OSD IT DIGITAL MODERNIZATION ROADMAP
FY2026 – 2030

OSDCIO │ CHIEF INFORMATION OFFICER

FOREWORD

Information Technology (IT) underpins every aspect of the Office of the Secretary of Defense (OSD) mission – from crafting defense policy to enabling warfighters and protecting the Pentagon. OSD cannot perform its mission without a robust and reliable technology foundation. Unfortunately, years of disparate representation of OSD IT requirements has resulted in IT support that is slow to react to customer needs, increased cybersecurity vulnerabilities, underperforming networks, aged IT equipment, and a lack of visibility into IT budget and execution; these pain points will be addressed in the execution of this roadmap. Further, a February 2023 Defense Business Board (DBB) study found the Department of Defense's (DoD) IT capabilities and services – which include capabilities and services for the OSD workforce – fall short of expectations, and user experience lags behind industry standards.[1]

Our OSD workforce needs secure networks, reliable devices, a responsive help desk, and modern software applications to carry out OSD's broad mission set. These capabilities are critical to supporting key National Defense Strategy (NDS) priorities of building enduring advantages over our adversaries.[2] We face ever-growing mission requirements, a legacy of underinvestment, and growing adversary capabilities and intent to derail the OSD mission via digital disruption. There is no quick fix or single solution for these challenges.

The OSD Chief Information Officer's (CIO) office has outlined specific business outcomes as objectives over the next five years, with the overarching goal of continuously modernizing the OSD IT landscape. As described in this roadmap, the OSD CIO is focused primarily on improving the user experience by achieving business outcomes of **protection of DoD data, a responsive global service desk (GSD), a reliable remote experience, continuous access to current technology, and consistent network performance**. OSD CIO will drive toward these outcomes through a formalized process of collecting, prioritizing, and addressing OSD IT requirements into a cohesive, united perspective, which will in turn drive IT resourcing decisions. To achieve this, the OSD CIO is continuing its partnership with its customers, DoD CIO, and the Pentagon's IT service provider in deploying new solutions and measuring success. Together, we will work toward a future environment that is more responsive to customer needs and supports seamless collaboration, reforming information sharing to advance warfighter needs.

The Secretary of Defense stated in his memorandum introducing the 2022 NDS that "in these times, business as usual at the Department is not acceptable." Ensuring effective management of OSD IT is essential to reform. The Department, including the OSD IT enterprise, must not be complacent or accept the status quo. Instead, we must challenge traditional ways of doing business to better support our nation's top defense priorities while making the best possible use of taxpayer dollars.

Danielle Metz
Deputy OSD CIO

---

1   "Recommendations to Improve the IT User Experience within DoD," February 2023 Defense Business Board Study. https://dbb.defense.gov/Portals/35/Documents/Reports/2023/DBB%20FY23-02%20IT%20User%20Experience%20Report%20Cleared%20Final%20Approved%20Printing1.pdf.

2   U.S. Department of Defense Mission Statement. Retrieved January 30, 2024. https://www.defense.gov/About.

CONTEXT: THE OSD IT LANDSCAPE

IT is a critical enabler to every OSD mission. People use IT at all organizational levels to do their jobs. To do those important jobs effectively, they need fast and secure networks, modern IT equipment, access to enterprise collaboration capabilities, and the ability to get help quickly when required. The OSD CIO must ensure the OSD workforce has these key enablers, and we need to do it in the most efficient way possible.

The 2022 NDS lays out a vision for focusing the DoD on key priorities amidst the known and emerging threats of our swiftly changing world and near peer competition. All facets of the Department must strive to support these priorities, including management and modernization of our IT environment. Specifically, modernization of the OSD IT enterprise supports the Department's **future military advantage** by building a **resilient OSD ecosystem**, which is part of the larger defense ecosystem. The business outcomes described in this roadmap are designed to **build enduring advantages across the OSD ecosystem**, with a focus on **innovation and agile adjustment to new strategic demands**. Further, the DoD's 2019 Digital Modernization Strategy describes a modernization goal for the Department to "optimize for efficiencies and improved capability.[3]" The OSD-specific outcomes described in this roadmap align with this goal and its corresponding objective of "shifting from Component-centric to enterprise-wide operations and defense model."

In 2022, the Director of Administration and Management (DA&M)'s OSD IT Study found that a lack of IT requirements and resources at the Pentagon and Mark Center negatively disrupted user experience over time. Customers expressed concern with the level of IT support provided, specifically with network performance, and with the resulting impact of current technology impeding their ability to conduct their missions. A February 2023 DBB evaluation of the DoD IT user experience yielded similar findings and cited that 80 percent of respondents rated their IT user experience at average or below. Many of these themes have been echoed over the past year during OSD CIO listening sessions with OSD organizations and user surveys. Recent examples of modernization activities performed to address these concerns include the deployment of modern communication tools on classified networks and a technology refresh of the service desk. In crafting this roadmap, we have structured the business outcomes to leverage existing efforts and strengthen the OSD ecosystem's capacity to uphold missions crucial for the nation's top priorities.

THE FUTURE OF OSD IT

The OSD IT enterprise workforce is comprised of personnel within 18 Principal Staff Assistants (PSAs) and six Defense Agencies and Field Activities (DAFAs)[4] who require access to a functioning suite of IT equipment to include desktops, laptops, and mobile phones loaded with secure, reliable software that enables office productivity and modern communications. The OSD CIO's vision to deliver a mission-enabling consistent and continuous IT user experience for all OSD employees aims to guarantee that the OSD enterprise workforce is armed with a solid IT foundation, providing the common capabilities required to perform their missions and inform senior leader decision making.

> **Deliver a mission-enabling consistent and continuous IT user experience for all OSD employees.**

---

3   "DoD Digital Modernization Strategy." July 2019. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF

4   The OSD IT enterprise represents the offices of the PSAs, Washington Headquarters Services (WHS), Pentagon Force Protection Agency (PFPA), Defense Technology Security Administration (DTSA), and parts of the DoD Education Activity (DoDEA), Defense Human Resources Activity (DHRA), and the Defense Security Cooperation Agency (DSCA).

The three operational goals initially described in the February 2023 OSD IT Enterprise Implementation Plan continue to guide OSD CIO's efforts. In alignment with these goals, this roadmap describes five desired business outcomes critical to achieving the OSD CIO vision: protection of DoD data, a responsive global service desk, a reliable remote experience, continuous access to current technology, and consistent network performance. Appendix A also describes OSD's business process – or "the business of doing" – for navigating from the generation of IT requirements to resourcing priorities, then executing against those priorities and measuring performance. Figure 1 illustrates how these elements build upon one another to ultimately come together and improve the OSD IT enterprise.
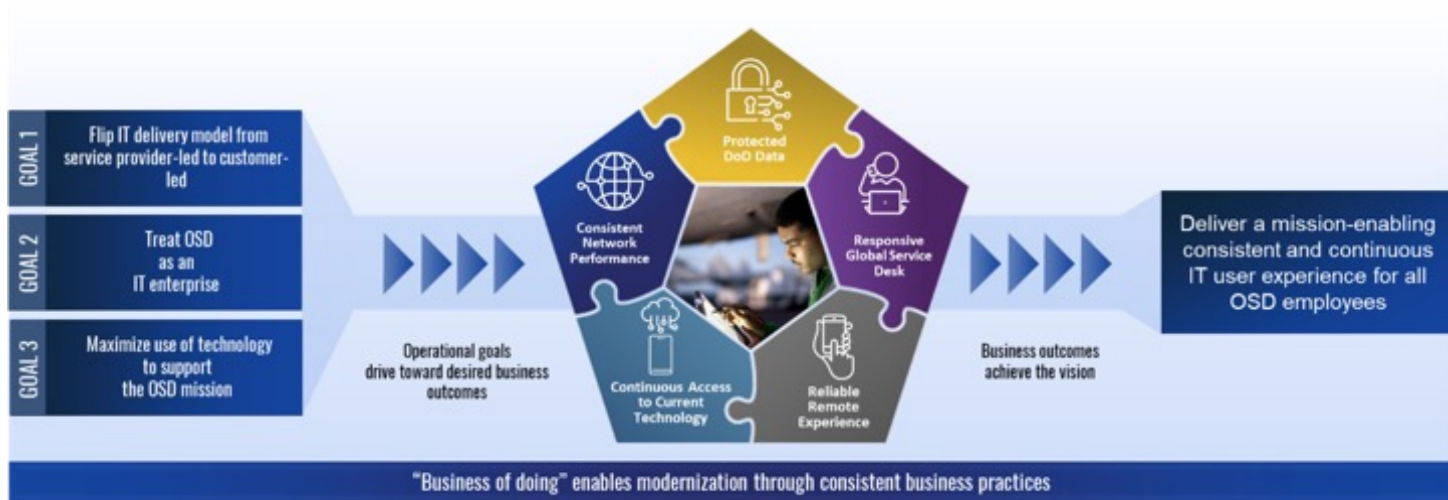

FIGURE 1: OSD CIO Goals and Business Outcome

BUSINESS OUTCOMES AND PRIORITIES

Over the next five years the OSD CIO will address OSD IT customer needs and ultimately help the Department achieve its strategic priority of building a resilient joint force. Each business outcome, as shown in Figures 1 and 2 and described below, provides a critical piece of a solid IT foundation required to build an enduring advantage and enable OSD mission success.

» **Protected DoD Data:** Protect OSD IT from cyber threats via thorough cybersecurity risk management activities, zero trust practices, an OSD Authorizing Official (AO), and secure cloud migration.

» **Responsive Global Service Desk:** Provide fast, relevant, democratized help desk support to OSD IT customers. Modernize the OSD property accountability process by acquiring resources and appropriately automating workflow.

» **Reliable Remote Experience:** Provide reliable, secure remote work capabilities to OSD customers that meet or exceed their personal IT capabilities.

» **Continuous Access to Current Technology:** Ensure OSD customers are equipped with world-class technology that supports their everyday mission requirements to end user personal devices and conference room equipment.

» **Consistent Network Performance:** Ensure OSD customers have consistent and reliable network connectivity whether in the building or working remotely, in line with enterprise DoD offerings.

FIGURE 2: OSD IT Environment Business Outcomes

Figure 3 highlights the rollup of these business outcomes tied to priorities and defined performance metrics to measure success, with the following section highlighting each business outcome in more detail.

BUSINESS OUTCOME	PRIORITIES	PERFORMANCE METRICS
PROTECTED DOD DATA	Create an OSD enterprise around cybersecurity	• Stand up OSD enterprise AO function by FY27 • Align AO and defense cyber operations (DCO) functions to single office by FY29 • Target level zero trust for common IT by FY28
	Assist OSD with cloud migrations	• Increase number of systems migrated to cloud by 50% by FY28 • 100% of cloud contracts via Enterprise Cloud Offerings by FY29
RESPONSIVE GLOBAL SERVICE DESK	Transition to enterprise help desk	• Increase first call resolution to 50% for Global Service Desk (GSD) • Reduce average speed to answer phone to under 30 seconds/answered 80% of the time for GSD • Maintain under 5% call abandonment rate for GSD • Score at least 75% customer satisfaction score (survey scores 1-9) for GSD
	Standardize property accountability and asset management	• Obtain 100% property accountability by FY27 • Merge virtual and physical inventories to a single inventory by FY28
	Enhance enterprise help desk capabilities	• Increase self-help or self-service capabilities to 15% of all service requests by FY29
RELIABLE REMOTE EXPERIENCE	Provide increased capabilities to offsite workforce	• Deploy modern virtual remote desktop capability by FY27 • Increase remote IT user satisfaction by 20% by FY28
	Make available IT assets for hoteling across OSD workspaces	• Pilot Pentagon hoteling capability by FY28
CONTINUOUS ACCESS TO CURRENT TECHNOLOGY	Standardize services for common IT between service provider and OSD customers	• Signed Memorandum of Agreement (MOA) in FY24; updates by FY27 and FY30
	Modernize end user devices	• Implement and resource four-year lifecycle refresh (LCR) by FY26
	Improve IT aspects of the OSD onboarding process	• Establish business process owner for onboarding in FY24 • Implement plan to improve OSD onboarding by FY26
	Increase use of provided communication tools	• Increase use of OneDrive across OSD to 100% by FY26
CONSISTENT NETWORK PERFORMANCE	Standardize and simplify the OSD network environment	• Transition to Fourth Estate Network Optimization by FY27 • Maintain under 3% average packet loss rate • Maintain under 70% utilization on key circuits

FIGURE 3: Business Outcomes Tied to Priorities & Performance Metrics

PROTECTED DOD DATA

OSD does not have a unified cybersecurity approach. There is currently no single entity in charge of cybersecurity within the Pentagon.[5] Part of the risk mitigation plan is to create a more unified and streamlined approach to cybersecurity for both cyber operations and system authorization. As the cyber risk manager for OSD enterprise data, the OSD CIO will work to reduce the impact of cyber threats and ensure the continuity of OSD business operations by standing up an enterprise Authorizing Official (AO) function that will provide oversight on behalf of the OSD IT enterprise, streamlining AO and defense cyber operations, and ensuring the deployment of target level zero trust for common IT.

MISSION PURPOSE
- Protect OSD IT from cyber threats via thorough cybersecurity risk management activities, Zero Trust practices, an OSD AO, and secure cloud migration

Cybersecurity

The OSD CIO will continue collaboration with OSD customers to gain insights into their specific cybersecurity needs and ensure that security measures are aligned with mission-critical functions. This effort includes verifying that all security measures and practices adhere to established DoD CIO and U.S. Cyber Command cybersecurity guidelines and regulations through continuous integration with Joint Force Headquarters-DoD Information Network (DoDIN). Partnership with the cyber operations community is essential to ensuring that OSD maintains pace with defensive cyber operations.

Unlike many other DoD Components, the OSD enterprise currently lacks an enterprise AO[6]. OSD IT enterprise customers must rely on the Defense Information Systems Agency (DISA) for AO services or stand up their own authorization offices. In the former case, OSD's AO needs are queued along with the other Components that DISA services, while in the latter case, there is an increased resourcing requirement for each new authorizing official that is established. To alleviate these concerns, **OSD CIO will stand up an AO role and build out its responsibilities so that the OSD enterprise's IT systems adhere to risk management framework principles, enhancing the overall cybersecurity posture of the enterprise. The OSD AO will closely collaborate with OSD IT enterprise organizations to accredit mission IT for OSD to have more influence over its cyber posture and increased flexibility in cybersecurity risk management.**

---

5   Reference the 2022 OSD IT Study (summary located at https://dam.defense.gov/Portals/47/Documents/IMT/OSD%20IT%20Study%20Summary%2010.7.22.pdf?ver=KrclAnJXEDMKURBHT5AbBg%3d%3d)

6   Per NIST definition, an AO is an "Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals" (https://csrc.nist.gov/glossary/term/authorizing_official).

OSD Cloud Adoption

The Department has widely embraced cloud computing, and the DoD Joint Warfighting Cloud Capabilities (JWCC) contract has significantly improved access to cloud services. However, many of the OSD IT enterprise services and products, such as the defense business systems that service the OSD IT enterprise, have not yet undergone a complete shift to the cloud. The OSD CIO will continue to collaborate closely with OSD IT enterprise customers to provide guidance and support throughout their cloud migration processes. **By doing so, the OSD CIO aims to maximize the benefits of cloud computing, including enhanced security, flexibility, and accessibility, for the entire OSD enterprise.**
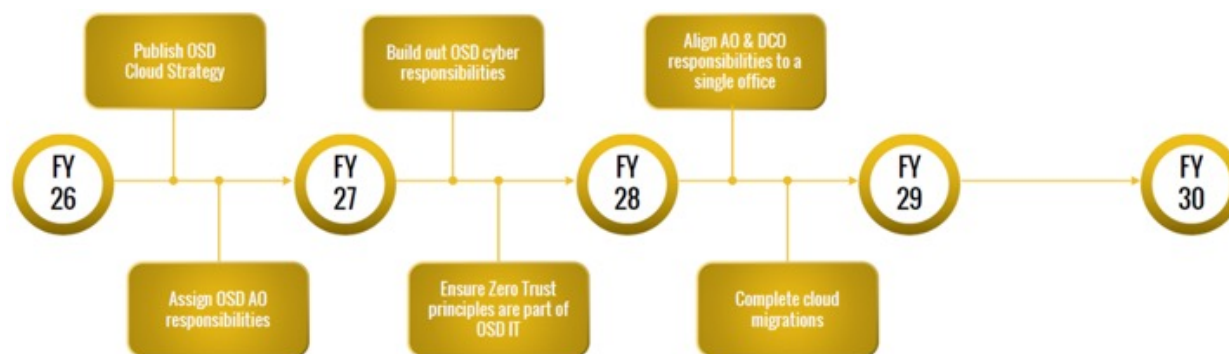

FIGURE 4: High-level Data Protection Activities

RESPONSIVE GLOBAL SERVICE DESK

The 2023 DBB study identified that 80 percent of DISA J6 Pentagon customers rated IT services as average or below average.[7] Pain points for the service desk included a cumbersome DISA J6 ticketing process, multiple help desks being required to service a single ticket, and ineffective help desk personnel. OSD requires a single, integrated resource that quickly and efficiently provides help with IT problems, supports automation of business processes, and regularly reports performance metrics. The Global Service Desk transition is in line with the Department's IT modernization policy; it is the first step in the approved Fourth Estate Network Operations (4ENO) transition.[8]

MISSION PURPOSE
- Provide fast, relevant, democratized help desk support to OSD IT customers
- Modernize the OSD property accountability process by acquiring resources and appropriately automating workflow

A Phased Approach to Implementing Global Service Desk

DISA, OSD CIO, and DoD CIO are working together to implement a phased approach to modernizing the Pentagon's service desk. Phase One, which began enactment in FY24, involves the transition to a new toolset for the service desk. The new toolset brings an enhanced user experience through improved first contact resolution, same day resolution, call abandonment rate, and transparency. New capabilities such as customer service automation and an increased number of self-service tools will ultimately drive down service support interactions with the service desk. Phase Two of the GSD transition includes the transition of most of the service desk personnel from contractors to civilians, which will reduce turnover and creates more knowledgeable and seasoned service desk agents.

---

7   "Recommendations to Improve the IT User Experience within DoD," February 2023 Defense Business Board Study. https://dbb.defense.gov/Portals/35/Documents/Reports/2023/DBB%20FY23-02%20IT%20User%20Experience%20Report%20Cleared%20Final%20Approved%20Printing1.pdf.

8   "Fourth Estate Network Optimization Execution Guidance," DSD memorandum signed August 19, 2019.

Property Accountability and Asset Management

Asset management is not currently standardized within OSD. DISA J6 does not currently provide IT asset management services to OSD; OSD Components each track their own assets using loosely aligned standard operating procedures. OSD CIO will partner with the service provider to update policies regarding property accountability and spiral in new GSD capabilities like process automation to create a more responsive property system of record. Working with the service provider for the implementation of new tools, the OSD CIO will ensure property custodians and each OSD organizational lead has training on emerging asset management tools. The customer base will be able to perform tasks such as verifying IT inventory across the OSD IT enterprise. **The OSD CIO will reengineer and automate business processes to eliminate error, support faster workflow, and optimize automation**. OSD IT enterprise customers should expect to have same-day replacement for a poorly performing device, either as a loaner or new hardware, when issues occur on their assigned devices. This level of service requires the use of end-point monitoring on all devices, a well-resourced service desk staff, and an adequate operationally ready inventory.

Increased Service Desk Capabilities

The transition to GSD is the first step in modernizing OSD's service desk environment. Based on OSD IT Enterprise Committee (OITEC) Working Group requirements, OSD CIO will lead the transition to a self-help, automated service desk environment powered by artificial intelligence (AI) bots. **Future capabilities include the ability to access the service from a remote device if their furnished IT equipment is broken, increased knowledge management for zero service troubleshooting, and the implementation of AI bots that will automatically solve simple issues like Common Access Card (CAC) PIN resets.**
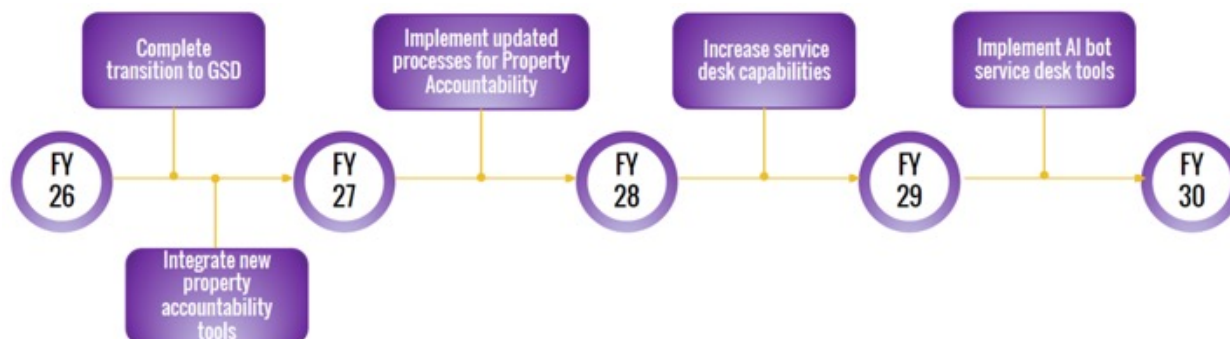

FIGURE 5: High-level Global Service Desk Activities

RELIABLE REMOTE EXPERIENCE

The aftermath of the COVID-19 pandemic changed the way the Department does business and proved that many DoD missions could be delivered remotely.

MISSION PURPOSE
- Provide reliable, secure remote work capabilities to OSD customers that meet or exceed their personal IT capabilities

Virtual Remote Desktop

OSD remote workers regularly utilize a home computer to access their work environments. The current usage of existing virtual desktop infrastructure (VDI) type capabilities across the Pentagon is sporadic. Additionally, there is no standardized guidance for how the OSD IT enterprise should properly address a reliable remote experience consistently. Using OSD CIO's established governance processes, the OSD IT enterprise is documenting its virtual remote desktop requirements and participating in a pilot that will eventually deploy a modern virtual remote desktop capability with established business processes to OSD. **The aim is to drive culture change by providing a limited number of standardized virtual remote desktop options that will fit each organization's common IT requirements while still staying with the limits of repeatable, consistent business practices across OSD.**

Hoteling

The Pentagon reservation lacks adequate office space and amenities for the number of OSD personnel who are assigned there. The OSD CIO will support Washington Headquarters Services (WHS) on initiatives to analyze Pentagon space requirements based on the number of full-time, in-office personnel versus the number of part-time remote workers. This analysis will determine the efficacy of acquiring a hoteling system that would enable remote workers to find a workspace on days they are at the Pentagon reservation. Hoteling has the additional benefit of enabling work-life balance and providing the ability for DoD to attract and retain talent. **A functioning system to determine open desks for all OSD**, along with providing the required IT capability for all office spaces, is the IT contribution to this effort.
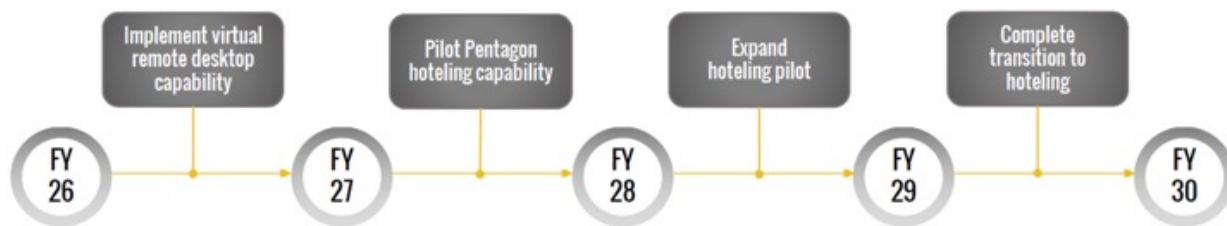

FIGURE 6: High-level Remote Experience Activities

CONTINUOUS ACCESS TO CURRENT TECHNOLOGY

OSD is not a market leader in access to current IT equipment. The 2023 DBB study of DoD IT found inadequately funded IT has created a DoD-wide digital environment of outdated hardware, software, and IT infrastructure. On average, desktop equipment across the DoD is six years – which is well beyond

MISSION PURPOSE
- Ensure OSD customers are equipped with world-class technology that supports their everyday mission requirements to end user personal devices and conference room equipment
- Alleviate "work stoppage" when customer devices are on order or with the help desk

industry standards. The 2022 OSD IT study found that OSD users frequently complained about the length of time required for their workstations to turn on, with many reporting wait times far above what is found in the private sector or personal use. The forced wait time caused a lack of access to mission critical information and lost productivity. Providing OSD access to high performance desktops, laptops, and mobile devices will enable OSD organizations to perform their critical job functions and not see IT as a mission hindrance.
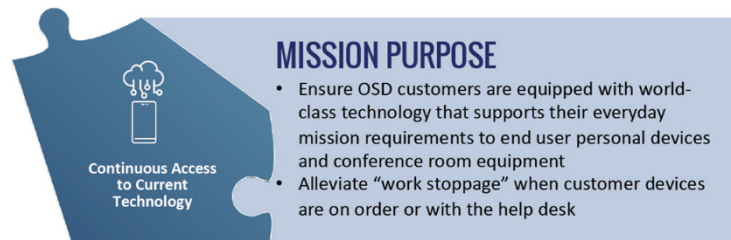
Memorandum of Agreement

OSD CIO collaborated with DISA and the OSD IT enterprise customers in FY23 to develop a Memorandum of Agreement (MOA) for common use IT for the OSD IT enterprise – the first of its kind to clearly define roles and responsibilities throughout the OSD IT community. **The MOA, signed in February 2024, defines OSD common IT requirements from the service provider and tracks service provider performance through service level agreements.** The MOA will be reviewed and updated on a periodic basis to ensure it stays current with DISA's infrastructure, OSD IT enterprise common IT requirements, and the associated performance metrics used to measure services.

End User Device Modernization

In the summer of 2022, the OSD CIO partnered with DISA to increase productivity through initiating a four-year lifecycle replacement strategy for OSD IT enterprise end users that will include individual endpoint devices as well as conference and team room technology. Maintaining a four-year lifecycle requires dedicated funding and support so that resources are not siphoned off to other priorities. This includes the creation of a **"standard IT package"** across the OSD IT enterprise, which will baseline the end user equipment provided, to include a virtual remote desktop option. The OITEC Working Group will determine different IT packages for

the various user types and capabilities and will work with the service provider to ensure the end user device packages are standardized across the OSD IT enterprise.

Improving the IT Aspects of the OSD Onboarding Process

A study conducted in March 2022 to assess the existing OSD civilian onboarding process found that the process is not owned by a single entity, dependencies on collaboration exist across multiple business systems and support organizations, IT timelines are tied to non-IT business processes, and initial account provisioning is tied to DoD-wide IT system timelines (i.e., personnel, identity, and licensing systems).[9] In response to these findings and with direction from the Deputy Secretary of Defense (DSD), the Performance Improvement Officer (PIO)/DA&M is establishing a business process team to baseline the onboarding execution time to expose areas for optimization. The OSD CIO, in coordination with WHS, PFPA, DHRA, and DISA, are identifying areas of automation for all or part of the end-to-end process; opportunities for rationalization of workflows between systems; and examining the feasibility of expanding the time-to-hire dashboard, to include onboarding workflows and metrics. **The outcome is an OSD-wide standardized, repeatable onboarding process with a reduced onboarding timeline for civilian hires.**

Increase Usage of Communication Tools

As cloud software-as-a-service technology matures and DoD increases its adoption, the same communication tools deployed on unclassified networks for voice, video, chat, and storage will be delivered on classified networks. **Lower training and knowledge overhead will be required for users when transitioning from one domain to another**. Further, backend storage infrastructures will be   modernized, transitioning from on-premises data stores in DoD datacenters to accredited commercial cloud vendor solutions that are more scalable and accessible.
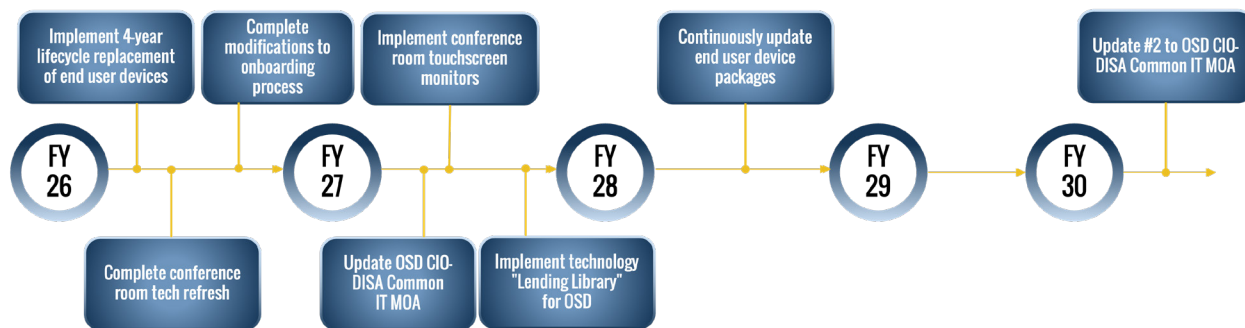

FIGURE 7: High-level Continuous Access to Current Technology Activities

CONSISTENT NETWORK PERFORMANCE

A substantial portion of the OSD enterprise workforce operates within a hybrid work environment, necessitating fast and dependable network connectivity both within and outside of the Pentagon for the execution of mission-critical tasks. The OSD IT study uncovered significant lags in log-in times, and the DBB study confirmed that some users experience log-in wait times that disrupted productivity and impeded a positive user experience. OSD CIO will continue to work with DoD CIO and DISA to streamline network architectures, eliminate complexity, and reduce downtime through network simplification and software defined networking tools.

MISSION PURPOSE
- Ensure OSD customers have consistent and reliable network connectivity whether in the building or working remotely

Consistent Network Performance

---

9   "New Hire Onboarding and Information Technology Access Package," WHS study completed in March 2022.

Simplifying networks servicing the OSD IT enterprise will lead to improved network performance, greater reliability, reduced costs, enhanced security, and an overall improved user experience for OSD customers. The Fourth Estate Network Optimization migration, along with the transition off legacy capabilities that complicate network performance and onto a zero-trust enabled, software defined wide area network, will pave the way for OSD's network simplification. OSD CIO will support the planning, resourcing, and execution of both initiatives.
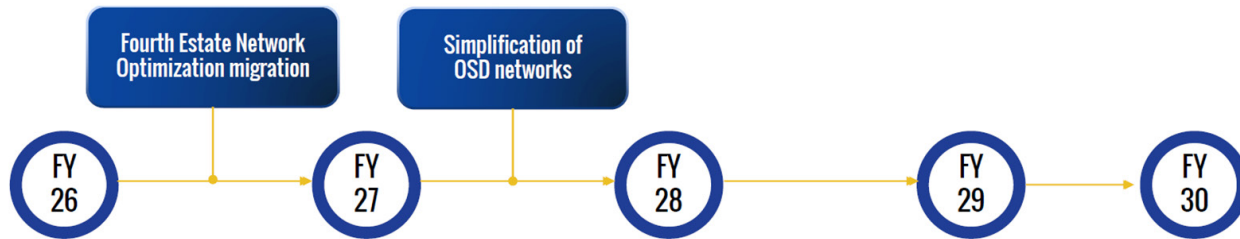

FIGURE 8: High-level Network Performance Activities

BENEFITS FROM ACHIEVING BUSINESS OUTCOMES TO OSD IT CUSTOMERS

The roadmap elements described above outline work the OSD IT enterprise and DISA will perform over the next five years. They will drive OSD toward an enduring advantage in the IT environment, supporting NDS priorities and DoD guidance regarding digital modernization. These outcomes will also yield tangible benefits for OSD IT customers. The figure below outlines common challenges users face every day in the current OSD environment versus user benefits of OSD achieving its desired business outcomes.
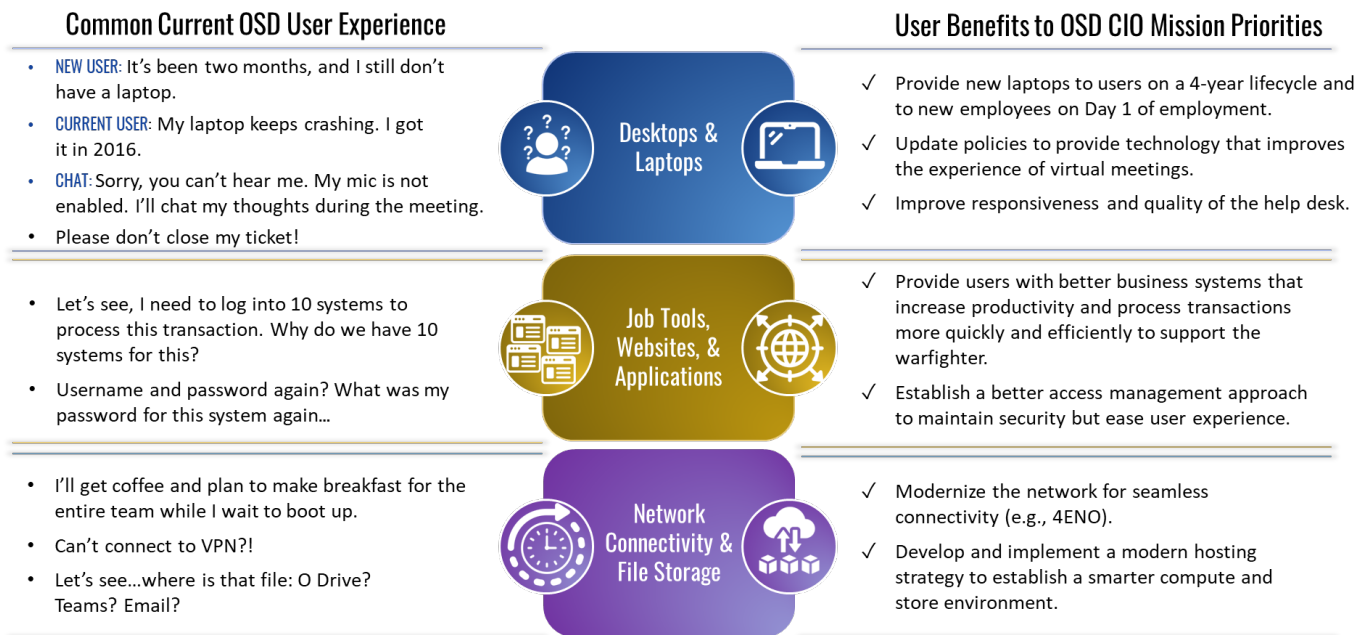
Common Current OSD User Experience

- NEW USER: It's been two months, and I still don't have a laptop.
- CURRENT USER: My laptop keeps crashing. I got it in 2016.
- CHAT: Sorry, you can't hear me. My mic is not enabled. I'll chat my thoughts during the meeting.
- Please don't close my ticket!

Desktops & Laptops

- Let's see, I need to log into 10 systems to process this transaction. Why do we have 10 systems for this?
- Username and password again? What was my password for this system again…

Job Tools, Websites, & Applications

- I'll get coffee and plan to make breakfast for the entire team while I wait to boot up.
- Can't connect to VPN?!
- Let's see…where is that file: O Drive? Teams? Email?

Network Connectivity & File Storage

User Benefits to OSD CIO Mission Priorities

- ✓ Provide new laptops to users on a 4-year lifecycle and to new employees on Day 1 of employment.
- ✓ Update policies to provide technology that improves the experience of virtual meetings.
- ✓ Improve responsiveness and quality of the help desk.

- ✓ Provide users with better business systems that increase productivity and process transactions more quickly and efficiently to support the warfighter.
- ✓ Establish a better access management approach to maintain security but ease user experience.

- ✓ Modernize the network for seamless connectivity (e.g., 4ENO).
- ✓ Develop and implement a modern hosting strategy to establish a smarter compute and store environment.

FIGURE 9: Benefits to OSD IT Customers

OSD users can anticipate reduced instances of service disruptions resulting from sluggish service desk responses, outdated equipment, or network latency. The roadmap includes a commitment to providing standardized end user devices every four years, with capabilities designed to bolster performance in both office and remote work settings. The transition to shared enterprise services will further augment productivity by implementing a streamlined user experience.

SUMMARY

As the OSD CIO pursues its mission to elevate the digital capabilities of the OSD IT enterprise, this roadmap seeks to streamline and enhance OSD IT, making it more agile and responsive to the rapid pace of technological advancements. It is a roadmap to support the mission and needs of the OSD workforce, with a strong emphasis on customer satisfaction and efficient resource allocation. Appendix C outlines a consolidated schedule of all planned modernization activities for the OSD IT enterprise contained in this roadmap.

Fundamentally, this roadmap is a shift in the way IT services are delivered, moving from a service provider-led approach to a customer-centric one where the customer defines its IT requirement, solidifying OSD as a single Component when it comes to IT. Achieving these business outcomes will position OSD to address the complex challenges in the upcoming years. As the OSD IT landscape begins to achieve the outcomes outlined in the roadmap, the OSD CIO will continue to explore emerging technologies. This will ensure that the OSD IT enterprise remains aligned with evolving technological trends and its customers base is capable of accessing and using technology to effectively perform their mission.

FOLLOW US ON LinkedIn

APPENDIX A: THE BUSINESS OF DOING

To enact the IT modernization efforts outlined in this document, the OSD CIO has created a repeatable framework to positively influence IT programs. This iterative cycle utilizes IT governance forums, the Planning, Programming, Budgeting, and Execution (PPBE) resourcing cycle, capability delivery, and performance metrics to ensure the IT program is delivering required capability in line with this roadmap's mission outcomes.

The business of the OSD CIO is guided by three primary ideas: 1) The organizations comprising the Office of the Secretary of Defense should be treated as a single OSD enterprise, 2) OSD customers are the primary drivers of OSD common IT requirements, and 3) OSD CIO and service provider operations should be held accountable to performance standards. The Governance circle in Figure 10 shows the cycle of delivering capability; governance is the starting point for any modernization initiative in the OSD IT enterprise. The OSD CIO strives to identify, document, and prioritize OSD customer requirements both accurately and completely, and uses multiple channels to ensure requirements are captured at all levels of customer organizations. The governance process documents, sorts, prioritizes, and determines performance measures for OSD common IT requirements. The OSD CIO then works with customers to determine an appropriate funding plan for each requirement and acts both for and with customers to acquire the requisite funding. Once funded, the OSD CIO acts as a liaison with the service provider to execute and provide the requirements to the standards determined in the OSD governance process. Performance metrics are analyzed, and requirement activities are reevaluated to determine if a course correction needs to be made or if there are additional, unidentified requirements that need to be fulfilled. At each stage of OSD business, the customers are engaged with the OSD CIO.
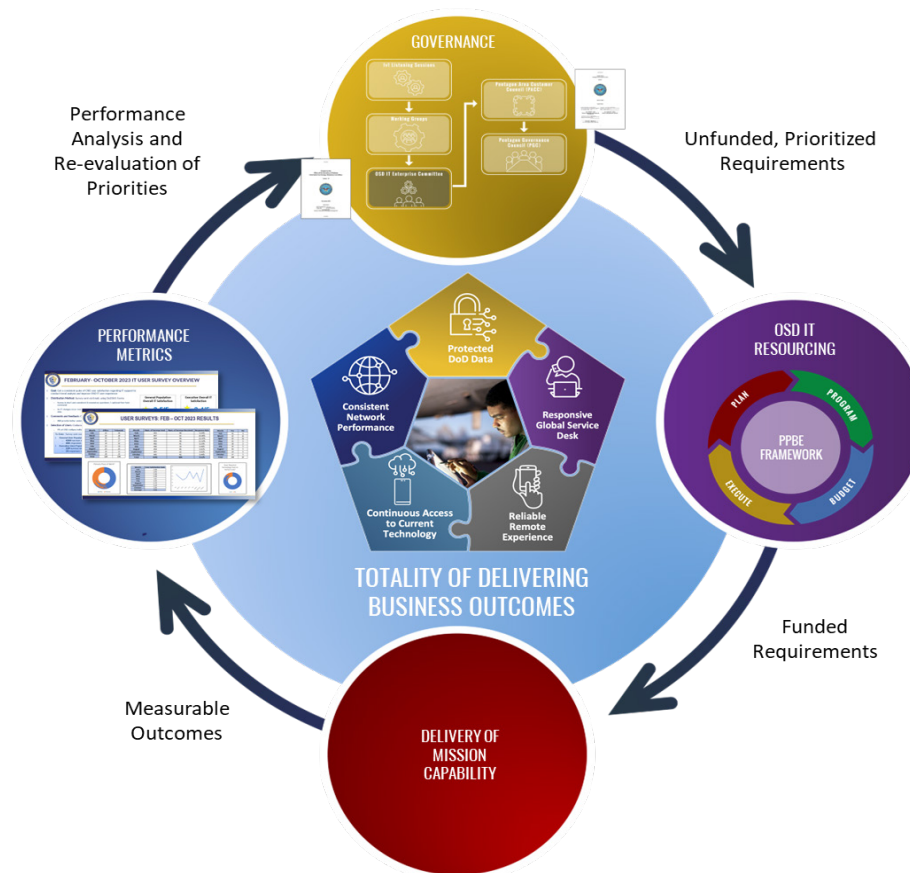

FIGURE 10: OSD CIO Business Process

CREATING A DYNAMIC, EFFICIENT GOVERNANCE PROCESS

One of the first actions of the newly established OSD CIO was to institute an OSD IT governance framework designed to collect and prioritize requirements, address issues, and collectively work though areas of focus and then drive recommendations up the governance chain to final decision makers. A strong, collaborative governance model is critical to the success of the OSD CIO because OSD's commitment to the modernization of the OSD IT enterprise requires the active participation of each OSD IT enterprise stakeholder so that their perspectives and requirements are understood and addressed.

With a customer-driven focus, it is critical that OSD enterprise Components be engaged and invested in the workings of OSD IT from the initial discussion through execution of the decision result. While OSD CIO provides executive secretariat support to the governance forums, the collective set of OSD IT managers and senior leaders are critical to the success of governance objectives.

FIGURE 11: OSD IT Governance Framework

The OSD IT enterprise governance model is a multi-layered model where each layer is comprised of different stakeholder groups from across the OSD enterprise. The OSD governance structure is detailed in the **Pentagon Area Customer Council (PACC) charter** and the **OITEC charter**.

RESHAPING OSD IT RESOURCING

Delivering a mission-enabling consistent and continuous IT user experience requires dedicated and consistent funding and transparency of assets and expenditures. A transparent and democratized funding model is crucial for accountable financial stewardship, trust, and credibility between enterprise constituents, as well as the equitable inclusion of smaller OSD Components, stakeholder inclusion in financial decision making, adaptability to evolving needs and challenges, and alignment with OSD IT enterprise mission and values. Information resource management is a key CIO responsibility and a key priority for OSD leadership to understand where and how many IT resources are being expended. The OSD IT Digital Modernization Roadmap and anticipated business processes and products associated with the roadmap will drive the annual execution of services.

To that end, OSD CIO has partnered with the OSD IT enterprise stakeholders over the last two program cycles to actively advocate for funding to enable new technology, modernization tools and processes, and reliable remote capabilities through the annual program and budget review process.
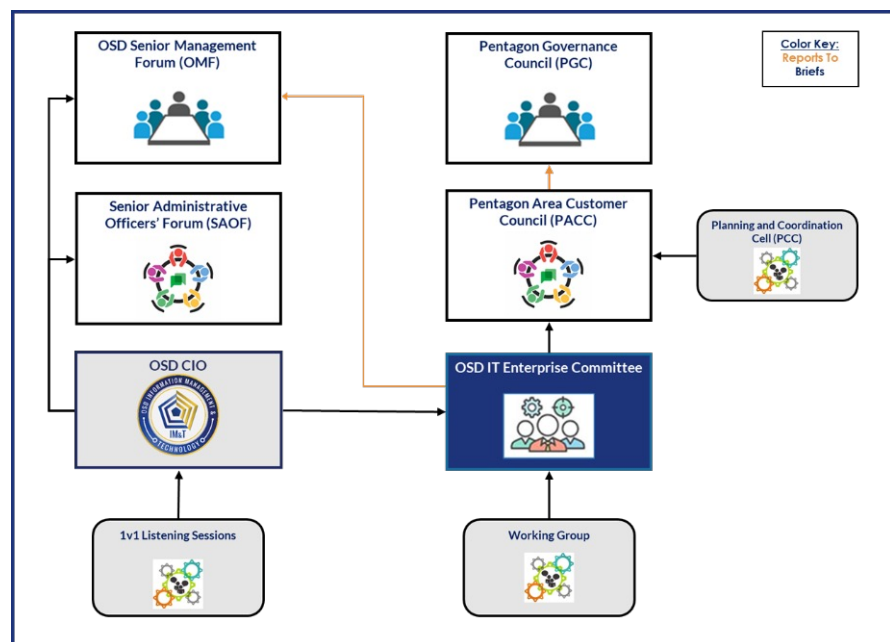
Separately, conceptually working from the principle of equitable access to resources, the OSD CIO is partnering with the PACC, the OSD IT enterprise customers, DISA, and the DoD financial community to baseline user requirements and consumption levels, capture total cost of ownership for the delivery of common IT services, identify baseline cost and potential resource gaps, and shape business processes to govern future delivery of identified capabilities with the transparency and accountability they deserve. **This analysis and outcome will allow more flexibility to resource new technology insertion and provide centralized management of OSD IT financial resources.**

DELIVERING MISSION CAPABILITY

The OSD CIO mission initiatives are based on requirements that have been approved and funded through the governance structure and resourcing process or from environmental factors such as changing DoD technology priorities that must be addressed for the OSD IT enterprise. Prior to implementing mission initiatives, the OSD CIO collaborates with the service provider to develop a plan and timeline for implementation. As mission requirements are being addressed, the OSD CIO collaborates with the service provider and reports progress and elevates issues to the working group.

PERFORMANCE METRICS

Performance metrics play a crucial role in quantifying the health and status of the OSD IT environment. Well-considered metrics provide valuable insights for strategic decision making when it comes to resource allocation and planning for new initiatives. Presently, many operational metrics are monitored to assess operational status, but there is a notable absence of metrics linked to the overall customer experience and business objectives. In recent years, OSD has invested resources in dashboards and data visualization tools. However, the relevance of these tools depends on the accuracy of the data sources and the information being captured. The OSD CIO is currently capturing metrics around technology, project management, and customer satisfaction. As the OSD CIO continues to drive mission initiatives forward, they will continue to employ various methods to capture performance metrics.

Detailed descriptions of OSD IT performance metrics for common IT products and services can be found in the OSD MOA for common IT services. Project management and IT performance data will be collected throughout the execution of mission initiatives. OSD CIO will build upon its effort to capture the overall OSD IT user experience through user surveys, refining and expanding the metric collection while ensuring that metrics are tied to business outcomes. End user experience data will be collected through the deployment of new enterprise data collection tools, tracked through the established OSD governance forums, and used to inform future IT requirements, resourcing, and priority initiatives.

All performance data will be collected, analyzed, and reported through collaborative efforts with the OITEC, the OITEC Working Group, and the PACC, as well as in the OSD CIO Annual Report.

APPENDIX B: PROGRESS AGAINST OSD IT GOALS

To achieve the desired business outcomes described in the OSD IT Digital Modernization Roadmap, the OSD CIO set three goals: flip IT delivery model from service provider-led to customer-led, treat OSD as an IT enterprise, and maximize use of technology to support the OSD mission. These goals, outlined in the February 2023 OSD IT Implementation Plan, play a crucial role in shaping the operational framework of the OSD CIO. Each of these goals is designed to address specific issues identified in the OSD IT study, forming the cornerstone for the effective execution, assessment, and allocation of resources to mission objectives and priorities.

GOAL 1: FLIP IT DELIVERY MODEL FROM SERVICE PROVIDER-LED TO CUSTOMER-LED

The OSD IT study revealed instances of customer dissatisfaction and disparities in IT service provision within the OSD enterprise. The primary objective of the OSD IT enterprise was to transform the approach to delivering IT services to OSD customers. In our inaugural year of service, our primary focus was to shift the IT service delivery model from being provider-driven to customer-driven. This shift involved placing a higher emphasis on understanding and addressing the needs and concerns of our customers. We employed customer-centric communication to identify their requirements and established a governance structure dedicated to advocating for their needs. While our initiatives may originate from various sources, our foremost and enduring source of inspiration for future strategic planning lies in meeting the needs of our customers and addressing their pain points. Remaining attuned to the ever-changing landscape of OSD IT enterprise requirements enables the OSD CIO to achieve its goals of providing cutting-edge technologies that align with OSD IT enterprise objectives and offering tools that enhance the mobile and remote work experience.

User-Centricity: Our North Star in OSD Modernization

The OSD CIO recognizes the importance of prioritizing user experience when providing products and services, understanding that this approach is essential for enabling solutions that are not only functional but also widely embraced. It ensures that what is provided to users meets their needs and expectations. To ensure they have an accurate and comprehensive understanding of user needs, the OSD CIO engages with customers in multiple ways to ensure that users at every level of the organization are heard and their technology needs are acknowledged and satisfied. Some of the methods used are outlined below.

PSA 1v1 Listening Sessions

The Deputy OSD CIO conducts monthly one-on-one sessions with her peers in OSD Component organizations to gather their concerns and issues around IT. These sessions offer valuable insights into how senior leaders utilize technology in ways distinct from other members of their organizations and the specific technology and IT expertise required to meet their missions.

IT Management 1v1 Listening Sessions

OSD CIO action officers meet monthly with IT managers from individual OSD IT enterprise Components. These meetings serve to answer questions, capture concerns, and facilitate communication between the IT managers and the service provider, as necessary. Typically, any issues stemming from these sessions are directly handled by OSD CIO action officers, but sometimes common issues arise from the various OSD Components in these sessions. When that happens, the OSD CIO action officers raise the issue at the monthly OITEC Working Group to determine if the issue is widespread and should be addressed through the governance process.

OITEC Working Group

The working group convenes monthly and typically includes IT managers from every OSD Component organization, along with representatives from the service provider. This collective body makes the initial assessment of all shared IT requirements and handles any issues that might emerge within their respective organizations due to the implementation of DoD enterprise IT initiatives. Additionally, the working group manages a Microsoft Teams channel dedicated to the exchange of documents and information.

User Surveys

The OSD CIO sends out short user experience surveys to the general OSD IT enterprise community. Each month, ten percent of OSD users are randomly selected to participate in the survey, and their responses are collected for tracking and analyzing trends in the overall user experience. The data from these surveys are analyzed annually to identify patterns and trends and to assist in the refinement of survey questions for the following year.

The OSD CIO analyzes its customer communication methods regularly to assess their adequacy and effectiveness and determine whether they require addition, modification, or replacement.

GOAL 2: TREAT OSD AS AN IT ENTERPRISE

When the DSD established the OSD CIO office, one of the chief goals was for the OSD CIO to transform the disperse OSD Components into a single enterprise. The DSD recognized that the collective OSD enterprise would bring more power to bear in solving OSD problems than would 17 individual PSAs and 6 DAFAs. Each new mission priority is addressed and solved as an enterprise requirement, driving a distinct culture change within OSD. As the OSD CIO continues to shape the OSD IT enterprise, they will address key areas for development to enable the OSD CIO to continue driving modernization: the OSD IT enterprise ecosystem, OSD IT resourcing, and OSD IT cybersecurity. Without a firm infrastructure, appropriate funding, and a strong cyber footprint, the OSD IT enterprise cannot be successful at representing its collective interests.

GOAL 3: MAXIMIZE THE USE OF TECHNOLOGY TO SUPPORT THE OSD MISSION

As the Department rolls out new technology for the DoD workforce, it can be challenging for employees to stay on top of the capabilities available to them, much less how to use them. DoD365 was implemented in 2021, and basic capabilities have been available and in use since. But as new capabilities continue to be made available by DISA, the general workforce has little easy visibility of these capabilities and even less visibility in how to use them. Providing access to technology is certainly one mission objective for OSD CIO, but helping OSD users understand the full benefit of the technology available to them will increase productivity, increase the speed of daily mission tasks, and foster collaboration in new and exciting ways. The OSD CIO envisions a workplace where users feel supported when technology capabilities change and know where to get their questions answered.

OSD CIO has developed a DoD365 Campaign Plan and is partnering with DISA and Microsoft to make OSD IT enterprise users aware of the full set of DoD365 capabilities available to them, where they can access training aids, and who can answer their questions or model how to use a specific capability. As new enterprise capabilities are introduced, the OSD CIO will communicate with users to understand the transition to the new tool or service, the timeline for the transition, and resources available to smooth the shift to new technology. The OSD IT Annual Report for 2023 contains information regarding ongoing efforts the OSD CIO has undertaken to maximize the use of technology.

APPENDIX C: CONSOLIDATED SCHEDULE OF MODERNIZATION ACTIVITIES

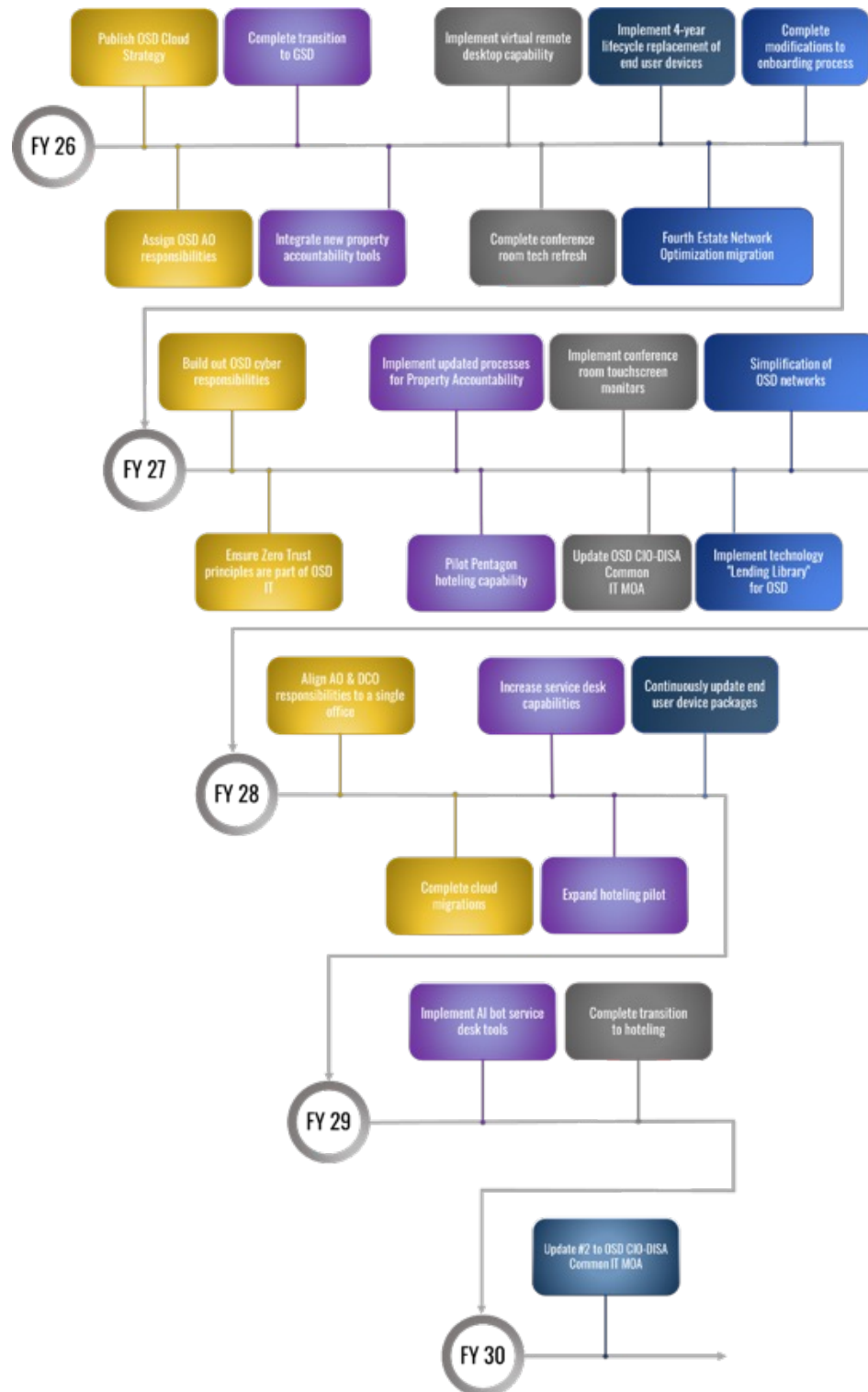The figure below illustrates all planned modernization activities addressed in this roadmap.

FIGURE 12: Consolidated Schedule of Modernization Activities

OSDCIO | CHIEF
INFORMATION
OFFICER