in the ORE is a central dashboard through which an end user is able to access all of their relevant applications from one location. The ORE leverages open standards to enable the government to integrate government selected open standards applications into the ORE system. The applications can be customized and tailored to the user through an automated process utilizing preset attributes, or manually by an Admin user. This can also utilize automated configurations for the IDP to integrate the applications with the single sign on feature so that the applications can be accessed securely and quickly from within the ORE.

5.3 Managing PEO Pilots in an Agile Manner

Overview: As the Navy seeks digital transformation and any degree of optimization of its IT resources, developing and implementing new software, processes, or other IT solutions will be a natural and necessary part of its institutional and IT life cycle. In order to do this in a modern environment, it is essential to integrate Agile principles into this cycle in relation to both IT development and business development. And for Agile methodology to have any impact, the enterprise must have software and infrastructure solutions that support a scalable Agile approach. Concerning its current pilots, as well as future pilots of software and other IT solutions as a part of a regular approach to modern institutional life cycle management, the DON needs a technology foundation that will support a scalable agile methodology.

Status Quo: The Navy currently leverages ServiceNow to provide Agile tools. However, this solution presently lacks the flexibility to integrate with other tools that may be necessary for software development, or project efficiency. Even though service now leverages an API development architecture, not all their API services are exposed for consumption. In addition, the pricing model of consuming their API's will depend on the service they expose for consumption.

ORE Feature/Process Alignment: The ORE includes a turnkey Agile management application that can be used for software development, project management – anything that lends itself to Agile management principles. There is a Kan ban board, Gantt chart, issues list (of features, bugs, tasks, deliverables), wiki, etc. which all help to prioritize tasks, personnel, and resources. This application is designed with the ORE's integration principles in mind and therefore already possesses the flexibility to integrate with any other API driven tool as necessary.

So, for the PEO Pilots, this integrated Agile capability in the ORE gives the COO visibility and control over the entire process from beginning to end, and it provides an instrument that enables portfolio managers to have visibility into all the resources they have allocated for these projects so they can be cost effective and improve performance.

5.4 Integrated SCM, CI/CD Pipeline

Overview: As a part of modern service delivery model, a functioning CI/CD pipeline is the goal and requires a source code management solution that scales to the size of the organization and has the ability to integrate and control all the different development operations associated with the various projects that need to be managed. Therefore, while version control is built in to SCM tools, in an organization the size of the DON, governing over the DevSecOps process well enough to provide CI/CD necessitates a solution that enables visibility and collaboration between business, development, operations, and security teams throughout the entire process so that the development, automation, monitoring, testing, and decision making stakeholders and tools are coordinated and orchestrated to achieve modern service delivery.

Status Quo: The DON currently does not have a system to coordinate or provide visibility into the many different segmented development activities being performed across its many offices and commands and by vendors. It does not have an integrated source code management solution, nor does it have centralized or coordinated automation, monitoring, or testing.

ORE Feature/Process Alignment: By synchronizing and integrating applications like the Source Code repository, the Artifact repository, the Secrets repository, and the Agile Management repository, the ORE enables the CI/CD pipeline, making the deployment of software, fixes/patches, or other resources truly a part of a modern service delivery framework. It provides a central location to store source code and images, as well as providing the coordinated automation and monitoring necessary for stakeholders in the DevSecOps team to access and manage resources efficiently, and gives leadership visibility into the entire process. For example, the automated synchronizing of the SCM repository provides the visibility necessary for project leads to ensure the code for software is healthy and secure.

This type of integration and orchestration is necessary if you're going to have rapid deployment of software and mitigate the risks of code failure or performance degradation and the loss of time and cost that go along with it.

5.5 Workflow Pipeline Synchronization and Source Code Health Check Analysis

Overview: In each project, for the DevSecOps workflow to support a Ci/CD, modern service delivery framework, there must be an efficient method for appropriate stakeholders to review source code for software being utilized and deployed by critical IT solutions in order to remove vulnerabilities and optimize performance. The Navy needs a solution that uses automation and machine to machine secrets to enable both government stakeholders and contractors to review code without giving unnecessary access to sensitive data by sharing account access to the applications. In this way, source code health checks can be done by multiple stakeholders as a part of a robust DevSecOps workflow without jeopardizing security.

Status Quo: The DON currently does not have the ability to integrate, synchronize, or analyze applications and data in this way, and therefore it does not have ability to use automation to facilitate source code health checks as a part of a robust DevSecOps workflow.

ORE Feature/Process Alignment: One of the ways the ORE enables modern service delivery is through the automated synchronization of different applications so that relevant data can be pulled from, stored, and utilized for analysis, quality control, monitoring, decision-making, reporting, or any operation in which visibility and control are critical. This capability is critical to a robust DevSecOps workflow that provides CI/CD, and it enables the secure data sharing that facilitates source code health checks. By using the ORE, instead of giving out passwords and making new accounts for everyone who needs to look into data for a certain solution, the ORE can use automation and the management of machine to machine secrets to pull in relevant data for testing, and then make only that data available to others through the secure sharing features in the ORE. This information can be shared with as many vendors or stakeholders as needed to receive the desired input. These capabilities could be leveraged to analyze data from any application with a consumable API.

A good example of this functionality already being put to use is that 2Twelve Solutions was asked to analyze the SANDE/Netdevops repository because there was a lack of visibility into the work. The ORE was used to pull in the source code data and analyze the repository in order to give recommendations concerning the gaps and vulnerabilities that were present.

5.6 Decommissioning Obsolete/Legacy Systems

Overview: The question of how and where to store network data for decommissioned applications is critical for the resolution of the technology adoption life cycle, for institutional knowledge management, and for compliance with government regulations. The DON needs a solution that will enable it to securely extract, store, transfer, and retrieve data from obsolete systems before they are decommissioned in order to prevent data from being lost, from being retained in a format that cannot be used, or from giving up control of the data to an outside vendor.

Status Quo: The DON does not currently have a solution that enables government to own, control, and continue to utilize data from decommissioned systems. Due to the DON's lack of any system to archive and securely share information with the proper access control, many tools have not been divested and continued licenses are paid to maintain these services.

ORE Feature/Process Alignment: The archival, retrieval, and sharing features of the ORE's document/file repository along with the ORE's ability to synchronize applications through API integration, provides a central location for securely extracting, storing, and archiving data from legacy or obsolete systems, and it is able to do it with data from any cloud platform. It is then retrievable if the data still needs to be used. This mitigates the risk of vendor lock and eliminates the need to incur unnecessary ongoing licensing costs for systems that are no longer needed, or to incur exorbitant costs to pay vendors to deliver data that the government should already own and manage. In addition to cost savings, this promotes an environment of optimization instead of stagnation, improving mobility and resilience.

5.7 Test Automation

Overview: A modern service delivery model is not possible without automated testing. To have a modern CI/CD pipeline or to manage a cloud native platform, it's essential to be able to do test validation, to replicate test results, to do analysis of vulnerabilities, etc. when developing software. Every part of the CI/CD process needs to be reviewed, tested, and updated, and the

results need to be able to be stored in an accessible location. In order to do testing sufficient for modern service delivery, especially at the scale of the DON, the vast majority of this testing must be automated. The DON needs a solution that can facilitate extensive test automation.

Status Quo: The DON does not currently have a solution that enables extensive test automation. Almost all of the testing is currently done manually, and many types of tests that are industry standard for software development and required for rapid delivery of services are not currently performed as a part of any standard development process in the Navy (i.e. security testing, unit testing, SAST testing, etc.).

ORE Feature/Process Alignment: The ORE enables and facilitates extensive automation through the secrets management, source code management, and artifact repositories, all orchestrated in the central ecosystem through API integration and secure distributed hybrid cloud storage. It consolidates and gives centralized visibility into the pipeline workflow, enabling the customer to create and store test scripts and configurations so that they can be standardized and reused, to leverage automated machine to machine secrets, and to securely govern and control the software development process of the entire organization in a unified manner with operational resiliency.

5.8 Visibility Metrics/Dashboards

Overview: One of the most important requirements for good governance and control over enterprise systems is visibility into the operations, processes, decision making workflows, and user behavior within the system. In order to have this type of visibility, it is necessary to have tools that are able to aggregate data in a location that is accessible to the appropriate leaders and to synthesize that data into information that is easily understood and relevant to accomplishing the mission and objectives of the enterprise. This visibility is especially important considering the DON structure, being an enterprise of enterprises. And this structure also necessitates a tool that has multi-tenant capability so that sensitive information can be segregated where necessary among the different commands, and centralized where necessary for overall leadership, without jeopardizing security at each level of governance. In this way, managers at every level will have metrics relevant to them, without having access to those that are not.

Status Quo: The DON currently does not have any tool that provides data metrics on an enterprise scale, nor does it have any centralized location for accessing metrics. Any monitoring and analysis of data must be done at the level of individual applications or specific functions of the network, but none of the services are synchronized, there is no aggregation of data from multiple sources, and there is no visibility or control of data from the perspective of top level leadership.

ORE Feature/Process Alignment: One of the critical functions of the ORE is to provide a central ecosystem where applications and other IT systems can be synchronized, integrated, and orchestrated through API architecture and automation. Add to this the multi-tenant design and the ability to extract, store, and retrieve data from distributed systems and configure it into visuals on customized dashboards, the ORE enables the customer to have the visibility necessary to govern a robust enterprise system. Dashboards and Metrics can be customized according to the needs of the users and securely segregated or centralized according to the needs of the enterprise. Therefore, the appropriate users can be provided relevant information necessary for governance and management decision making, enabling leadership to truly exert control over its data and technology environment whether it is managing government owned and operated

systems or overseeing contractor operated systems that must integrate with the ORE. Without this ability to view and analyze data metrics, it will be extremely difficult to effectively manage and control the many projects and processes the DON must manage.

5.9 Onboarding/Single Sign-on

Overview: The user onboarding process for the DON is one of many processes that can be optimized as part of the goal of digital transformation and modern service delivery. However, for an enterprise of this size, it is difficult to completely overhaul such a system without substantial costs in terms of time, risk, and finances. The DON needs a solution that leverages the current process while still enabling the desired modernization of the approach.

Status Quo: The DON currently has an onboarding process that utilizes single sign-on providers. However, it does not have a solution that optimizes the onboarding process in coordination with an enterprise-wide modernization effort that uses automation and integration to synchronize the configurations and software for user provisioning across the Navy from a central location and provisions resources for new users efficiently and remotely.

ORE Feature/Process Alignment: The ORE is designed for a hybrid, multi-cloud, cloud native environment with the ability to integrate and synchronize applications from legacy and modern networks. Because of this ability to integrate applications, the ORE can leverage the existing onboarding process with the ORE's capabilities. It can use the government's authoritative source of truth for ID management but use automation to populate customized features like user roles, user permissions, and relevant applications and dashboard metrics, and provide single sign-on access to relevant applications using whatever single sign-on software is most effective for the Navy.

5.10 CAD Drawing Storage, Sharing, Rendering

Overview: A specific application of the need for secure centrally accessible distributed storage and sharing of files is the engineering team's CAD drawings. There are potentially very large amounts of data in these files that need to be stored in a format that is easily retrievable and viewable, but is also secure so that sensitive files are not accessed by the wrong users. Engineers need to be able to share sensitive files with the appropriate users while still keeping control of how those files are accessed and used so that the files are not able to be replicated and shared or manipulated insecurely or by the wrong users.

Status Quo: The Navy does not currently have a solution that offers secure and controlled storage, rendering, and sharing of CAD files.

ORE Feature/Process Alignment: Since the ORE is able to store, retrieve, and view CAD files, this use case is another specific example of the secure and controlled sharing of files (documents, videos, and configurations) available in the ORE. Engineers have a secure, central location to store CAD files so they can be accessed by those who need them. Access to these files can be customized and restricted according to user permissions in the ORE, and temporary viewing access can be given to outside users according to ORE's secure temporary sharing capability. The ORE enables the user to control access to files by sharing information with outside users through a temporary and secure viewing room, in which the outside user is able to view the file but not download, print, or otherwise manipulate it. The granted access can be set for a defined period of time and can be revoked at any time. Therefore, engineers can securely share files while

controlling who has access and when, having visibility into who has access, and mitigating the risk of misuse of sensitive information.

5.11 VOD Storage, Sharing, Rendering

Overview: Another specific application of the need for secure centrally accessible distributed storage and sharing of files concerns video files. Video files are generally very large and therefore generate a tremendous amount of data ranging from conference videos to UAV feeds. There is a critical need for this data to be stored in a format that is easily retrievable and that also has Video on Demand (VOD) functionality so that the videos can be viewed, but is also secure so that sensitive files are not accessed by the wrong users. Appropriate personnel need to be able to share sensitive files with the appropriate users while still keeping control of how those files are accessed and used so that the files are not able to be replicated and shared or manipulated insecurely or by the wrong users.

Status Quo: The Navy does not currently have a solution that offers secure and controlled storage, streaming, and sharing of video files with VOD functionality in a multi-cloud capacity.

ORE Feature/Process Alignment: Since the ORE is able to store, retrieve, and view video files and dynamically render them with VOD functionality, this use case is another specific example of the secure and controlled sharing of files (documents, videos, and configurations) available in the ORE. Navy personnel have a secure, central location to store video files so they can be accessed and rendered by those who need them. Access to these video files can be customized and restricted according to user permissions in the ORE, and temporary viewing access can be given to outside users according to ORE's secure temporary sharing capability. The ORE enables the user to control access to files by sharing information with outside users through a temporary and secure viewing room, in which the outside user is able to view and render the video the file but not download, print, or otherwise manipulate it. The granted access can be set for a defined period of time and can be revoked at any time. Therefore, Navy personnel can securely share files while controlling who has access and when, having visibility into who has access, and mitigating the risk of misuse of sensitive information.

5.12 Leveraging Existing Work on Other Projects

Overview: In a large enterprise environment like the DON with many large projects to manage that each have IT components, there are often many areas in which expensive and time consuming work has been completed for one project that could also relate to other projects. It would make sense for the Navy to reuse such work on all the projects for which it is relevant in order to limit costs, limit time spent, limit redundancy, limit errors, and to optimize the work as more and more competent teams use it, test it, perfect it, and share that information.

Status Quo: Currently, The DON does not have a comprehensive system that facilitates this level of sharing and collaboration. There are often circumstances in which software, configurations, data, or other work are unused because their is a lack of visibility that hinders collaboration and thus simply a lack of knowledge of the potential opportunities that exist, or a project is ended and the data is not stored in a usable format, or work is done by contractors who hold and manage all the data themselves and then charge the government to transfer and

configure that data on a government system even though the data should already be government owned.

ORE Feature/Process Alignment: This case once again highlights the foundational design of the ORE that enables orchestration and integration of software, configurations, and other data from distributed applications on any cloud-native platform through API integration in a central ecosystem that provides visibility and control to enable good governance. The increased visibility and collaboration, combined with the ability to securely and efficiently transfer, store, and retrieve data, will enable the DON to reuse and optimize processes and software and decrease or eliminate costs associated with redundancy and vendor lock in. Some specific examples of how this could be applied include transitioning work from one vendor to another, assigning access to multiple vendors for current work in order to advance code, reusing analysis/synchronization from one repository for other projects, enabling peer review from multiple sources to improve code over time.

5.13 Acquisition/Sustainment Strategy

Overview: The enterprise level scope of the DON acquisition and sustainment of digital assets such as hardware, software, contracted services, or IT personnel resources requires secure and efficient processes and tools to make sure data and configurations are able to be captured, stored, communicated, and shared with different stakeholders involved in every stage of the IT solutions delivery and sustainment process. This requires the capability of orchestrating applications on a broad scale so that configurations can be centrally managed and utilized across Navy commands and projects, and the efficient integration of new resources with the current system to take advantage of automation, economies of scale, central visibility that make the acquisition and sustainment of these resources cost effective and secure while providing a level of performance that enables a modern service environment.

Status Quo: The DON currently has robust systems for acquisition and sustainment at many levels. The problem is that the systems are not all coordinated, and they are not in line with a modern services model. The lack of orchestration, centralization, and automation (i.e. control plane) of the overall process leads to an inability to share information to coordinate resources, a lack of visibility from a leadership perspective that hinders decision-making, and a lack of efficiency in resource allocation, maintenance, and optimization.

ORE Feature/Process Alignment: The ORE's ability to capture data and configurations and facilitate secure, centralized, and efficient sharing of information across any cloud native platform provides the visibility and coordination necessary for the DON to achieve modernization of its acquisition and sustainment strategy. And it does this without completely overhauling the current systems, but facilitates their optimization for operation in a modern services environment. Some specific examples of areas where this would apply include: having sufficient visibility into relevant repositories to know when to transition for logistics purposes or for maintaining code, managing the entire software supply chain through an integrated supply chain management repository, maintaining oversight and security of the process through the synchronization and analysis of IT solutions, and extracting and storing data from weapons platforms that can be used for maintenance and improvement of those systems on a large scale and efficient archiving of that data for use in optimizing new systems. Additionally, the ORE can enable cost analysis and financial forecasting based off of the configuration templates which

provide accurate resource allocation and return on investment including cloud consumption and projects.

5.14 Resource Utilization

Overview: As an enterprise, the DON has a large amount of software resources utilized for many purposes across various projects and operational roles. These software solutions require licenses or other implementation or deployment costs that must be managed well in order to optimize costs. Therefore, a tool is needed to provide visibility into metrics on how the software is being used, such as the total number of licenses available for each solution, how those licenses are being used and who is using them, and how those licenses align to mission objectives and organizational roles. The ideal solution would facilitate the efficient use of these licenses while at the same time facilitating collaboration between different users and groups in the enterprise without proliferation of licenses through the ability to share relevant and/or significant information securely with non-licensed personnel.

Status Quo: The DON currently does not have any tool that provides high level visibility into enterprise system resource utilization. The lack of visibility and the lack of secure sharing capability leads to misalignment of resources and causes software licenses to be inefficiently proliferated and leads to under or over utilization of resources.

ORE Feature/Process Alignment: The ORE provides the central ecosystem and the orchestration through which metrics concerning resource usage, availability, and alignment can be aggregated and made available to decision-makers. For example, while the ORE is NOT a software license management system, it has the ability to provide input to a software license management system. The ORE contains key elements needed by resource management such as code and Infrastructure as Code (IaC). These provide inputs that, when combined with other endpoint and server data provided by discovery agents that send back information on what software is actually running, along with license contract data, will enable the enterprise to accurately determine if they are over or under resourced. Additionally, the ORE enables cost analysis and financial forecasting based off of the configuration templates which provide accurate resource allocation and return on investment including cloud consumption and projects.

This centralized availability will not only impact the alignment of resources within entities in the DON but also across entities such that economies of scale can be leveraged to manage resources for multiple agencies, teams, and projects at one time with confidence that resources purchased more directly aligns with the actual necessary usage by relevant stakeholders. Also, the resources used to provision, implement, and manage software can be centrally consolidated and re-leveraged for multiple deployments. The overall utilization of resources can be reduced through this alignment, as well as through the ability that the ORE provides to store and securely archive and share data such that relevant information within the software can be transferred to the ORE and shared with necessary stakeholders without the necessity of provisioning those stakeholders with licensed accounts to the software. This sharing is made secure through the access control provided by the multi-tenant shared services design of the ORE that segregates data according to the DON's desired security policies and therefore only gives stakeholders access to information relevant to their role.

5.15 ATO Automation

Overview: A large barrier to contract acquisition is the ATO security authorization process that is a necessary component to maintain security of government systems when working with third party vendors. This process is time and cost intensive and potentially prohibitive for certain vendors, which dilutes the pool of potential talent contributing to government systems and creates potential schedule and performance risks for contractors working on projects for the DON. Automating the ATO process would reduce the time and cost of ATO accreditation and therefore enhance the Navy's contracting process and mitigate these risks. However, to sufficiently automate this process, it is necessary to have a tool that is capable of integrating the software solutions involved in the automation process, which also require a cloud native platform to function properly.

Status Quo: The DON currently does not have a tool that is able to integrate its software solutions on a cloud native platform sufficiently for extensive automation.

ORE Feature/Process Alignment: The ORE enables and facilitates extensive automation through the secrets management (machine to machine and user to machine), source code management, and artifact repositories, all orchestrated in the central ecosystem through API integration and secure distributed hybrid cloud storage. This automation capability can be leveraged for software solutions that are used in the ATO process to make data entry and storage more efficient and less costly.

5.16 Risk Management

Overview: Risk management is critical for the success of the DON mission, and therefore must be optimized according to modern IT standards as a part of the DON digital transformation effort. This includes utilizing tools that evaluate and integrate with a modern hybrid cloud native network and address the risks arising from the use of modern IT solutions relating to cloud native platforms,applications, or other IT solutions.

Status Quo: The DON has a robust risk management process. However, it needs to be integrated and applied to a modern service delivery framework and a cloud native network. To do this, the DON needs a tool that will enable that integration as well as provide the visibility and metrics necessary to assess the cost, time, and performance risks associated with a modern system. The DON currently does not have a tool that can facilitate this integration and visibility in a modern environment.

ORE Feature/Process Alignment: The ORE is designed to orchestrate and integrate IT solutions in a modern environment and has many features that impact risk management or the solutions that facilitate risk management. Some examples include: cloud resource monitoring mitigating risk of cost overruns, integration and synchronization of data and applications through API architecture and open standards preventing time inefficiencies and costs related to vendor lock (e.g. as it relates to decommissioning systems, transferring information, moving to new technologies, integrating with other systems, etc.), modern services framework mitigating the risk of scheduling problems and performance degradation or product failure, multi-tenant zero trust framework and granular access control mitigating security risks, and the visibility provided by metrics and information sharing making the risk management process more efficient.

5.17 Knowledge Management

Overview: Knowledge management is critical for an enterprise and intersects with many other facets of the organization. Institutional knowledge needs to be efficiently acquired, created, refined, stored, transferred, shared, and utilized among many different users, teams, departments, or other organizational roles. The DON needs a system that can orchestrate and integrate the different tools leveraged to manage knowledge as a part of an enterprise-wide knowledge management framework that enables all the different commands and offices to communicate, collaborate, and advance institutional knowledge to increase the effectiveness of the entire Navy at meeting its objectives.

Status Quo: The DON has several tools that contribute to knowledge management and collaboration among different users such as document and content management systems, source code repositories, limited structured or unstructured data storage, etc. However, these tools are siloed and the storage is localized or individualized such that there is no visibility or control over the data and no ability to access, aggregate, synthesize, analyze, and archive relevant data. Therefore, it is difficult to use the data effectively for a comprehensive knowledge management plan.

ORE Feature/Process Alignment: Many of the ORE features are critical to enable the Navy to implement a modern knowledge management framework for all its IT solutions and processes including the DevSecOps and CI/CD pipelines, acquisition and sustainment strategies, and project and technology adoption life cycles. The ORE provides the ability to orchestrate and integrate software solutions through API driven architecture and open standards, thus enabling the Navy to aggregate data from all of its solutions being leveraged across the enterprise. The ORE optimizes document and content management systems by providing a file repository that provides archival and sharing of end state multi-media content including document, video, 3D image, and CAD, with secure granular data access control. This enables the Navy to efficiently and securely store and share files across the enterprise. The ORE has a multi-tenant design throughout the system which provides the ability to segregate and aggregate data according the Navy's organizational structure and security framework. All of these features will enable the Navy to efficiently onboard users and tenants, aggregate data for visibility metrics, synthesize and store data so it can be retrieved in usable formats, protect data through granular access control, quickly procure and provision knowledge resources centrally and remotely, capture software states so they can be analyzed and optimized as well as shared and reused, transition data from localized or individual storage to institutional systems so that individual knowledge is institutionalized, and optimize all of these processes through extensive automation.

6.0 Summary Note on Alternatives

Throughout this document it has been maintained, and will be summarized here, that there is no viable alternative to the ORE that supports the government's strategy of having a cloud native multi-cloud hybrid network infrastructure environment. The ORE was developed through a prototype OTA process after market research and analysis of alternatives showed that no commercial product existed that would meet all military mission requirement for multiple data classifications (secret/top secret) including cross domain systems. This drove the additional features, specs, and hardening in the production order upon successful prototyping to

extend the capabilities of the commercial financial application initially developed by 2 Twelve for military purpose use. There is no other tool on the market that currently has a consumable system that meets all of the government's specifications and will enable the DON to achieve its goals of zero trust, operational resiliency, and modern services.

As previously noted, there is either a lack of expertise or a lack of incentive for IT providers to create a product with the ORE's capabilities. The ORE is designed to reduce the proliferation of costs of software licenses and implementation, limit the cost and utilization of network and platform resources, prevent vendor lock by integrating systems and providing an environment in which transferability of solutions and vendors is efficient and convenient, and enable an environment in which the government owns and controls all of its data in a way that is searchable and retrievable without being dependent on particular vendor solutions. All of these things are opposite of the incentives of IaaS, PaaS, and SaaS providers which, according to their business models, are designed to increase their profit by promoting and facilitating the direct opposite - i.e. proliferating licenses and implementations of software, maximizing utilization of network and platform resources, ensuring vendor lock into their own products, and causing the government to be dependent on them by controlling the access and configurations for what should be government owned data.

The Navy is saturated with technical debt which inhibits innovation and adoption of modern technology. The ORE will enable the API "glue" to help with transition and embrace automation to move into a modern service delivery end state. The Navy is currently working against itself by piecing together countless IT systems that are saturated with technical debt and that are not API driven, and trying to use these to achieve the modern flexibility and agility industry has achieved in embracing API driven application constructs and design. Therefore, without the integrated environment and synchronization features of the ORE, the Navy will fail to meet the WAM outcomes as it continues to experience ballooning costs, increased inefficiencies, lack of mobility, operational failures, and an extremely difficult end user experience. The Navy will continue to be at increased risk of cost overruns, time delays, performance degradation, and security vulnerability, which is increasingly becoming an untenable situation.

7.0 Conclusion

This Business Case Analysis (BCA) assessed the features of the Orchestrated Repository for Enterprise (ORE) as they relate to the Department of the Navy's vision to modernize its legacy IT infrastructure and transform it into a cloud native, hybrid, multi-cloud environment. This includes the ORE's capabilities and benefits, it's assumptions and constraints, use cases, and consideration of the Navy's current capabilities and those of other alternatives (for more technical information, see the PEO Digital Concept of Operations for the ORE).

The ORE is the **only** solution available to the Navy that meets all government specifications for its modernization strategy with all of the following characteristics:

- Singular, comprehensive, and **consumable**
- Cloud native, API driven
- Deployable and running on multiple cloud and on premise environments
- Enable operational resiliency through distributed, multi-cloud hosting and storage

- Enable Navy to provide ubiquitous access to data to end users through federation and open standard API architectures
- Enable integration, orchestration, and archiving of all Navy's networks, data, software, configurations, etc.
- Enable Navy to maintain independence, ownership, and control of its networks, data, software, configurations, etc.
- Enable the Navy to implement modern service delivery model with end user centricity in mind through end to end multi-tenant, shared services design
- Enable Navy to monitor deliver WAM outcomes
- Enable Navy to implement zero trust framework
- Enable cost projection of configurations/IaC to support pilot transition into production based on the horizon MSD pilots

The Navy is saturated with technical debt which inhibits innovation and adoption of modern technology. It cannot achieve the flexibility and agility of modern systems that have embraced API driven constructs and designs by its current approach of piecing together isolated systems that have not embraced these designs. Therefore, the ORE is critical to the Navy's effort to meet the WAM outcomes. Without it, the Navy will continue to experience ballooning costs, increased inefficiencies, lack of mobility, operational failures, and an extremely difficult end user experience with increased risk of cost overruns, time delays, performance degradation, and security vulnerability.

In conclusion, the ORE was developed through a prototype OTA process after market research and analysis of alternatives showed that no commercial product existed that would meet the Navy's requirements, which drove the development of the additional features and capabilities of the ORE. The ORE is the only solution that supports the government's strategy of having a cloud native mult-icloud hybrid network infrastructure environment, and it is the only tool on the market that currently has a consumable system that meets all of the government's specifications and will enable the DON to achieve its goals of zero trust, operational resiliency, and modern services.

Appendix A: Acronyms

API - Application Programming Interface

ATO - Authority to Operate

BCA - Business Case Analysis

CAC - Common Access Card

CAD - Computer Aided Design

CI/CD - Continuous Integration/Continuous Deployment/Delivery

COO - Chief Operating Officer

DevSecOps - Development Security Operations

DoD - Department of Defense

DON - Department of the Navy

GCP - Google Cloud Platform

IaaS - Infrastructure as a Service

ICAM - Identity Credential Access Management

IdAM - Identity Access Management

IT - Information Technology

NEN - Naval Enterprise Network

NMCI - Navy Marine Corps Intranet

ORE - Orchestrated Repository for Enterprise

OSI - Open Systems Interconnection

OTP - Other Transaction Authority Production

PaaS - Platform as a Service

PEO - Program Executive Office

SaaS - Software as a Service

SAST - Static Application Security Testing

SCM - Source Code Management

WAM - World-class Aligned Metrics

Appendix B: References

NEN-ORE Concept of Operations

Performance Work Statement (PWS): Transition of IWRP-19-LANT-0012 to Operationalize Enterprise Capabilities as a Service