DEFENSE BUSINESS BOARD

Business Excellence in Defense of the Nation

DBB FY23-02

RECOMMENDATIONS TO IMPROVE IT USER EXPERIENCE WITHIN DOD

February 02, 2023

An independent report analyzing and evaluating DoD's current IT architecture and developing recommendations to improve these frameworks across the Department.

Table of Contents

Executive Summary

Tasking: On 9 May 2022, the Deputy Secretary of Defense (DSD) tasked the Defense Business Board (the "Board" or the "DBB"), through its Business Operations Advisory Subcommittee (the "Subcommittee"), with preparing an independent report (the "Report" or the "Study") to provide recommendations to improve the user experience for basic Information Technology (IT) services within the Department of Defense (the "Department" or the "DoD") on the Non-Classified Internet Protocol Router Network (NIPRNET). The Subcommittee results within this Report specifically focus on IT users' ability to efficiently authenticate on the network, access their Non-Classified Internet Protocol Router (NIPR) emails, and effectively use the Microsoft suite of applications and collaboration tools. The Terms of Reference (ToR) provided by the Deputy Secretary of Defense directed the following tasks:

- Identify industry organizational and technical best practices and user experience frameworks to maintain a positive user experience that facilitates productivity;
- Evaluate the current state of DoD user experience for basic IT services across the Department;
- Provide case studies and distilling best practices from relevant private sector companies on how they maintain and enhance their employees' IT user experience;
- Develop recommendations to manage and improve DoD user experience for basic IT services across the Department; and
- Include any related matters the Board determines relevant to this task.

Approach and Methodology: Twenty-first-century military operations require an agile information environment to achieve an information advantage for personnel, their units, and mission partners. To gain the information advantage, everyone in DoD must be able to access the information resources required to perform their functions on any computer on DoD networks anywhere in the world, consistent with security classification and special access restrictions. To address the concerns in the ToR, the nine-member Subcommittee, with the support of the DBB staff, performed a six-month Study to understand the DoD IT landscape better, to evaluate indicators for applicability, and to validate perspectives. In addition, the Subcommittee conducted formal interviews with more than 29 IT industry professionals, including:

- Past and present DoD senior leaders inside the IT community;
- Chief Information Officers (CIOs), Chief Executive Officers (CEOs), and Chief Operating Officers (COOs) from top U.S. companies recognized for their IT capability and expertise; and
- Academic professionals specializing in analytics, the Chief Data Officer (CDO) role, and data governance models.

Survey questions and responses were analyzed from 20,000 participants within an approved Interactive Customer Evaluation (ICE) IT Satisfaction survey for all end-to-end supported Joint Service Provider (JSP) users in the Washington National Capital Region (NCR).[1] The survey provided current quantitative and qualitative IT user-experience satisfaction feedback. While this survey covered only a small sample size of the overall DoD IT user population, it provided valuable insight into issues plaguing the nucleus of headquarters elements and agencies for the Department.

A literature review analyzed data to ground assumptions and to provide context for this Study's findings, including more than 100 published articles, academic journals, previous DoD studies, business case studies, and other literary items.

Background: The DoD is America's largest government agency, with over 3.4 million military service members and civilian personnel operating around the clock at 4,800 sites across 160 different countries and an annual budget of $816.7 billion.[2] By most measures, it is the largest, most complex enterprise spanning the globe. The scope and scale of the DoD make managing business operations at the enterprise level a massive undertaking – akin to running a country, given that the Department's economy equals that of the 21st largest in the world (gross domestic product).[3] An organization of this magnitude must ensure it provides the requisite IT infrastructure, networks, devices, and software applications, so the men and women of the DoD are fully equipped to properly carry out the most sophisticated and routine tasks to accomplish their jobs and support the DoD's mission to provide combat-capable military forces needed to deter war and to protect the security of our nation.[4] To accomplish this mission, the DoD operates 24/7/365 and must always be ready to act on information promptly and effectively.

The Department operates one of the world's largest and most complex sets of networks with a budget of more than $56.6 billion in FY22, roughly ten-thousand operational systems, thousands of data centers, tens of thousands of servers, millions of computers and IT devices, and hundreds of thousands of commercial mobile devices. The Department's networks must be mobile enough to support missions worldwide and flexible enough to facilitate collaboration with any partners a task requires, expected or unexpected.[5]

Today, the DoD's IT capabilities and services are not meeting expectations, and as a result, the user experience is simply not what it needs to be nor on par with industry standards. In accordance with industry standards, a recent Gartner Research noted "A computer that saves an employee ten minutes a day, including boot-up, logging in, opening apps, shutting down, and running security software efficiently, will save roughly 40 hours a year per end user. If applied to DoD the annual savings for resolving these productivity issues would be $548M per year. For the past few years, an increasing

---

1 Washington Headquarters Services. "JSP, Interactive Customer Evaluation IT Satisfaction Survey." November 17, 2022.

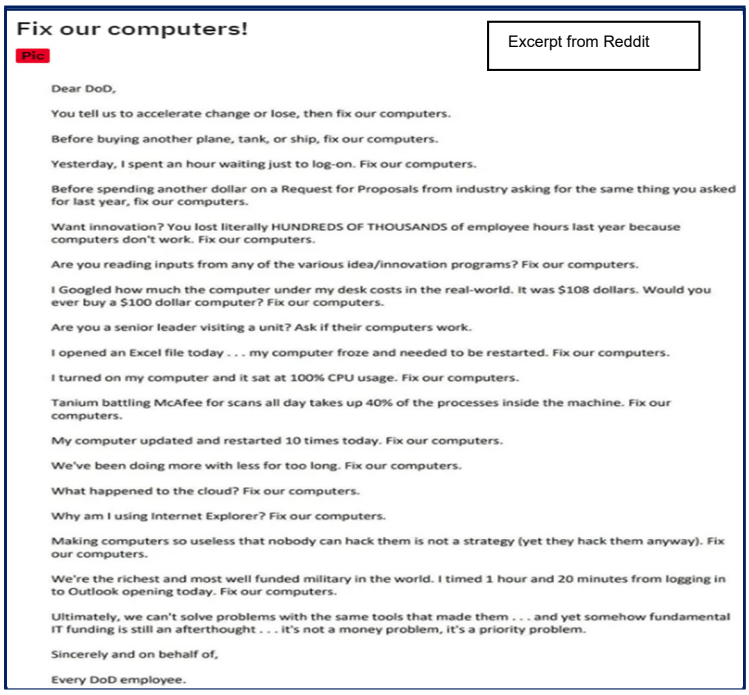
2 U.S. Department of Defense. About. Retrieved November 7, 2022. https://www.defense.gov/About.

3 The World Bank. "GDP (current US$) Data." Retrieved December 3, 2022. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

4 U.S. Department of Defense. Mission Statement. Retrieved November 5, 2022. https://www.defense.gov/About.

5 Department of Defense Information Resource Management Strategic Plan FY19-23. "DOD Digital Modernization Strategy 2019." Page 7. July 12, 2019. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

number of complaints from current and former DoD employees have highlighted, on various social media platforms, from Reddit to Linkedin, their frustration with the state of IT and the IT department's poor customer experience. Further, survey data gathered for this report confirms this untenable reality.



Fix our computers!

Pic

Excerpt from Reddit

Dear DoD,

You tell us to accelerate change or lose, then fix our computers.

Before buying another plane, tank, or ship, fix our computers.

Yesterday, I spent an hour waiting just to log-on. Fix our computers.

Before spending another dollar on a Request for Proposals from industry asking for the same thing you asked for last year, fix our computers.

Want innovation? You lost literally HUNDREDS OF THOUSANDS of employee hours last year because computers don't work. Fix our computers.

Are you reading inputs from any of the various idea/innovation programs? Fix our computers.

I Googled how much the computer under my desk costs in the real-world. It was $108 dollars. Would you ever buy a $100 dollar computer? Fix our computers.

Are you a senior leader visiting a unit? Ask if their computers work.

I opened an Excel file today . . . my computer froze and needed to be restarted. Fix our computers.

I turned on my computer and it sat at 100% CPU usage. Fix our computers.

Tanium battling McAfee for scans all day takes up 40% of the processes inside the machine. Fix our computers.

My computer updated and restarted 10 times today. Fix our computers.

We've been doing more with less for too long. Fix our computers.

What happened to the cloud? Fix our computers.

Why am I using Internet Explorer? Fix our computers.

Making computers so useless that nobody can hack them is not a strategy (yet they hack them anyway). Fix our computers.

We're the richest and most well funded military in the world. I timed 1 hour and 20 minutes from logging in to Outlook opening today. Fix our computers.

Ultimately, we can't solve problems with the same tools that made them . . . and yet somehow fundamental IT funding is still an afterthought . . . it's not a money problem, it's a priority problem.

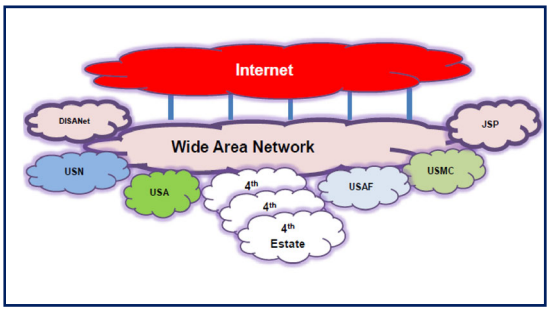
Sincerely and on behalf of,

Every DoD employee.

Moreover, since the Department measures the user experience for a limited set of its customers, it tends to problem-solve in a reactionary rather than proactive manner.

While there has been much discussion in recent years, at all levels of the Department, over the state of DoD's IT capabilities, it remains true that IT is not yet seen nor treated as the priority it must be. Indeed, given that IT is essential to virtually every operation the DoD performs, leadership at every level must finally focus on delivering a world-class user experience.[6]

In recent years, the DoD has invested substantial resources and improvements in building critical IT capabilities; however, it has not provided a consistently high-quality user experience across the enterprise. The overall enterprise is comprised of numerous interconnected stakeholder clouds that intersect, overlap, run parallel, and ride atop one another to connect end-user devices to a network. Additionally, global events, such as the COVID-19 pandemic, radically changed how the DoD conducts its routine business and how it adapts to how employees work globally. As a result, many DoD organizations mandated the switch from a pure office to a distributed remote setting.[7] The pandemic further magnified the need for, and challenge in, providing exceptional user experiences and a better understanding of IT user experiences to proactively predict and resolve issues, enabling employees to efficiently and effectively deliver on their missions.



Observations:

6 Reddit.com. "Fix our computers!" March 2022. https://www.reddit.com/r/Military/comments/sdlvk7/fix_our_computers.

7 U.S. Department of Defense. Press Release. November 30, 2020. "DOD Guidance on Extension of Maximum Telework Flexibilities." https://www.defense.gov/News/Releases/Release/Article/2430245/dod-guidance-on-extension-of-maximum-telework-flexibilities.

1. DoD has not provided a high-quality or a reliable end-user experience for all IT users, nor does it routinely measure and share data around the user experience or its impact on worker productivity or mission efficiency;
2. Basic IT services are widely disconnected and not managed/owned from initial planning through acquisition through end of life by one singular entity down to the endpoint device, resulting in inefficiency in providing consistent, high-quality experience;
3. Operational and mission-support functions are prioritized over IT support services;
4. The Department has dedicated and committed military and civilian personnel across its many IT departments who share a desire to improve delivery, reliability, and quality of IT User Experience. However, ongoing efforts within the Department to attract, retain, and develop IT service talent remains highly challenging, and significant workforce gaps persist; and
5. Enterprise IT support services require immediate and sustained leadership attention with more accountability, reliable levels of IT-related funding, and higher levels of coordination across DoD IT departments.

Key Findings:

- Key Finding #1: DoD Lacks Actionable Performance Metrics for Enterprise IT User Experiences
- Key Finding #2: 80% of Survey Respondents Rate User Experience Average or Below
- Key Finding #3: Insufficient Infrastructure to Proactively Isolate and to Resolve Performance Issues
- Key Finding #4: Broad Endpoint Disparities in and Among User Groups
- Key Finding #5: Varied and Siloed IT Policies Cause Inefficiencies Across the DoD
- Key Finding #6: Redundant Deployment of Security and Cybersecurity Tools
- Key Finding #7: Insufficient IT Funding & Lagging Acquisition Implementation
- Key Finding #8: MILDEP Approach the IT User Experience & Effectiveness Differently

Recommendations:

- Rec #1: Implement Endpoint Monitoring Across ALL Devices and Prioritize DOD IT Funding to Consistently Monitor and to Improve End-user Experience
- Rec #2: Leverage Metrics for IT User Experience to Drive Accountability from Service Providers and to Deliver Acceptable Quality of Service

- Rec #3: Review and Upgrade Device Replacement Strategy and Device Life Cycle Management
- Rec #4: Simplify Security Layers, Move Faster to Zero Trust/Application-Level Security
- Rec #5: Establish/Designate Permanent Chief Experience Officers
- Rec #6: Centralize Acquisition and Vendor Negotiations Where Possible
- Rec #7: Streamline, Standardize, and Consolidate Help Desks Across the DoD
- Rec #8: Centralize Reference Architecture, Network, and Security Standards Under DoD CIO and Federate Delivery and User Experience Accountability to the MILDEP CIOs
- Rec #9: Clearly Define DISA's Role in the Unclassified User Experience

The Board also notes that Congress has explicitly recognized many similar challenges this report identified. The FY 2023 National Defense Authorization Act includes specific language and required actions that, in the main, align well with the findings and conclusions in this Report. This law presents a genuine opportunity for the Department to capitalize on congressional interest and potentially collaborate on meaningful, forward-leaning solutions.

Final Comments: The Subcommittee appreciates the confidence the Deputy Secretary of Defense shows in entrusting it with this critical Study. In addition, the Subcommittee sincerely recognizes the hardworking people of the Department of Defense that generate, curate, and manage its information technology and digital modernization initiatives. The Subcommittee hopes this report is helpful in improving the delivery of IT services and the IT user experience of all those in the Department.

The full DBB approved the observations and recommendations on February 2, 2023.

Respectfully submitted,

David Beitel

Subcommittee Chair

Preface

This Study, DBB FY23-03, Recommendations to Improve the IT User Experience on NIPR, is a product of the DBB. Recommendations provided herein by the DBB are offered as advice to the DoD and do not represent DoD policy.

The DBB is a federal advisory committee established by the Secretary of Defense in 2002 to provide the Secretary and Deputy Secretary of Defense with independent advice and recommendations on applying "best business practices" from the private sector's perspective to the overall management and business processes of the DoD. The DBB's members, appointed by the Secretary of Defense, are senior corporate leaders with demonstrated executive-level management and governance expertise.

DBB members possess a proven record of sound judgment in leading or governing large, complex organizations. Members apply experience in examining issues and creating reliable and actionable solutions to complex management issues guided by proven best business practices. All DBB members volunteer their time to this mission.

The management of this Study was authorized and governed by the Federal Advisory Committee Act of 1972 (5 U.S.C., Appendix, as amended) and governed by the Government in the Sunshine Act of 1976 (5 U.S.C. § 552b, as amended), 41 CFR 102-3.140, and other appropriate federal and DoD regulations.

Observations

"Government must be held accountable for designing and delivering services with a focus on the actual experience of the people whom it is meant to serve."

~ President Joe Biden, 13 December 2021[8]

The DoD understands its IT infrastructure and systems are essential to maintaining its warfighting superiority, as demonstrated through its substantial investment in this critical capability. However, DoD IT has not provided a consistent, high-quality end-user experience to its more than 3.4 million users. Unreliability has led to frustration; impacted productivity due to unacceptable login times and undependable access to basic applications; and resulted in attrition within the DoD. **The frustration was explicitly called out in an open letter from a senior official to DoD on Linkedin, resigning due to many issues ranging from 100% CPU usage, ten or more reboots, and 80 minutes to log into Outlook.**[9] Further, the Department does not consistently conduct and share regular user-experience analysis or consistently prioritize those analyses in resource planning.

Suboptimal Services: The Department of Defense is responsible for the most critical and time-sensitive missions of any government agency. As such, it only stands to reason that the Department must provide the resources, personnel, and equipment capabilities to meet and overcome any foe, anytime, anyplace. Unfortunately, **it is clear that when it comes to basic information technology and the attendant user experience, the Department is delivering sub-optimal or failing services that, in turn, drain essential resources from other needs and sub-optimize or can threaten mission execution**. In short, while IT is mission-critical, it is too often treated as just another support service. That cannot be allowed to stand.

Examples of Inefficiencies:

- In a November 2022 DBB survey, out of more than 3,500 respondents (spanning a cross-section of users from the services and the Department), 40% noted it took them five minutes or longer to power up/wake up their computers to enable access to basic office applications.[10] Industry averages are 10-30 seconds and faster on newer devices. **At once a day, five minutes equates to 22 hours (nearly three work days) a year per user waiting for access**;[11]

---

8 The White House. "Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government." December 13, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/

9 Kannan, Michael. Linkedin.com. "Michael Kannan's Post." February 2022. https://www.linkedin.com/posts/michaeljkanaan_technology-future-innovation-activity-6891726752759074816-2qCv.

Washington Headquarters Services. "JSP, Interactive Customer Evaluation IT Satisfaction Survey." November 17, 2022.

Office of Personnel Management. Policy, Data, Oversight. "Fact Sheet: Computing Hourly Rates of Pay Using the 2,087-Hour Divisor." Retrieved January 8, 2023. https://www.opm.gov/policy-data-oversight/pay-leave/pay-administration/fact-sheets/computing-hourly-rates-of-pay-using-the-2087-hour-divisor.

10

11

- In that same survey, 70% of respondents reported they had to re-authenticate their Common Access Card (CAC) multiple times a day compared to industry standards of once a day on average;
- One OSD office reported waiting 30 days for a laptop for a new hire, even though the Service Level Agreement (SLA) governing such purchases required no more than a 48-hour turnaround; and
- Most large DoD departments and agencies the Subcommittee interviewed revealed inconsistently defined and followed endpoint refresh strategies, incomplete inventory management systems, and indeterminate amounts of deployed hardware over four years of age.

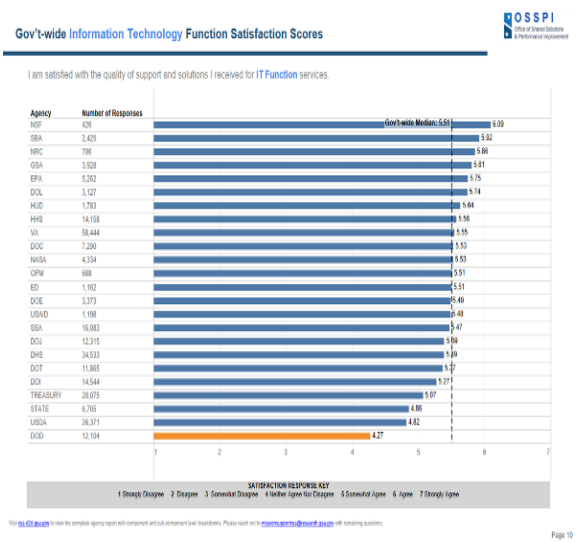
In simple terms, through 29 interviews, survey data, literature reviews, and informational resources, it is clear to the Subcommittee that **the Department's basic IT services are widely disconnected, inconsistent, and in severe need of immediate and sustained leadership attention.** Moreover, it is unclear how the available levers of accountability are being utilized to ensure that performance meets expectations. Additionally, the issues are endemic, are associated with all aspects of the IT user experience, and are not solely grounded in the unique challenges that emerged during the pandemic. Indeed, in the above-referenced survey, the user experience for those working remotely (full-time or part-time) was no worse than those working on-site. Moreover, while the survey results are associated explicitly with customers of the Defense Information Systems Agency (DISA) JSP outside sources such as, Facebook posts, Reddit articles, and our interviews support similar frustrations and poor performance in the Military Departments that are not JSP customers. To be fair, there are new, promising initiatives intended to change the course of users' experiences and satisfaction significantly. But while promising, these initiatives are Military Departments (MILDEP)-specific and are not a part of a unified, common enterprise-wide IT strategy. As promising and well intentioned as they may be, it is also possible, even likely, that their continued disconnection from a unified strategy could perpetuate or exacerbate other enterprise IT challenges.

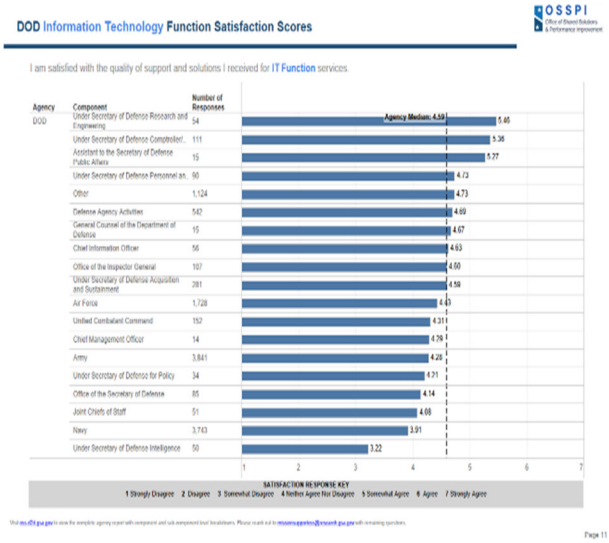
General Services Administration (GSA) Survey Satisfaction Results: In March 2022, the GSA surveyed more than 260,000 federal employees at the CFO-Act agencies to assess their satisfaction with mission-support services during the previous 12 months.[12] The primary population, GS-13 and above supervisors, received the entire survey. In contrast, the rest of the survey population received a subset of questions on the IT functions and IT commodity service areas. Collectively, responses provided a detailed picture of customer satisfaction for 24 service areas across the Contracting, Financial Management, Human Capital, and IT functions. In addition, respondents across all government agencies ranked their satisfaction with the quality of support and solutions they received for IT function services on a scale of 1 (strongly disagree) to 7 (strongly agree). The government-wide satisfaction median was 5.51 (somewhat agree +). The

[12] U.S. General Services Administration. "GSA Survey Satisfaction Results." March 2022. www.gsa.gov/reference/reports.

DoD's response average was 4.27 (neither agree nor disagree), down from 4.41 in 2021, and ranked last across all government agencies surveyed.[13]

Lastly, the level of satisfaction with support and solutions received for IT function services for all MILDEPs, components, Combatant commanders, Under Secretary of Defense for Policy, Office of the Secretary of Defense (OSD), Joint Chiefs of Staff, and Under Secretary of Defense Intelligence were all below the median agency satisfaction level.





How does the Department improve the Non-classified Internet Protocol Wide Area Network IT user experience? Specifically, the DoD must focus on recommendations to efficiently enhance the IT-user's ability to authenticate on the device and the network, easily access NIPR emails, and efficiently use the Microsoft suite of applications and collaboration tools. Also, those efforts must be routinely assessed, with the data and metrics shared across all relevant functions and leadership.

It is clear that while there are pockets of excellence that are focused on improving the end-user experience within the DoD, these practices are often in early pilot stages and not replicated across the Department in a unified enterprise strategy (see Key Finding #8 and Recommendation #5). Therefore, this Study recommends strategic DoD-wide improvements across services, components, and agencies to provide a consistent and measurable end-user experience.

[13] U.S. General Services Administration. "GSA FY 2022-2026 Strategic Plan." Retrieved December 12, 2022. www.gsa.gov/reference/reports/budget-performance/gsa-fy-20222026-strategic-plan.

Key Findings

Key Finding #1: DoD Lacks Actionable Performance Metrics for Enterprise IT User Experiences

Central to providing and improving any service is to have a:

- Well-defined customer or user base utilizing that service;
- A clear understanding of the needs of the customer being served;
- Complete set of metrics to measure the successful delivery and usefulness of service; and
- Review those critical metrics at the appropriate organizational level with a clearly defined Service Level Agreement.

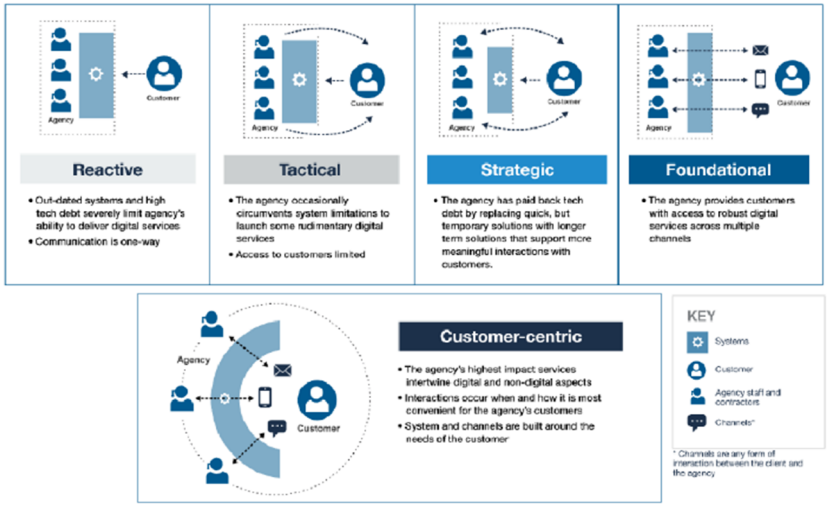
Customer Experience Maturity Model (CEMM): Essential to any effort to enhance a customer-facing service is understanding the customer experience and, as is the case in this study, the IT-user experience (IT UX). As described in the CEMM graphic below, those that do not demonstrate consistent expertise or that lack the service level awareness, bi-directional communication, structure, and flexibility required for exceptional digital services are usually at the lowest levels of the model.[14]

Because there is a lack of an IT user experience definition and a multiple-ownership model across the DoD, each federal agency fits into one of the five levels of user/customer-experience maturity:

- Reactive: Agencies with a rudimentary understanding of their customers;
- Tactical: Agencies with occasional forays into customer research, usually as part of larger IT projects;
- Strategic: Agencies with enough customer-related initiatives to warrant aligning research and analysis efforts;
- Foundational: Agencies with coordinated customer experience efforts designed intentionally to fit within well-articulated strategies; and
- Customer-centric: Agencies with structured, measurable goals and metrics that satisfy customers' needs.

[14] CentreofExcellence.com. "Customer Maturity Model." Page 13. Retrieved December 22, 2022. https://www.centreofexcellence.com.

How agencies at different levels of CX maturity deliver digital services

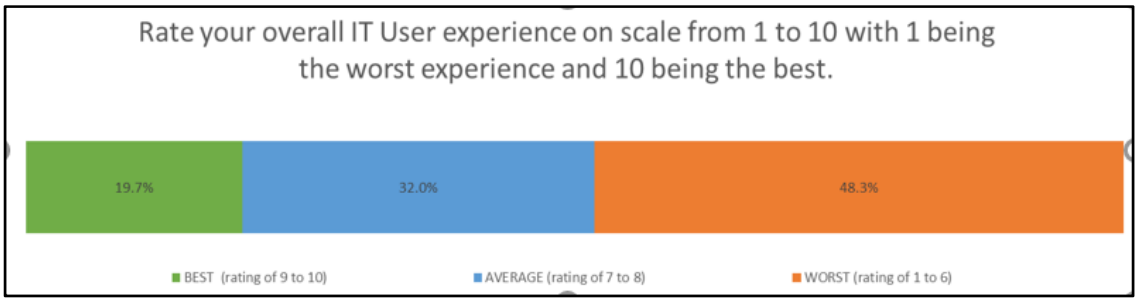


Based on the assessment of the Subcommittee, DoD as an enterprise is presently in the Reactive Phase according to the CX Maturity Model. The DoD has varying levels and specific definitions of service and customer experience across the technical offerings. Additionally, there are **inconsistent, incomplete, and, sometimes, missing sets of metrics used to assess the customer experience end-to-end**, often relying on weak and conflicting definitions, including help desk tickets, infrequent survey responses, and anecdotal reports. **There is a distinct lack of endpoint monitoring across the entire DoD, limiting the Department's ability to assess endpoint computer device performance accurately.** Interviews with the Defense Information Systems Agency, MILDEPs, and agencies acknowledge no basic definition for understanding the user experience. Furthermore, across DoD, there is no agreed-upon definition or promise returned back to the customer detailing a commitment of expectations for a successful customer experience or accountability from the provider. **Without a clear single definition across all user groups and reportable backup to leadership in an aggregate and actionable format, the Department cannot effectively measure, action, or improve end-user experience**.

Key Finding #2: 80% of Survey Respondents Rate User Experience Average or Below

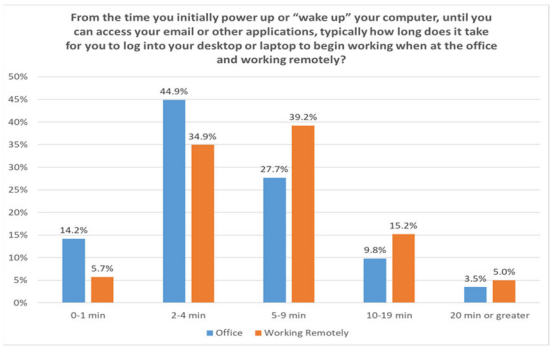
To better understand the state of user satisfaction with basic IT services, the Subcommittee surveyed more than 20,000 users. Due to the size and scope of the Department, the Subcommittee limited this particular effort to Joint Services Provider customers.[15] As a result, user satisfaction is nowhere near the level needed to meet Department mission goals effectively. While the population surveyed and the response rate was robust, the survey's limited organizational scope confines the extrapolation of its results across the broad range of services, components, and agencies not included. That is not to say that user satisfaction in those components is either better or worse than those surveyed. It does, however, argue for further user satisfaction assessments in those components not.

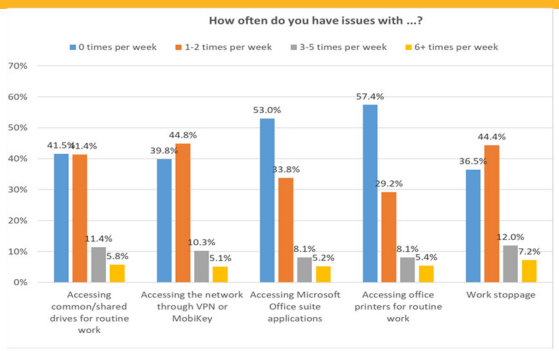
Work Stoppage: The survey highlighted a core problem for DoD. **Less than 20% of respondents rated their experience "above average."** Particular concerns focused on what should be the simplest of activities - log-on times, ticket frequency, IT-driven work stoppages, re-authentication frequency, etc. Yet, those who have been working remotely frequently reported similar satisfaction to those who are working on-site. On the one hand, this suggests that the Department deserves great credit for having pivoted effectively during the pandemic. But, on the other hand, it also makes it eminently clear that user satisfaction problems are endemic.



Further, the Subcommittee suggests that the productivity losses and the commensurate mission impacts associated with sub-optimal IT performance are genuine, as evidenced by the data, including the number of IT-driven work stoppages, excessive login times, etc. The Subcommittee recognizes the nature of government is such that it is not likely feasible

[15] Washington Headquarters Services. "JSP, Interactive Customer Evaluation IT Satisfaction Survey." November 17, 2022.





to assess productivity impacts in the same way, a commercial entity might. However, it is nonetheless present and impactful and must be part of the resource decision processes.

Intel Corporation Survey – 42 Hours Per Computer Per Year Lost Productivity: In two surveys conducted by Intel Corporation in 2014 and 2018 across five countries, **employees were 20.82% less productive on PCs older than five years**, costing employers $12,495 per year per computer user, specifically, in lost productivity. That results in **an average of 42 work hours per computer per year downtime** on old computers while being repaired or operating slowly and inefficiently for various work-stoppage issues.[16]

User Experience Common Standards: Unfortunately, there have been no enterprise-wide readily identifiable, consistent, transparent, and comprehensive user satisfaction assessments in the DoD. While some efforts have made strides in the right direction, they remain too disaggregated and disconnected to have a systemic impact. Although it may be very challenging to conduct a single assessment across an institution as large and complex as DoD, there are no common standards of customer satisfaction and experience against which components can measure and report.

Finally, the **survey results strongly suggest that most DoD employees and uniformed service members have come to expect sub-optimal IT services as the norm, even though the commercial world does not accept this performance.** And in the view of the Subcommittee, given the centrality of IT to virtually every aspect of the Department's operations and missions, it should also be intolerable in DoD. Appendix F shows a summary of the survey results.

[16] Douglas, Robert. Planet Magpie. "How Often Should You Replace Your Company PCs?" August 7, 2018. www.planetmagpie.com/news/woof-newsletter/2018/08/07/how-often-should-you-replace-your-company-pcs.

Key Finding #3: Insufficient Infrastructure to Proactively Isolate and to Resolve Performance Issues

The Subcommittee interviews with senior-level DoD IT leadership revealed **insufficient coordination, technology, and authority across the DoD enterprise to effectively monitor the IT end-user experience, including device, network, and productivity application performance.** For example, although some network monitoring is in place at DISA, the data is not captured in an overall user-experience framework. Additionally, the Subcommittee could not find evidence that it is reviewed by anyone outside of the DISA help desk or used for decision-making or investment prioritization. The lack of accurate and timely monitoring of end-user devices limits the Department's ability to consistently and proactively isolate performance issues and, ultimately, makes it difficult to provide efficient and effective IT services.

Help Desks: The DoD operates over a hundred individual help desks worldwide that similarly conduct their functions. However, because DISA does not provide the last mile of transport or manage quality of service (QoS) over the entire path, service management, endpoint devices, and various support services, like help desks, are under the control of multiple MILDEPs, Combatant Commanders (COCOMs), and agencies. It is inefficient and costly to staff, operate, and maintain this structure. According to a senior government official, an overarching goal of the DoD is to move everyone to a single-tenant, single-monitoring system. Reportedly, Microsoft has expanded the size of a single-tenant installation it can support; however, this has never been deployed and tested with the DoD and with the number of users therein. Support for a multi-tenant installation with configured interoperability is, however, available for DoD use.

According to a senior government official, the purpose of the JSP Service Desk Consolidation initiative is to streamline the assortment of installation-level and organization-level help desks into a single DoD-level Service Desk (e.g., Army-level, Navy-level, Air Force-level, etc.) provided from the DoD cloud. Leveraging IT industry best practices, sharing IT infrastructure, and establishing consolidated Enterprise Service Desks for each COCOM, MILDEP, and agency will eliminate redundant services and capabilities. It will also enable efficient and proactive root-cause analysis and, ultimately, result in hundreds of millions of dollars in savings across the DoD. While there is progress in onboarding DAFAs to the unified Service Desk, no other timeline is available to complete this migration.[17]

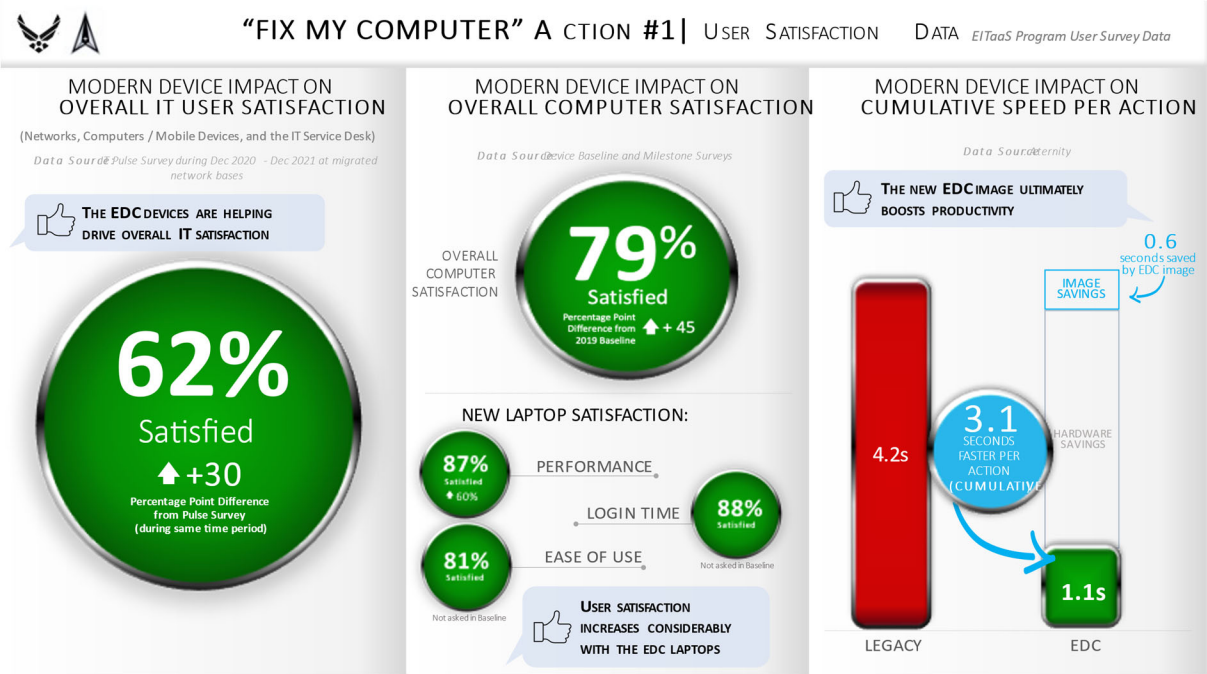
DISA JSP Ticketing Process: In the last six months, with a customer base of approximately 55,000, JSP has responded to more than 160,000 tickets. Inquiries ranged from work orders and commodities requests to device access and security tools, overwhelming capacity to access and operate technology. In one case, according to a senior government official, a user's security tools took up 50-75% of the available CPU

[17] U.S. Department of Defense. "Federal Data Center Consolidation Initiative." November 8, 2011. https://dodcio.defense.gov/Portals/0/Documents/FDCCI-Final-2011.pdf.

bandwidth. Hence, JSP suggested an internal review of how much security is needed, including active scans, to reduce the burden on the local system.

The ticket process is inconsistent due to having multiple help desks that are not standardized or integrated. This inconsistency leads to limited real-time sharing across the various units, thus creating an environment where troubleshooting is primarily reactionary, with little to no predictive analysis.

End User Feedback: Although DISA-controlled services, such as DoD365-Joint, enable feedback mechanisms, there is no DoD-wide comprehensive user feedback loop. The lack of continuous survey feedback prevents an accurate understanding of user experiences and leads to inefficiencies in operations and deliverables. **The DoD's minimal IT metrics are not comprehensive and are not necessarily standardized or designed with a focus on end-user productivity.** Any metrics currently collected are often viewed in isolation and are not part of a broader IT leadership up to the respective CIOs review. However, the **Subcommittee did observe some pockets of best practices, such as the Air Force's more developed and mature processes to measure and report user experience metrics, including hiring and implementing a new Chief Experience Officer (CXO).**



[18]

Other examples include the Global Service Desk (GSD) help desk for JSP and DoDNET/4th Estate Optimization (4ENO), which have feedback mechanisms to help measure user feedback, issues, and impact.[19] The top three problems JSP routinely addresses include connecting to the network, connecting to network drives, and opening applications manifesting issues with the inability to access files. According to a senior

[18] United States Air Force. Metrics. Retrieved December 18, 2022.

[19] Barnett, Jackson. Fedsoop.com. "IT consolidation for military's Fourth Estate agencies is coming next year, officials say." Page 19. December 1, 2020. www.fedscoop.com/dod-fourth-estate-modernization-initiative-disa.

government official, a significant concern is how much work stoppage due to IT issues contribute to lost productivity.

Technology Risks: Without real-time monitoring of end-to-end user experience or the ability for technicians to make adjustments on end-user devices, it is difficult to quantify the current state or to maximize efficiency as it relates to productivity, work stoppage, and lost costs. **Intel Corporation suggests the optimum replacement cycle for a business computer is every three to no more than four years because the total cost of maintenance, troubleshooting, and downtown begins to rise significantly after that.**

Intel PC Life Cycle Study

Downtime Costs *- Downtime costs increase with older computers because they have more problems with both hardware and software. Technology is evolving at a record pace, and many 4-year-old computers no longer have the specifications needed for newer software; this can cause conflicts that take a PC down. Computers over 4-years old have twice the downtime of those that are 3-years old; this means the increasing possibility of more operational disruptions with older computers.*

Rising Maintenance Costs *- Older computers often require more service and maintenance calls to keep them in operation. PCs older than 4-years old have nearly twice the number of annual service calls as those 3-years old. The support calls are also longer, by about 20 minutes more each.*

Productivity Loss *- When an employee waits on a slow computer or spends 40 minutes of the day struggling with an issue and rebooting, that lost productivity can add up fast. Forty-two (42) hours per year in productivity are lost on average on a computer older than four years while an employee is waiting on repairs or service. If an employee is making an average of $28 per hour, that is a loss of $1,176 annually. And this doesn't include the loss of being slowed down. If an employee is slowed down just 30 minutes a day by working on an older computer, that equates to approximately 100+ more hours of lost productivity each year, another $2,800+ in losses*

Data Breach Risk *- A costly risk with older computers is the susceptibility to data breaches and malware infections, and this is largely due to upgrade barriers with an operating system or software as a result of aging out of having the needed specifications to support and update security measures In a 12-month period, Canadian companies reported an 82% increase in the volume of cyberattacks, with PCs older than four years having three times as many security breaches than those computers less than three-years-old.*

Data Loss *- Older computers are shown to have higher data loss incidents, with older than four-year old computers suffering data loss three times more than those younger than 3-years old. As PCs age, they often begin having hard drive problems which can lead to crashes. When a hard drive on a computer syncing with a cloud storage software (which is not the same as a cloud backup) crashes, there is the potential for lost cloud storage files.*[20]

Metrics: In addition to measuring end-user experience, most private companies also measure employee IT-related satisfaction because companies simply cannot afford to lose productivity due to IT-related issues. However, research indicates that IT-related issues affecting employee performance are under-reported yearly. For example, one survey from the *Harvard Business Review* showed that the average employee would encounter two IT issues per week, with **a productivity loss of 28 minutes per incident**, while others suggest that the productivity loss rate is even greater. Lack of reporting also drives a disconnect between what IT departments think of their tools and the end user's

20 Haxxess Enterprise Corporation. "How Often Should We Replace Our Business Computers?" Retrieved January 16, 2023. www.haxxess.com/how-often-replace-business-computers.

experience. Interestingly, **84% of surveyed employees believed their organization should be doing more to improve the digital work experience, but 90% of the IT leaders thought their workforce was satisfied with their technology tools**. This gap in perception is particularly problematic because companies cannot afford employee dissatisfaction and attrition risk due to IT challenges.[21]

The breadth and depth of current metric monitoring across DoD are fragmented and largely ineffective. For example, there are some examples of detailed network monitoring at DISA, some fairly robust user-experience monitoring at the Air Force, and pockets of network monitoring across MILDEPs, agencies, and components. However, this fragmented monitoring does not allow for data analysis-based assessment of the end-user experience, limits the ability to target high-impact areas for correction, and prevents a proactive approach to problem-solving before consistent, possibly predictable issues.

Endpoint Monitoring: It is critical to measure what matters from the right point of view; employee experience significantly impacts productivity. There is reportedly some interest across the DoD in using standardized software that provides telemetry monitoring on endpoint devices to evaluate performance, application level, security, and system-level data. Telemetry monitoring can help move from a reactionary response to a predictive service, offer different metrics, and provide essential information like maxed-out memory, capacity, and what software uses the most bandwidth.[22] According to a senior government official, JSP has used a commercially available monitoring tool to troubleshoot a select workstations, but it is not consistent or broad enough, is not steadily mined, and has broad licensing issues or restrictions, as cited by numerous sources.

The Subcommittee found little device/computer-level performance and IT user-experience metrics collected throughout the Department. However, the Air Force has successfully managed these metrics on a small subset of devices (~25k users) and used the collected data to measure actual end-user experience, identify IT issues, and adjust roadmaps and budgets based on collected data. **This feedback loop is critical to understanding the actual experience customers are having.** This data can also help uncover devices that need replacing/upgrading, as well as conflicting local applications and security implementations. Therefore, device-level monitoring is necessary to **yield actionable IT user experience metrics and data.**

Net Promoter Score (NPS) Metric: Two-thirds of *Fortune* 1000 companies utilize the Net Promoter Score, a primary measure of customer sentiment; its popularity is rapidly growing globally. As the NPS metric moves onto C-suite dashboards, most agree the value does not come from the number itself but from customer feedback based on that number rating. In 2020, Vanguard CEO reviewed his firm's NPS every time he looked at his management dashboard. California Closets CEO checked his company's score first thing every morning and structured his company's IT strategy on feedback. Intuit product managers checked their company's NPS daily for 17 years. With more than 40,000

[21] Batchelder, Grossman, Martin, Newcomb, Rockart & Yetter. *Harvard Business Review*. "The End of the Delegation? IT and the CEO." September-October 1995. Retrieved hbr.org on October 27, 2022. https://hbr.org/1995/09/the-end-of-delegation-information-technology-and-the-ceo.

[22] https://www.sumologickorea.com/glossary/telemetry.

employees at IBM following its NPS, one executive noted, “It’s more than a metric. One could use the word ‘religion.’”[23]

> ***It’s about understanding what our customers want and need from us…. Even though the score gets all the attention, it’s the second question – ‘Why did you give the score that you gave?’ that delivers the value,”***
>
> ***~ Deborah Campbell, Verizon’s vice president of consumer & marketing insights***[24]

[23] Colvin, Geoff. Fortune.com. “The simple metric that’s taking over big business.” Page 11. June/July 2020. https://fortune.com/longform/net-promoter-score-fortune-500-customer-satisfaction-metric.

[24] Colvin, Geoff. Fortune.com. “The simple metric that’s taking over big business.” Page 11. June/July 2020. https://fortune.com/longform/net-promoter-score-fortune-500-customer-satisfaction-metric.

Key Finding #4: Broad Endpoint Disparities In and Among User Groups

The inconsistent management of endpoint devices results in broad disparities in and among user groups. According to senior government officials, **the Life Cycle Replacement (LCR) plans for IT endpoint devices are inconsistent across the Department**. They are considered a liability in a legacy inventory management system that has created latency for replacement. In other words, far too many DoD personnel are attempting to conduct critical work on substandard equipment. With LCR plans outside the three-year standard, it is challenging to navigate or to fix the issues this presents to end-user productivity.

Antiquated Hardware: The industry standard to replace hardware is 36 months. The Defense Property Accountability System (DPAS), inventory management, and the policy for accounting for hardware are antiquated. IT hardware, and the need to make data-based decisions quickly, necessitates more modern inventory systems, procurement, and delivery methods to ensure the right equipment is available to DoD employees to perform their duties efficiently and effectively. This approach would improve device replacement time and ensure all DoD team members are on a timely hardware release without having to complete two hours of paperwork and supervisory signatures, which is what officials told us is the case now. According to a senior government official, the user experience suffers because IT is not a priority in the overall budget. The Subcommittee could not determine the actual number of devices and funding needed to upgrade all devices outside the recommended life cycle range, through the interviews and research completed.

Device Replacement is a Balancing Act Between a PC's Productive use and Replacement Cost

When to Replace a Company PC? Lack of budget is a common reason why old technology continues to be used; however, while budget is always a valid concern, support costs can quickly outstrip the cost to replace.

As PCs slow down with age, so does productivity decline, support costs increase, and lost time increases. In addition, software becomes outdated, causing poor performance, more frequent freezing, and corruption-eating files; environmental conditions like moisture, heat, and dust wreak havoc on the system inside; connections begin to burn out, fans clog, and components short out.

Productivity-losing issues typically arise in years four and five and after the initial three-year warranty. In addition, replacing a PC is necessary if more than five serious support issues or support calls have increased significantly over the last six months.

A three-year replacement interval schedule for one-third of inventory will help better predict costs, manage upgrades, avoid lost time, and reduce support costs.[25]

IT Inefficiencies: Furthermore, the current state does not fully maximize the current IT technology available or enable full use of collaboration tools, like cameras. In addition, a heavily disparate and antiquated endpoint environment prevents the ability to deploy standard images. A senior government official noted because every machine is unique

25 Douglas, Robert. Planet Magpie. "How Often Should You Replace Your Company PCs?" August 7, 2018. www.planetmagpie.com/news/woof-newsletter/2018/08/07/how-often-should-you-replace-your-company-pcs

in terms of hardware and “software image,” it makes troubleshooting issues extremely difficult. While the subcommittee was unable to get good data on the scale of this problem, anecdotal reports show that it is difficult for the service provider to keep up with premium, isolated systems.

Key Finding #5: Varied and Siloed IT Policies Cause Inefficiencies Across the DoD

Siloed and inconsistent DoD IT policies, ownership, and services deployment (service management, support services, help desk support, etc.) contribute to poor user experience across the Department and the digital workplace.

DoD Authority: DoD does not have a way to manage essential IT across the enterprise. As a result, there are inconsistencies and unreliability in many areas. Not only are some end-user devices well past the recommended life cycle, but there are numerous non-standard configurations, particularly for security. A severely decentralized organizational model with multiple overlapping areas of responsibility exacerbates this challenge leading to a lack of clear accountability for end-to-end user experience. This challenge contributes to multiple approaches across the MILDEPs, agencies, and components on how to solve these issues, and ultimately, a vastly different implementation and resulting user experience across the DoD.

DOD CIO: Every MILDEP, and nearly every Defense organization of any significant size, has its own CIO, which totals approximately 50 across the enterprise.[26] The DoD CIO is appointed by the President and is confirmed by the Senate, with responsibilities for appointed policy, oversight, and guidance of IT & cybersecurity matters and with authority, direction, and control over DISA and the Information Assurance Directorate of the National Security Agency (NSA). The DoD CIO is also responsible for implementing and enforcing a process for developing, adopting, and publishing standards for information technology, networking, and cyber capabilities for all departments and agencies.[27] In addition, each service has a CIO who answers to the secretary of that service and who is responsible for producing a component-level IT architecture, service-level management, and support for the end-user experience.[28]

OSD CIO: Additionally, a new OSD CIO role was developed after a four-month (April-July 2022) study completed by the Director of Administration and Management (DA&M), which yielded findings in three critical themed areas:[29]

1. The lack of clear authorities and governance (for transversal IT services) created a gap in requirements management;
2. Repeated IT consolidations for efficiency purposes resulted in significant resource shortfalls; and

---

[26] Miller, Jason. Federal News Network. "DHS on cusp of hiring as many as 100 CX experts." December 13, 2022. www.federalnewsnetwork.com/hiring-retention/2022/12/dhs-on-cusp-of-hiring-as-many-as-100-cx-experts.

[27] U.S. House of Representatives. (n.d.). 10 USC 142: Chief Information Officer. Office of the Law Revision Counsel United States Code. Retrieved January 11, 2023, https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title10-section142&num=0&edition=prelim#sourcecredit.

[28] U.S. House of Representatives. (n.d.). 44 USC 3506: Federal Agency Responsibilities. Office of the Law Revision Counsel United States Code. Retrieved January 11, 2023, https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title10-section142&num=0&edition=prelim#sourcecredit.

[29] Gill, Jaspreet. Breaking Defense. "OSD gets new IT directorate, own CIO after study found 'degradation' of services. October 14, 2022. https://breakingdefense.com/2022/10/osd-gets-new-it-directorate-own-cio-after-study-found-degradation-of-services.

3. The absence of OSD IT service standardization impacted performance and increased cybersecurity risk.

The OSD CIO role assumed some responsibilities previously held by the DoD CIO and is equivalent in objectives to MILDEPs, agencies, and components CIOs. Currently, the small, fewer than a dozen, OSD CIO office focuses on policy/governance at the OSD level and on ensuring JSP drives the implementation of OSD-prioritized requirements. The Subcommittee believes creating the OSD CIO role is a step in the right direction. However, additional work is needed to fully empower and resource the role to meet the stated responsibilities and to provide further clarity on the role and responsibilities between OSD CIO and DISA.

DoD Governance Structure: In today's modern IT environment, IT end-user experience requires the tight coordination and alignment of all elements of the IT value-chain or stack (device, applications, network, and server) across the enterprise. An effective DoD governance structure to consistently deliver on this alignment requires DoD CIO-driven leadership to establish directions and to hold the DoD IT organizations accountable for agreed interconnected SLA targets. **This governance must include the structures, standards, and processes for setting, monitoring, and correcting the end-user experience, strategic direction, and objectives; establishing standards; and prioritizing IT investments to meet the goals.**

Today, the DoD CIO leads an ad hoc IT CIO Council but does not have the authority to establish or enforce DoD-wide policies. Without the structured, empowered governance process, the user experience will remain largely uncoordinated and inconsistent. Furthermore, the current budgeting and planning process results in uncoordinated and siloed resourcing decisions across MILDEPs, components, and agencies within DoD.

Through interviews, the Subcommittee found that DoD established DISA to provide core network services for NIPR to the components; however, there aren't integrated processes, data-sharing, or relationships across DISA and the components, or within DISA silos, for implementing or managing user experience.

Finally, the Subcommittee found **no enterprise-wide DoD metrics or SLAs for the end-to-end user experience.** Air Force has defined user-experience metrics but is not responsible for influencing the core network that may affect a large portion of the end-user experience. DoD needs to define metrics for the end-to-end user experience and clarify ownership, processes, and tools to manage these metrics.

Key Finding #6: Redundant Deployment of Security and Cybersecurity Tools

Regarding IT user experience, specifically in the workplace, a user-friendly environment accompanied by a stable, secure network is essential in promoting productivity, efficiency, and effectiveness from all personnel. Additionally, user proficiency and satisfaction will decline without a reliable and consistent security/cybersecurity system. Unfortunately, due to stagnant deployments of security frameworks, multiple levels of layered security, and poor configuration of security software, **the IT experience within the Department of Defense has been negatively impacted and not meeting expectations**.

Zero Trust Framework: According to DoD's Zero Trust Reference Architecture (ZTRA), Zero Trust is an "evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."[30] This standard emphasizes the need for complete user authentication and encryption practices to be implemented across all workflows regardless of location (physical or network) and ownership to ensure impenetrable security and protection across all security frameworks. Furthermore, it minimizes data leaks, phishing attacks, and other unauthorized tactics to accumulate classified and unclassified information. Although the Zero Trust framework will be a tremendous asset to DoD, it poses one issue: **"TIME" - Zero Trust will not be available to agencies, or Department-wide, until fiscal year 2027.**[31]

Layered and Redundant Cybersecurity: Defense-in-depth/layered security is a framework that employs various layers of security to safeguard its organization's assets. One challenge of DoD's implementation of layered cybersecurity is the lack of critical lab testing for interactions of layers, security patches, and continuous software updates. Testing cybersecurity structures before the rollout is crucial to ensuring maximum user effectiveness. If not properly assessed, it can cause significant problems and enable work stoppage amongst personnel. Additionally, our interviews with senior government officials revealed multiple reports of redundant security applications installed on devices, usually competing for local CPU, memory, and disk resources and impacting usability. Sometimes, this resulted from multiple security application recommendations from different IT vendors who lacked awareness and had not coordinated the security implementation plan.

Work Stoppage: Work stoppage is a primary symptom of poor cybersecurity processes. It elucidates the inadequacy of given IT resources to complete day-to-day work tasks and accountability to colleagues depending on deadlines and deliverables. In addition, lengthy login times produced by authentication scripts contribute to the widespread loss of productivity within DoD.

---

30 Barnett, Jackson. Fedsoop.com. "IT consolidation for military's Fourth Estate agencies is coming next year, officials say." Page 19. December 1, 2020. www.fedscoop.com/dod-fourth-estate-modernization-initiative-disa.

31 Liu, Nancy. SDx Central. "DoD Discloses Zero-Trust Strategy, Roadmap. "November 23, 2022. https://www.sdxcentral.com/articles/news/dod-discloses-zero-trust-strategy-roadmap/2022/11/#.

Key Finding #7: Insufficient IT Funding & Lagging Acquisition Implementation

IT Procurement: Contracting officers, program managers, and other acquisition professionals are performing adequately in acquiring IT solutions to assure warfighter effectiveness. The number of IT acquisitions at the post/camp/station level, through intermediate commands, up to Department-wide purchases, is massive.[32] However, the Subcommittee finds DoD acquisition processes are being sub-optimized by current Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) policies that drive the lowest price/minimally technically acceptable acquisition meeting all validated requirements. While overpaying for unnecessary bells and whistles is never an intelligent practice, nor is it wise to focus solely on cost as a sourcing determinant, as many interviewees suggested is often the case at DoD. The Joint Capabilities Integration and Development Systems (JCIDS) infrequently validate requirements and, instead, individual entities are making decisions unrelated to DoD enterprise solutions and capabilities.

Moreover, contracts, which, if used DoD-wide, would derive substantial cost and technical interoperability benefits to the Department, are being eschewed in favor of Individual Military Department-unique, intermediate command, or local contracts. The Subcommittee recognizes that requiring all MILDEPs, agencies, and components to procure IT from a single enterprise contract may not be viable. Moreover, as suggested above, the Subcommittee recognizes cost efficiencies should not be the sole driver for acquisition decisions. At the same time, **DoD IT contracting actions should be consistent with an enterprise-wide set of standards and strategies and not duplicate existing capabilities**. Successful IT integration will require DoD to establish a common set of DoD Enterprise Information Environment (EIE) acquisition and procurement strategies. Technical standards can achieve a level of interoperability, and DoD must synchronize acquisition and procurement strategies across all components.

IT Funding: The Subcommittee is also concerned that the DoD, or elements within DoD, have either inadequately funded IT or have used intended IT funding as "bill payers" for other mission-related requirements (e.g., steaming hours or flying hours). From our interviews, the Subcommittee believes this situation correlates strongly to negative IT user experience*s*, damages unit effectiveness, and costs the Department a great deal in lost productivity. For example, the Subcommittee received multiple anecdotal reports of **users waiting for 5, 10, and even 20 minutes for "morning boot-up."** With these delays, the loss in work productivity to the Department is substantial. Underfunded IT budgets result in outdated hardware, software, and IT infrastructure. For example, the average age of desktop equipment across DoD is six years, much longer than the industry's best practice of replacing devices every three to four years. Industry has learned that this pace of technology refreshment is essential to leverage new technology, assure system supportability and compatibility, derive the benefit of the latest hardware and software security features, and operate most effectively and efficiently. Using

[32] Department of Defense Information Resource Management Strategic Plan FY19-23. "DOD Digital Modernization Strategy 2019." Page 7. July 12, 2019. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

outdated equipment can negatively impact morale, on-the-job performance, and employment choices.

A.J. Gold & Associates conducted a study that demonstrates the value of replacing company computers every three to four years to be a 249% return on investment the first year and a 498% in the second for an office worker.

Roll Based Scenario	Office Worker	Engineering	Admin	Business Analyst	Web Programmer	IT Staff
1 Year ROI	249%	642%	397%	264%	547%	249%
2 Year ROI	498%	1285%	794%	528%	1093%	499%

A salary percentage was used to calculate the productivity improvement cost savings based on time saved per employee. In a two-year period, the company saved approximately $10,153 with an office worker and $16,193 with an admin using a new faster computer.[33]

Lagging Behind Industry Best Practices: DoD's IT current funding, procurement, and auditing processes are not agile and lag behind industry standards. *Breaking Defense*, a publication focusing on current US defense policies and practices, highlights the Pentagon's inability to establish a rapid and consistent system that delivers adequate software to stakeholders.[34] Furthermore, it emphasizes how renovating and strengthening DoD's IT budget is crucial to efforts to produce a constructive and updated technological environment. **Modernizing current hardware and software across DoD will improve user experience, increase enterprise engagement and provide a platform for innovation and productivity amongst military and civilian personnel**. In addition, realizing the benefits of cloud computing means identifying future skill gaps and conducting regular evaluations of customer experiences and user needs.

The Department must find the right balance of authorities (among the components and OSD and among the relevant IT, finance, and acquisition functions) to ensure that IT investments are both adequately funded and are tied to a common set of standards and performance metrics/budget justifications. Indeed, tying IT investments to a common set of standards and measurable, reportable performance metrics is crucial. Unfortunately, to date, this does not appear to have been the norm, and the continuation of the status quo is not likely to deliver the mission support and effectiveness the Department's employees and uniformed members need and deserve.

33 Gold, A. J. & Associates. Research. "Value of Replacing Company Computers Every Three Years." Retrieved November 21, 2022. https://jgoldassociates.com/research.

34 Gill, Jaspreet. Breaking Defense. "OSD gets new IT directorate, own CIO after study found 'degradation' of services. October 14, 2022. https://breakingdefense.com/2022/10/osd-gets-new-it-directorate-own-cio-after-study-found-degradation-of-services.

Key Finding #8: MILDEPs Approach the IT User Experience & Effectiveness Differently

The twenty-first-century, all-domain military operations require an agile information technology environment to achieve dominance in a multi-faceted and highly-contested world. Accordingly, DoD personnel at all levels must be able to rapidly and seamlessly access the IT systems necessary to execute their dynamic missions. Furthermore, these basic resources must be available worldwide, consistent with security and special access restrictions. Unfortunately, as discussed below, DoD's IT structure, as currently funded and implemented, fosters unnecessary complexity and redundancy, directly impacting the end user's experience and effectiveness. This structure has led individual MILDEPs to pursue their own user-focused programs. Each of the MILDEPs' approaches has merits, but they are all siloed in nature.

Enterprise-wide Implementation: As noted in previous findings, highly effective enterprise-level IT leaders from industry conduct consistent, ongoing, and thorough analyses before deciding on the type of hardware, software, and security protocols needed for enterprise-wide implementation, considering:

- Users' mission(s) (including ever-evolving requirements, goals, and capabilities);
- Users' knowledge, training, and expectations;
- Organization's available infrastructure (network, bandwidth, cloud architecture, etc.); and
- Available industry-leading IT innovations.

Organizational Effectiveness: After multiple interviews across industry and DoD, the Subcommittee found that these "best-in-class" IT operations are singularly focused on enabling user productivity, data access, security, and mission success. All strategic, operational, and tactical actions center on improving user efficiency and capability. Rather than top-down mandates, these leaders begin with the user by prioritizing change management at all levels of planning and ensuring user input is received throughout each step of the process and during ongoing operations. This **user engagement is not only a "factor" in IT decision-making but also a key measure of IT operational success**. Simply put, they focus on "individual IT user experience" as an indicator of organizational effectiveness.

To this end, effective public- and private-sector IT leaders have insisted upon consistent, transparent, and enterprise-wide governance mechanisms to balance available organizational resources and budget allocations with their end-users' mission needs, technology requirements, and individual expectations. These mechanisms have been successful in both centralized and federated organizational models, but all have put the user experience in a central governance role.

Unfortunately, although OSD has instituted multiple systems and structures to focus on the IT needs of the entire Department, its disjointed "Title 10-driven" IT organizational structure, decentralized budget authority, and "consent-based" governance has not aided in prioritizing user experience. Accordingly, MILDEPs have embarked on separate paths to achieve their organizational goals and user needs. Below is an overview of these efforts.

> ***"IT departments and organizations can identify important [Bring Your Own Device] BYOD issues and chart their own voyages…. IT consumerization may have mixed impacts on IT departments. On one hand, IT departments often cite security and risks as reasons to thwart end-users' technology initiatives. On the other hand, allowing end-users to use consumer technology at work increases employees' innovativeness, which may translate to the IT department's innovativeness."***[35]

Department of the Army: From interviews with senior-level personnel, the Subcommittee learned that with over 1.4 million personnel, the Army has an IT consumer base that dwarfs the other MILDEPs (and almost all private-sector companies), the 4th Estate, as well as private-sector organizations worldwide. It has a decentralized mission, with installations and units remotely dispersed worldwide in all types of garrisons, training, and combat environments. User experience and effectiveness are critical and play a significant role in the Army's willingness to seek service-specific innovations beyond the OSD program.

Accordingly, armed with "Title 10 budget authority," which provides each MILDEP with authority and independence generally not found in the private sector, the US Army CIO is piloting IT innovations focused on improving the Army's individual user's effectiveness. Although informed by OSD, the other MILDEPs, and the "remote worker" COVID-19 experience, these innovations are primarily done independently through the Army's individual contracting, budget, and technology decisions. Of note, the Army focuses on three key areas: innovative hardware management, improved network/cloud access speed, and a centralized help desk.

Regarding hardware management, with such a large pool of potential users, there is insufficient funding for the adequate issuance, periodic refresh, or upgrade of basic computer/mobile hardware. Accordingly, the Army recently launched a Bring Your Own Device pilot program to allow users to access both NIPR and SIPR through a Virtual Desktop Infrastructure (VDI) solution. VDI is a desktop virtualization technology managed in a secure cloud data center that runs the operating system. This system allows the virtual desktop image to deliver over a network to a user's endpoint device. As a result, **the user can access and use the operating system and applications as if they were running locally**. The endpoint may be a traditional computer or laptop and a mobile

[35] Curry, Koch, Milic, Yan, and Zhang. *Information Systems Management*. "How Consumer Technology is Changing the IT Function: A Multi-Case Study of Three Fortune 500 Companies." 2019. Vol 36, No. 4, Page 336-349. Retrieved January 18, 2023. https://doi.org/10.1080/10580530.2019.1652443.

device. The Army currently permits over 20,000 users to test this concept and expects to expand this service-wide.

> ***"Think of the operational effectiveness that will come with that [BYOD]," Lt. Gen. John Morrison said. "We have layered-in security all based off of zero-trust principles, and that notion of knowing who that individual user is and think of the possible economic or fiscal efficiency that we potentially could get."***[36]

The areas of networking, access, reliability, and quality are particularly concerning for the Army due to the enormous IT user pool size. While issues at the headquarters remain important, Army leaders focus on user experience and installation/unit-level efficiency.

With a senior government official noting Army spends more than $450 million on IT services to DISA, the service is concerned about DISA's perceived lack of transparency, affordability, and metrics. Accordingly, to address some of these issues, the Army is exploring moving away from DISA and contracting directly with an internet service provider to offer Army users faster and more reliable access to basic unclassified services at all levels. Specifically, the Army is testing a network concept called "internet as WAN," in which users directly access a secure cloud through any available internet provider rather than entering through a DISA-managed network. This network design is intended to dramatically reduce network latency and improve user experience and productivity.

Finally, to ensure a common level of assistance and data gathering, the Army has instituted a single, worldwide help desk to provide technical support. This approach will allow IT leaders to rapidly identify enterprise issues, trends, gaps, and potential threats.

Department of the Air Force: Similar to the Army, the Department of the Air Force (including US Space Force) exercises its Title 10 authority to make independent decisions on technology and capabilities to support user experience and effectiveness. Likewise, United States Air Force (USAF) leaders also participate in OSD IT planning and discussions, but it uses its own budgetary and policy authority for service-centric IT implementations. **Of note, the Air Force has appointed its first-ever Chief, IT User Experience Officer, which the Subcommittee found is an industry "best practice" for large-scale private sector IT-heavy organizations such as Microsoft.** The USAF User Experience Officer focuses on three critical measures: consistent enterprise-wide direct user feedback, digital effectiveness monitoring at the endpoint level, and enterprise performance management system development.

> ***"In the Air Force, we have tremendous buy-in from senior leadership that we need to work on this. The question is: At the next level down, what are the various goalposts that we have to shoot for, that we're going to have to hit and how are we going to get there? That's the function that I can serve: get everyone aligned toward those ends,***

[36] Gill, Jaspreet. Breaking Defense. Land Warfare, Network/Cyber. "Army Launches New Bring-Your-Own-Device pilot as it aims to leverage commercial capabilities. August 22, 2022. https://breakingdefense.com/2022/08/army-launches-new-bring-your-own-device-pilot-as-it-aims-to-leverage-commercial-capabilities.

figure out what their barriers are, help them get past those barriers and help them all move in the same direction," Colt Whittall, the Air Force's first CXO, 2022.[37]

Regarding direct user feedback, the Air Force uses a commercially available experience management tool to dispatch simple but effective IT User Satisfaction surveys. This tool allows the Air Force to understand specific users' IT issues and track each respondent's key demographics such as location, rank, age, and even career field. The Air Force distributes these survey tranches, so eventually all Air Force personnel are invited to comment over a year. It is a simple three to five question survey that has garnered a high response rate.

To implement digital monitoring at the endpoint level, the Air Force has adopted a commercially available software system that assesses the devices' overall application health and performance. According to a senior-level official, the Air Force deploys this software on approximately 6,500 endpoints across 65 facilities. Additional funding is available to increase this deployment to 25,000 endpoints. This system allows the Air Force IT leadership to obtain direct data on technical performance metrics, ranging from time to log in and time to access an application to the impact of the "security stack" on local Central Processing Unit (CPU) performance. Such endpoint monitoring is also considered an industry best practice in the private sector.

Next, the user experience officer develops and deploys an enterprise performance management system. Currently, the holistic monitoring tool is deployed at some 50 USAF bases worldwide, the Air Force is running multiple tests to obtain a real-time strategic view of the digital-user experience and service-wide IT landscape.

Finally, the Air Force Chief Information Officer has directed a weekly enterprise IT leadership discussion across the service. This discussion includes members of the HQ Air Force CIO, Chief User Experience Officer, regional CIOs, USAF Cyber, IT acquisition, and network operators. **This level of top-to-bottom engagement across the service allows for rapid identification of gaps, innovations, and potential threats to the system. In addition, it drives the user experience as a critical measure of organizational success.**

Department of the Navy: The Department of the Navy (including the US Marine Corps) exercises its statutory and budgetary authority to focus on and improve the user experience. Like its Sister MILDEPs, the Navy has dramatically embraced innovation and pilot programs to improve IT effectiveness over the last two years. According to a senior official, the Navy's focus, like the Army's, is on implementing a VDI with a cloud-delivered desktop and a BYOD program but also includes a multi-factor authentication option, which does not require the use of a CAC.

The Navy plans to employ over 200,000 virtual desktops, allowing access to the Department of Defense Information Network (DoDIN) without a CAC. The Navy has tested this with over 10,000 users and has seen a dramatic improvement in user

[37] Boyd, Aaron. Nextgov.com. "Air Force CXO: We Don't Have to Delight the User." Retrieved January 4, 2023. https://www.nextgov.com/emerging-tech/2019/10/air-force-cxo-we-dont-have-delight-user/160373.

experience over a legacy desktop system. Additionally, the future is in the cloud-delivered desktop. This approach will allow the Navy to manage one image in the cloud and to realize exceptional cybersecurity advantages and software upgrade capabilities.

Of note, the ability of the Navy CIO to have policy, budgetary, and decision authority has allowed improvements in user experience and effectiveness to be a realizable goal.

Summary: Based upon perceived operational necessity, many of the critical "user-focused" elements of DoD's IT infrastructure, applications, and software are developed, controlled, and operated by individual MILDEPs, components, and agencies. These foster different IT solutions not explicitly designed to be interoperable and complementary, and that create a significant impediment to an enterprise-level, seamless IT environment. For example, these include:

- Cumbersome migrations when users change organizations;
- Lack of permanent identity presence;
- Inability to view a global address and contact list that covers all MILDEPs, components, and agencies;
- Inefficient search capabilities; and
- The lack of integrated email platforms.

The different approaches mainly manifested themselves while fielding multiple Microsoft 365 tenants across the services. These require numerous licenses not configured to share addresses, calendars, and other information across tenants.

Recommendations

Rec #1: Implement Endpoint Monitoring Across ALL Devices and Prioritize DoD IT Funding to Consistently Monitor and to Improve End-user Experience

Rec #1 Summary:

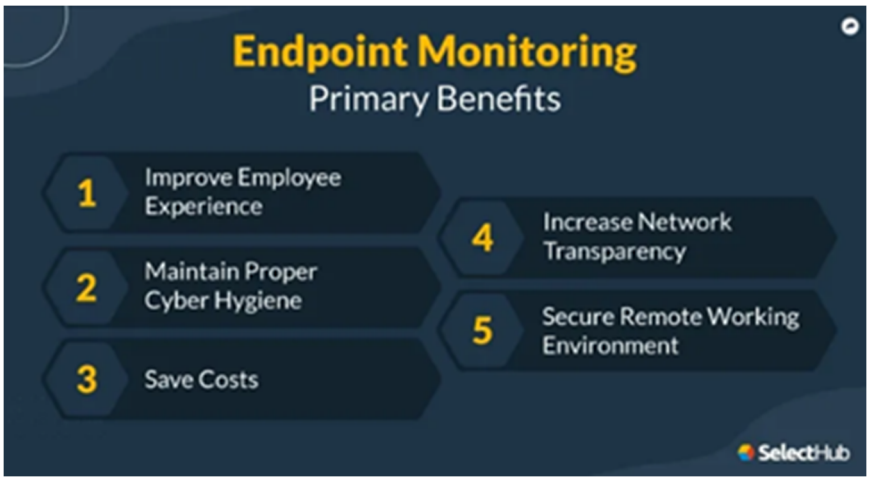
- DoD must recognize and **prioritize IT capabilities, particularly those that enable communications, logistics, and other support functions critical to warfighter success.** Because IT capabilities also drive productivity and employee engagement, prioritization must be addressed culturally and as a part of the funding/budgeting process.
- DoD must **consistently and accurately measure end-user experience**. End-user satisfaction measurement must include three critical components: **metrics representing user experience**, an **endpoint monitoring solution on all DoD endpoint devices**, and a **regular review of key metrics by the DoD CIOs and DoD CIO Council** with accountability throughout the IT process.
- DoD must **establish the structure and expertise to resolve IT-related work stoppage issues**. Accessibility and reliability are critical across DoD. There must be unambiguous accountability for resolving the problems that prevent, delay, or otherwise impair the use of IT systems and resources. DoD must **establish governance and clarify responsibilities to evaluate and solve problems**. Further, the Department must adopt a culture of continuous improvement in IT service measurement and delivery.
- Mandate and accelerate the adoption of **interoperable enterprise cloud services**.

Rec #1 Details:

As with the private sector, IT capabilities and systems that enable communication, logistics, and other support functions are critical to warfighter success. In addition, reliable and efficient access to these IT capabilities is essential to the productivity and effectiveness of the DoD employees that support this vital mission. These **critical capabilities include the "internet of things," cloud computing, mobile devices, productivity applications, and web services**. Therefore, keeping top-of-mind of the end-user experience (efficient and effective access to these tools and capabilities), the Subcommittee recommends the following considerations to better prioritize DoD enterprise-wide IT capabilities.

Consistently and Accurately Measure End-user experience: As indicated in Key Finding #2, 80% of end users surveyed by the DoD's JSP rated user experience average

or below. While the survey only sampled DoD employees, it revealed specific data points, including logon times, re-authentication frequency, ticket frequency, and work stoppage, that point to meaningful opportunities to improve existing IT capabilities and avoid unnecessary downtime.



As in the private sector, the Subcommittee believes **a continuous and well-structured DoD-wide survey of end-user experience will be critical** to help the Department identify the key issues that are reducing the productivity of the employees. Measuring end-user satisfaction should have three crucial components. First, **key metrics must be defined** (see Recommendation #2). A key to these metrics is that they must represent the end-to-end-user experience, from the device through the network to the target. Secondly, the Subcommittee recommends installing a **monitoring solution on endpoints to obtain data reliably**. The goal should be monitoring enterprise-wide on all devices. The Department can use a sampling approach to start as it moves toward the goal of all devices monitored subject to the available budget and timeline. With **66% of organizations experiencing increased endpoint threats**, proper endpoint monitoring has become crucial to scrutinize all suspicious activities and **achieve robust endpoint security**. Lastly, there has to be **accountability for improving and resolving the major problems.**[38]

Accountability is key to meeting the IT requirements and user expectations and to delivering a quality service. Accountability is needed to ensure ongoing improvement in key metrics, service quality, and performance and delivering projects and initiatives on the implementation roadmap (see Implementation Roadmap section below). Successful organizations set goals and expectations and hold leaders, individuals, and teams accountable to delivering against those goals. Appropriately scoped goals are defined, and progress against those goals are reviewed regularly and adjusted as needed with senior leadership. Weekly and monthly status meetings are held where key metrics and project status are reviewed and where input is gathered on hot topics and critical issues. Quarterly and annual reviews serve to take broader and, often, more strategic views of metrics, goals, and initiatives and related budgets. Stretch goals are also frequently used to set longer-term targets and to encourage the team to achieve higher performance and results. In industry when expectations and goals are not achieved, root cause analysis is used to understand what challenges and issues are preventing success, resulting in action plans, performance improvement plans, and coaching at the leadership and team levels. Repeated failures and lack of clear and meaningful improvement can often lead

[38] Das, Tamaghna. SectHub.com. "Endpoint Monitoring: A Comprehensive Guide." Retrieved December 6, 2022. www.selecthub.com/endpoint-security/endpoint-monitoring.

to more formal warnings, job-in-jeopardy messaging, reassignment of responsibilities to others in the organization and possible termination of employment. While this might seem harsh, this level of accountability is critical to deliver consistent and high-quality service.

Understandably, accountability is a cornerstone of DoD success and is inherent in the core values of the Department. The Subcommittee believes the right teams and leaders can be held accountable to deliver the basic IT services through the review of key IT-related metrics, help desk reports, and user surveys and through understanding the responsibility and ownership of delivering end-to-end IT services, performing root cause analysis of failures and issues, and planning and implementing fixes and enhancements. The MILDEP CIOs, OSD CIO, and DISA/JSP leadership; with the support of DoD CIO and of the DoD CIO Council (see Recommendation #8), the MILDEP CXOs (see Recommendation #5) would be responsible for holding their teams and leaders accountable within their departments and as an enterprise.

Elevate Customer Experience Improvement/Targets as Critical Objective for Annual DoD-level IT Investment/Budget Prioritization: The Department must make difficult choices to protect critical IT services from reductions. For example, security software testing (see Recommendation #4), device replacement and life cycle management (see Recommendation #3), and tools to measure end-to-end user experience must be established and protected. In addition, ongoing governance must ensure that investment is being made consistently in the areas impacting productivity and basic access to the systems required to enable warfighter success. In the private sector, information technology-investment decisions are exercised at the highest levels of an organization, as CEOs recognize these decisions are critical to organizational change, core business practices, and customer satisfaction.[39] An international professional services company the Subcommittee interviewed shared that it operates worldwide with one global Chief Information Officer overseeing all technology and managed with a strong central governance model.

The CIO is responsible for the Personal Computer (PC) operational budgets, but those are actually funded by each individual organization. In the DoD, the CIO works with approximately 50 CIOs of all the MILDEPs, components, and agencies to help them implement policy and approve their budgets. However, the DoD appears to lack standardization for IT capabilities. This standardization requires aligning centralized standards in a heavily decentralized model. The multiple tenants do not foster unity among best practices or measurable metrics to assess service provider performance and end-user satisfaction.

Resolve IT-related Work Stoppage Issues: Accessibility and reliability are critical across DoD. Research into the private sector also indicates that IT-related issues affecting employee performance are under-reported each year but significantly affect productivity. **The average employee will encounter two IT issues per week, with a productivity loss of 28 minutes per incident, while others suggest the productivity loss rate is even greater**. In fact, Gartner Research noted “A computer that saves an

[39] Batchelder, Grossman, Martin, Newcomb, Rockart & Yetter. *Harvard Business Review*. “The End of the Delegation? IT and the CEO.” September-October 1995. Retrieved hbr.org on October 27, 2022. https://hbr.org/1995/09/the-end-of-delegation-information-technology-and-the-ceo.

employee ten minutes a day, including boot-up, logging in, opening apps, shutting down, and running security software efficiently, will save roughly 40 hours a year per end user.[40]

Using Gartner's research numbers of 40 hours a year, $40.32 average hourly pay rate ($84K a year) and 10% (industry standard) of DOD's 3.4 million users' experience issues, the annual savings for resolving these productivity issues would be $548M per year.[41] [42]

Lack of reporting also drives a disconnect between what IT departments think their tools and services are providing compared to what end users are actually experiencing. This gap in perception is problematic because companies or DoD cannot afford employee dissatisfaction and attrition risk due to IT challenges. Interestingly, **84% of surveyed employees from the private sector believed their organization should be doing more to improve the digital work experience, but 90% of the IT leaders thought their workforce was satisfied with their technology tools.**[43]

Establish Cross-enterprise Initiative to Resolve the Critical Current Issues: Many of the issues experienced by end users are common across departments. However, interviews and surveys highlighted several intractable problems that drive a significant portion of today's poor experience and center on boot-up times and accessibility issues. To solve these issues systematically and efficiently, the Department should establish a DoD cross-CIO initiative to assess the problems systematically and to invest in resolving them in a coordinated way. The government-wide CIO Council[44] could be leveraged, but a DoD CIO Council is an appropriate construct, given the size, complexity, standard requirements, and experiences within the DoD departments.

Mandate and Accelerate Adoption of Interoperable Enterprise Cloud Services: Mandating interoperable enterprise cloud services would allow all users, regardless of DoD organization (e.g., MILDEPs, COCOMs, OSD), to have a seamless connection to store and access data and programs over the internet, rather than on a local computer hard drive. This service would also allow users to access information from anywhere at any time, effectively removing the need for the user to be in the same physical location as the hardware storing the data. In addition, interoperable services would include an address book and calendar interoperability across email tenants to support more efficient collaboration.

In summary, prioritizing IT capabilities to ensure warfighter success requires a cultural shift across the CIO teams. It is critical for DoD to monitor user satisfaction and performance to resolve issues in a timely fashion. Conducting surveys of end-user

---

40 Vbsitservices.com. "How Often Should Your Company Replace Computers?" Retrieved December 5, 2022. www.vbsitservices.com/2016/02/how-often-should-your-company-replace-computers.

41 Office of Personnel Management. Policy, Data, Oversight. "Fact Sheet: Computing Hourly Rates of Pay Using the 2,087-Hour Divisor." Retrieved January 8, 2023. https://www.opm.gov/policy-data-oversight/pay-leave/pay-administration/fact-sheets/computing-hourly-rates-of-pay-using-the-2087-hour-divisor.

42 Payscale.com. "Average Salary for U.S. Department of Defense Employees." Retrieved January 19, 2023. https://www.payscale.com/research/US/Employer=U.S._Department_of_Defense/Salary.

Help Net Security. News. "The true costs incurred by businesses for technology downtime." April 24, 2020. https://www.helpnetsecurity.com/2020/04/24/technology-downtime.

Higgins, Ryan. Chief Information Officers Council. "The Importance of Multifactor Authentication. October 26, 2022. The Importance of Multifactor Authentication | CIO.GOV.

43

44

satisfaction, deploying monitoring tools, as well as monitoring and reporting performance must be the responsibility of the implementation owners. In the case of DoD, implementation is owned by the MILDEPs and OSD CIOs. To support these efforts, ownership for cross-enterprise initiatives must be established, including DoD CIO-led Council for metrics and a review/study to establish lead for cross-enterprise critical issue resolution. (See Recommendations #8 for more on CIO responsibilities and #5 for Chief Experience Officer.)

4 Critical KPIS for Internal Help Desks to Improve End-User Experience

Research suggests the cost per help desk call is about $30 at 20% agent utilization; increasing utilization to 50%, costs can be reduced by one-third.

With IT under pressure from users to fix any application or network problems quickly, internal help desks often are a very busy resource. So, how do you improve end-user IT experience? Define and measure metrics for provider performance.

*One of the most important KPIs to consider when running a help desk is the **first call resolution (FCR**). Yet, even with a high FCR, help desk agents who take a long time while ensuring the problem is resolved thoroughly or end users who spend a long time on hold waiting can significantly increase the cost per call or mitigate the goodwill advantage of solving issues during the first interaction.*

***Average Response Time**: Waiting on hold is the worse and a pretty obvious goal for help desks to minimize the time from when a user dials the support line to communicating with someone.*

***Average Handle Time**: Not all tickets can be resolved on the first call, and handle times is a broad umbrella of resolutions. Time can be quickly absorbed with complex issues, faults in agent knowledge or expertise, underlying problems with products or services, or additional follow up for issues that cannot be resolved in the first call.*

***Cost per Incident**: Every help desk incident has a cost associated with it; however, that does not scale in the linear fashion. A call that is resolved by Tier 1 support will have one costs associated with it, while a call that escalates will have another, as will a response that requires a physical fitness to the digital workspace. There is not standard metric for calculating cost per call, because it would need to factor in pay and benefits of agent's time involved, equipment costs, transportation costs, and end-user downtime. In general, the higher the agent utilization, the lower the average cost per call.*

***Agent Utilization**: How much time should IT agents spend on the phone resolving issues? Although it seems a likely answer would be 100%, even at a 90% rate, that is only six minutes per hour of idle time, or just seconds between calls. This has proven to lead to a higher burnout rate and, thus, a higher turnover rate and higher costs to train and hire. A widely-agreed-upon industry formula for help desk agent utilization is:*

*Agent Utilization Formula = (Tickets per Agent per Month * Handle Time per Ticket)*
*/ (Days worked per Month * Minutes Worked per Day)*

The best metric, though, is 'problems solved before the end user even becomes aware of one,' so monitoring apps and networks, from devices or the cloud, users depend on will provide the help desk more essential and timely data upfront. Agents are then more able to find and fix problems faster as

45

45 Sanders, Andrew. AppNeta. "4 Critical KPIS for Internal Help Desks to Improve End-User Experience." November 13, 2017. www.appneta.com/blog/4-critical-kpis-internal-help-desks-improve-end-user-experience.

Rec #2: Leverage Metrics for IT User Experience to Drive Accountability from Service Providers and to Deliver Acceptable Quality of Service

Rec #2 Summary:

- DoD must **define, log, report transparently, and measure** against appropriate targets and user experience metrics to drive accountability from internal and vendor service providers and for end-user satisfaction.
- **Specific metrics recommended** by the Subcommittee, listed below in Table 1, cover actual device-level metrics, the network/transport, and those measured against online IT services, like email, video conference/chat, and office suite applications.
- Chief Digital and Artificial Intelligence Officer (CDAO) provides a **centralized data warehouse and dashboards** for metrics data in Advanced Analytics (ADVANA), viewable at the appropriate levels and roles within the organization. **Reviewing metrics scorecards should be a regular practice across all levels of management, including the Department Secretary of Defense (DepSecDef), DoD CIO, and MILDEP CIOs, CXOs,** and down through the IT department to drive awareness and accountability.
- **IT roadmaps and future budget investments** must include an examination of these metrics and targeted improvements in those areas that fall below the metric targets. In addition, return on Investment (ROI) analysis and related impact on user experience from potential improvements must drive prioritization.
- Conduct regular IT Experience and **Satisfaction surveys** across all levels and IT users within the DoD at an appropriate cadence (no more than quarterly) to measure and confirm satisfaction and experience goals are being met, providing a qualitative and quantitative review of IT performance.

Rec #2 Details:

Private sector companies that excel in managing their IT services and IT user experience demonstrate strong organizational awareness, operational excellence, and core values. This excellence starts with solid leadership role modeling and expectation setting for all employees. When shortfalls exist, these companies employ a transformation process to achieve their objectives and aggressively manage the metrics to ensure they perform to the desired levels. Other Defense Business Board Studies have recommended linking key metrics to performance assessment and reward systems, which is an essential part of the change management process and delivering operational excellence.[46] The Subcommittee recommends the following considerations when defining metrics and their value.

[46] Defense Business Board. "Recommendations for the Next Generation of Business Health Metrics." November 10, 2022. https://dbb.defense.gov.

Metrics Drive Awareness and Accountability with Employees: Everyone in DoD needs to be able to access the information resources required to perform their functions on any computer on DoD networks anywhere in the world, consistent with security classification and special access restrictions. Metrics are critical to building awareness to make informed decisions regarding service delivery and enabling leadership to monitor the progress of necessary transformation and hold teams accountable. Although some metrics are being captured and analyzed for network and transport operations, more metrics throughout the technology stack, including those at the device/end-user level, need to be measured and monitored in an action-oriented manner. **DoD must define, log, report transparently, and measure against appropriate target user experience metrics to drive accountability from internal and vendor service providers and for end-user satisfaction**. CDAO would provide centralized reporting capabilities where metrics would be broadly collected and reported to leadership and DoD, as appropriate. The best practice metrics from the private industry cover an array of indicators (e.g., application and hardware modernization, cybersecurity risk, budget share, help desk statistics, infrastructure utilization, and downtime). The theme that threaded all indicators was simple - how is IT evolving to support employees better, drive business outcomes, and service customers and end users?[47]

Overarching Goal: Measuring actual performance and experience metrics at the user's end device provides the most accurate view of the actual received IT user experience. Monitoring only at other levels of the technology service stack, such as the network or external services (for example, the email service), provides an incomplete view of the actual user experience. Metrics at other layers are also essential to provide quality service and troubleshooting issues, but they alone are not enough. Therefore, the Subcommittee recommends the following device/end-user metrics to support the suggested overarching goal of IT service providers:

- Device startup time;
- Time to authenticate (login with credentials) on the device and gain access to desktop and applications;
- Application startup times for critical applications (browser, email clients, office applications);
- CPU and memory utilization, local process runtime metrics;
- Network metrics to measure ping, download, upload speeds, and latencies;
- Network metrics to measure access to critical systems/services; and
- Application-level metrics related to email, collaboration/video/chat applications, and Office suite application tasks.

These metrics will allow DoD IT providers to better understand and prioritize the needs of technology users and to better respond to and support all DoD employees with reliable, consistent access to technology from anywhere in the world, to perform day-to-day

[47] Defense Business Board. "Recommendations for the Next Generation of Business Health Metrics." November 10, 2022. https://dbb.defense.gov.

operations of any kind of digital workplace environment. **Applying standardized metrics from continual monitoring of networks and endpoints devices can provide insight into areas for future investments in wide area(WAN) and local area networks(LAN) to improve the user experience.** There are many devices deployed across the DoD user base, and the Subcommittee acknowledges there could be budget or other constraints that make it challenging to monitor all devices. However, monitoring a significant subset of devices that provide ample signal across user groups, locations, and use could be an adequate solution when complete monitoring is impossible. Surveys, ticketing data, and other indications could identify a subset of devices to monitor initially and adjust periodically.

Reasonable Metric Thresholds and Expectations: Metrics collection and regular monitoring against thresholds and targets, which are set at levels to support end-user experience goals, are essential requirements to hold internal and external service providers accountable to service-level agreements and to the quality of service. Each identified metric would have an expected threshold used for monitoring success. Additionally, service providers should set future metric targets for improvements expected from planned IT roadmap initiatives and associated budget spending to improve IT User Experiences.

Table 1: Recommended Metrics

● User Experience Satisfaction (by component, by IT system)
● % Systems Beyond 3-year Refresh
● System Service Performance
○ Network reliability and availability
○ Device boot-up / startup time
○ Time to login / authenticate and access desktop or Home screen
○ Launch time for key applications running locally
● Measure Network Access
○ Key systems and services
○ Ping, download speeds, and upload speeds
● Help Desk Support
○ Service response times (on hold, engaging in solution, follow up if necessary)
○ Ticket frequency
● Work Stoppage Time Lost
○ Login issues
○ Re-authentication frequency
○ Connecting to the network
○ Accessing the drive
○ Application or software issues
○ New hire delays
● Digital / Cyber Risk / Business Continuity Measures
○ National Institute of Standards & Technology (or other standards) Cyber Risk Score
○ % systems in use beyond end-of-life/support
○ Key cyber safety effectiveness measures: system recovery timelines and layers of security
● IT Investments and Savings

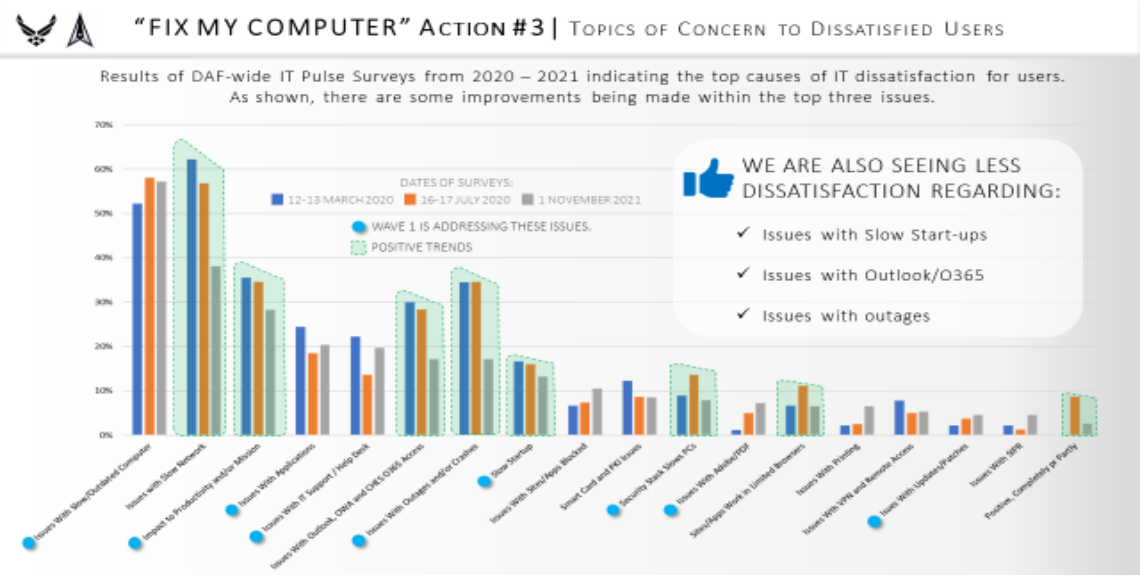
- Ongoing and projected IT development, modernization, and enhancement spend as a % total IT
- Ongoing and projected operational savings resulting from IT development, modernization, and enhancement vs. target

- Talent – the trend of talent and critical skills supporting the modernization projects vs. planned

Among many senior government leaders, the Subcommittee interviewed for this Study, **a common concern was that the DoD's IT process is not proactive in its approach toward end users but somewhat reactionary in response.** Metrics and monitoring will significantly impact service mindset, as will regular surveys on the quality of service, pain points, and overall feedback from the departments and employees. Service providers must understand past, current, and future disconnects with end-user expectations.

Leading Examples of Metrics Improving User Experience for Recommendations: Based on the Subcommittee's interviews with senior government and private-sector executives, there are leading examples of progress currently being made to improve the CX or end-user experience.

1. **Air Force:** Air Force captures device-level metrics for a subset of users, designed to measure user experience, inform IT, and roadmap investments.



[48]

In a recent survey of before and after the installation of new equipment and engineering changes to resolve conflicts for security protocols, the Cost Assessment and Program Evaluation (CAPE) saw improvements in the IT experience, increasing satisfaction from 30% to 60%. Although still not high enough, the dramatic increase is a sign the Air Force is moving in the right direction, responding to the needs of its personnel.

2. **Department of Veterans Affairs:** Recently recognized for its significant progress in positive user and customer experience with veterans, the Department of Veterans Affairs improved its rating from 55% to over 70%. That is a real and laudable change in the right direction for responsiveness and prioritizing veterans.

   To achieve this improvement, the VA identified several key strategies and updates to their systems and services. These enhancements were rooted in analyzing data and understanding trends in specific Veterans Health Administration (VHA) lines

[48] United States Air Force. Metrics. Retrieved December 18, 2022.

of business before they become problematic. The VA also worked to "conduct and continually expand performance improvement training using Veterans experience insights to help inform for opportunities in service delivery and systems improvements across VHA outpatient services."

While large, the VA is, of course, less complex in organizational structure and mission compared to DoD. The VA's journey to improvement has been long, very public, and the focus of significant, bipartisan congressional attention. The VA's strategies for improvement, particularly its use of data and focus on the user experience is highly informative. Additionally, the VA experience provides key insights into how an organization, including the DoD, can strive for 90% success and focus on overall satisfaction beyond the demonstrated improvements.[49]

3. **Private Industry Firm:** An international professional services company operates worldwide with a philosophy that world-class IT is a critical requirement within the firm. It uses metrics and performance reporting from all its operations to drive consistent global change management. This process is vital to keep the performance and user-experience data within the CIO chain of command. This approach will provide an overarching leadership role to collect, analyze, and apply relevant data from metrics designed specifically for IT end users to ensure service providers are delivering. As it relates to the DoD, the data being reported directly to the Secretary of Defense must include all the CIO Components' data analytics through the DoD CIO direct to the Secretary. The Subcommittee believes it will be more impactful to change management if the MILDEPs and components are answerable to the CIO, with centralized, shared, common metrics defined by the DoD CIO/DISA and to leveraging DoD CDAO's data warehouse and reporting requirements.

   The firm measures user experience with a multi-layered approach to ensure satisfaction. The plan requires organizational leaders to align objectives and key results with a goal-setting framework and metrics to measure progress and achievements. In addition, a continuous feedback loop is required to stay on target and immediately work to resolve any bottlenecks. The following metrics proactively predict performance on each endpoint. They predict potential challenges, capture employee sentiment, create a performance scorecard to hold vendors accountable to provide insight to technicians. These metrics will better resolve core issues and help determine budget needs and timelines to execute investments.

[49] Department of Veterans Affairs. "VA on Track to Improve Veteran Customer Experience." June 25, 2019. www.va.gov/VE/pressreleases/2019062501.asp.

Table 2: Private Industry Metrics Used to Measure User-Experience Effectively

Volume (volume against planned volume, used for resource planning)
Average Speed of Answer: Target 80% of Calls Answered within 45 Seconds
Abandonment Rate: Target 5% or Less
First Call Resolution: Target 60+%
Tier 1 Resolved: Target 70+%
Customer Satisfaction: Target 90+%
Customer Satisfaction: Target 96+%
Average Time to 1st Contact: Target 1 Business Day
Average Time to Resolve Ticket: Target 4 Business Days
Laptop Compliance: Target 80+%
Mobile Device Compliance: Target 100%

Rec #3: Review and Upgrade Device Replacement Strategy and Device Life Cycle Management

"Approximately 50% of the Air Force's PCs featured a spinning disk drive up until about a year ago, 2021. Spinning disk drives and underpowered old PCs, simply, cannot run the endpoint security stack," senior Air Force senior officer. [50]

Rec #3 Summary:

- The Subcommittee recommends that the Department, under the directive of the Deputy Secretary and the DoD CIO, **issue a policy establishing an endpoint refresh cycle timeline of three to four years to be reflected in all endpoint contracts and departmental and component budgets**. Further, to avoid the annual "billpayer" syndrome, the policy should require that adjustments may occur only via explicit resource tradeoffs.

- In each budget submission, each of the components of the Department should **include specific line items for IT modernization that define both the desired/expected end-state and how progress toward that end-state is to be measured and reported**. The submission should also include data from the preceding year's progress and UX reports. In industry, an average of 40% of IT budgets is spent on IT modernization initiatives (ranging from 34% to 45% depending on maturity stage and company size).[51]

- By comparison, across the federal government, including DoD, the average is far lower–less than 30% almost across the Department. **This has long been recognized as an unacceptable imbalance but remains largely unaddressed.**

- **Modernize or replace DPAS** to more accurately and transparently reflect the current state and age of fielded endpoint devices, a common definition of the term "current state," and a detailed schedule for maintenance and replacement for all endpoint devices. Additionally, this modernization would alleviate the initial issue and device replacement timelines. Done right, DPAS could become a central reference point for annual resourcing guidance.

Rec #3 Details:

Technology is essential to everything DoD does, and when it fails – the Department fails.

This philosophy is already prominent across the commercial sector, and it is one area where DoD should be aggressively adopting commercial best practices. **Gartner**

---

50 United States Air Force. Retrieved January 4, 2023.

51 InsightCDCT.com. "The State of IT Modernization 2020." Retrieved November 21, 2022. https://solutions.insight.com/getattachment/a67b34bd-1a9a-42fe-a408-7afe180b96d8/Complete-IDG-survey-results.aspx.

Research studied 177 businesses and discovered that the average lifespan of a desktop PC is 43 months, and 36 months for mobile PCs. Executives from the private sector emphasize technology as a very high priority, and they seek to replace end-user devices on a three-year life cycle.[52]

However, most senior government leaders interviewed for the Study did not believe that the IT user experience enjoys the requisite prioritization for this to be the case, as witnessed by the exceptionally long device refresh times and the perceived overall resource process. Additionally, the fact that a particular Technology Modernization Fund (TMF), government-wide, struggles for consistent and reliable funding serves as evidence of the lack of priority across the government assigned to accessible, dependable technology in a digitized workplace. Constant **feedback from the Subcommittee's interviews noted many were using devices that were five or six years old, with the Army at a four-year desktop refresh cycle and the Navy at six years - and that is just the planned refresh timeline.** As numerous interviewees reiterated, there is little

Microsoft: Holding on to Computers for More Than Four Years Costs More Than Buying Two New Computers

Microsoft conducted a study in New Zealand showing older computers are costing business owners more than 4,000 NZD, or US $2,736 a year after four years. According to the Pan-Asia Small to Medium Business PC study, the optimal age of PCs is no more than four years old, beyond which the cost of repairs and lost productivity make them cheaper to replace. Older computers are more than twice as likely to experience issues, including slow bootup, batteries depleting too soon, disk drive crashes causing data losses, application crashes, and network connectivity problems. The total cost of owning a PC older than four years is enough to replace it with two or more newer models.

Although the study focused on small to medium-sized business operations overseas, it is relevant because the DoD operates worldwide and because the results mirror Gartner Research and Intel's suggestions of when it is best to replace technology. In this survey, 70% of those surveyed use older than four years PCs with significant increases in maintenance costs; the main reasons cited were unbudgeted costs and the fear of incompatibility with existing internal business applications. As such, decision-makers should seek to adopt a device modernization strategy to maintain costs while safeguarding their organizations from newer digital risks. For example, new computers are much more effective at intercepting viruses, malware, or spyware infections and are significantly more effective at combating security breaches. Of those surveyed, 67% had experienced security issues or data theft breaches within the previous year.

"Regularly updating PCs and hardware can greatly help businesses combat security challenges and boost the performance of business applications. Security isn't just a software issue – newer PC hardware incorporates modern security architectures and features that simply don't exist in older machines…. Every business, no matter what size, should take the security advantage of newer PCs seriously. It is far cheaper than dealing with the aftermath of a security breach," proclaimed a Microsoft executive.

Takeaways

1. The optimal age of PCs is no older than four years, beyond which they are more expensive to maintain than replace.

2. A PC that is 4+ years old is 2.7 times more likely to be repaired, resulting in 112 hours of productive time lost

3 The total cost of operating a 4+ year old PC is $2,736, enough to replace with two or more newer PCs.

52 Vbsitservices.com. "How Often Should Your Company Replace Computers?" Retrieved December 5, 2022. www.vbsitservices.com/2016/02/how-often-should-your-company-replace-computers.

4. Older computers often are unable to support newer operating systems, jeopardizing security[53]

question that, as with other items not always seen as "mission critical," basic IT capabilities too often serve as bill payers for other needs deemed to be a higher priority. In reality, however, this is a self-defeating cycle because even the most basic IT services are mission essential. **The DoD should develop a policy approved by the Deputy Secretary via the IT Modernization Fund, establishing consistent and predetermined tech refresh (no more than 4 years) as a budget priority, underpinned by device and user experience data and adjustable only by explicit resource trade-offs**. **Technology cannot be a billpayer for other departmental needs, data is the new ammunition and must be prioritized as such**. While there are some reports of this happening, the evidence suggests it is not nearly as firm and consistent as need be.

Finally, inventory management via the DPAS and the policy for hardware accounting, is antiquated. **Hardware costs are dropping tremendously and should not be subjected to legacy inventory practices.** Significantly expanding the automated capabilities of DPAS would meaningfully improve device replacement time without requiring hours of paperwork and supervisory signatures. In some cases, DoD Net has opted to replace a device if it cannot be repaired within two hours; however, that only works if an employee is physically close to a Help Desk center. Otherwise, a patchwork of property and custodian accountability systems for inventory management is the norm. In today's technology environment, this is unacceptable.

53 Microsoft NZ News Centre. "True Cost of Not Replacing Computers." Retrieved November 22, 2022. https://news.microsoft.com/en-nz/2018/10/16/true-cost-of-not-replacing-computers-revealed-in-microsoft-study-more-than-4000-each.

Rec #4: Simplify Security Layers, Move Faster to Zero Trust/Application-Level Security

Rec #4 Summary:

- Create or leverage an existing lab and **establish testing to identify performance impacts of applications to endpoints,** including layered security packages that may cause performance issues and user-experience problems (note: requires a set number of configurations or "images").
- The Subcommittee supports the Department's **move to Zero Trust and recommends accelerating deployment.**
- **Establish DoD-wide security standards** to be adhered to by all MILDEPs, components, and agencies throughout DoD. This framework should be end-to-end, from the endpoint through the network to the perimeter. **DoD CIO should establish standards centrally to be implemented consistently across DoD.**

Rec #4 Details:

Minimize Installing Multiple Layers of Security Software and Test for Performance including CPU usage: While the configuration of security software is improving, reporting of long scans and high Central Processing Unit from security implementation is frequent. A performant CPU is vital to ensuring the success of DoD personnel IT tasks. If the CPU usage is too high or over capacity, it can produce slow computing times and introduce latency, resulting in work stoppage.

Currently, DoD utilizes a layered security framework. The layering of software can cause operational conflicts that impact system performance. One way to combat performance degradation is proactive lab testing for all layer interactions. If examined and analyzed thoroughly, DoD will be able to identify latent threats and shortcomings of the security system before it interferes with the integrity and availability of civilian and military personnel work efficiency. In addition to interaction testing, penetration testing should be performed annually and upon significant changes to ensure effectiveness. Content experts who specialize in specific testing areas should conduct the testing. Based on interviews with senior leaders, the Subcommittee suggests the following practices for implementation:

- **Minimize layered security platforms.** Where multiple platforms exist, use skilled experts to conduct interoperability and performance testing and mitigate any issues that lead to excessive CPU usage.
- **Maintain an adequate end-user device life cycle program** (see Recommendation #3) since older devices can be negatively impacted by having multiple security layers and may be less capable of accepting mitigation solutions (e.g., patches).

Continue Zero Trust Rollout: The layered security framework utilized by DoD has been effective, but this system needs to evolve as security threats become more sophisticated. **The Zero Trust Framework rollout will be challenging and requires the requisite level of technical expertise to transform the DoD's cybersecurity paradigms and frameworks**. It forecasts a stable and agile network that demands successful user authentication and encryption practices to ensure impenetrable security and protection across DoD. However, until the full deployment of Zero Trust (which could take up to five more years, i.e., 2027), DoD will have to strengthen and utilize its current security structure.

Create DoD-wide Security Standards: One key to success shared with the Subcommittee by a Private Enterprise CIO is the existence of a CIO Council, led by the Enterprise CIO that defines metrics and policies to which business units must adhere. One policy utilized in certain private sector entities is the bounding of deployed device types/configurations. It is unreasonable to expect a scaled enterprise to only have a single configuration that meets all needs. However, having a fixed number of configurations allows for a better user experience, including manageable testing requirements, an efficient help desk/support model, improved problem resolution, and scalable performance monitoring. Therefore, the Subcommittee recommends **DoD set a policy standard for the device endpoint options available for deployment throughout the enterprise.** For example, one large company specializing in IT services that the Subcommittee interviewed has over 30 PC standard configurations to cater to its personnel, ensuring it has the right equipment to yield desired results.

Additional standards recommended to be defined and reported centrally include key metrics, service level agreements for issue resolution and security policy for on-premise versus cloud applications. Lastly, set security standards centrally for the wide-area network (WAN) and local area network (LAN) (see Recommendation #8).

The Subcommittee recommends **creating or leveraging an existing lab** and establishing testing to identify performance impacts of applications to endpoints, including layered security packages that may cause performance issues and user-experience problems. DISA's Joint Interoperability and Test Command (JITC) should be evaluated to support these standards and testing recommendations.[54]

54 Joint Interoperability Testing Command (JITC). About. Retrieved January 18, 2023. https://jitc.fhu.disa.mil.

Rec #5: Establish/Designate Permanent Chief Experience Officers

Gartner Says, "Nearly 90% of Organizations Now Have a Chief Experience Officer or Chief Customer Officer or Equivalent."[55]

Rec #5 Summary:

- Each MILDEP, component, and agency should **designate a permanent Chief Experience Officer** or other senior employee reporting to the Department CIO. This individual is responsible for measuring user experience, identifying key gaps in service delivery, advising leadership on improvements, and goal setting aligned to related budget needs. The Subcommittee recommends high-performing GS-15s with IT experience, a customer-focused mindset, and the ability to work across the Department to get things done. Each of the CXOs should have the same performance plans that include specific targets for service standardization initiatives, customer experience numbers, and service level targets.
- MILDEPs, components, and agency Chief Experience Officers, in collaboration with their respective CIO leaders, should **share results and best practices to improve DoD-wide outcomes** and to drive transparency and best practices through the DoD CIO Council (See Recommendation #8).

Rec #5 Details:

Chief Experience Officer Responsibilities: The Subcommittee believes it is important for each service and OSD to identify a senior leader, reporting to the MILDEPs, components, and agency CIOs, whose primary duties are the ownership of the IT user experience. A Chief Experience Officer or another senior employee already reporting to the CIO or senior leader within the Department could fulfill this role. **This leader would be responsible for measuring the user experience of the employees within the service, identifying key gaps in service delivery, and advising senior leadership on improvements, goal setting, and related budget needs.**

This role and these responsibilities are also standard within the corporate space. As a result, organizations are taking customer experience (CX) more seriously by committing more resources and talent to the discipline, according to a Gartner 2019 Customer Experience Management survey. In 2017, more than 35% of organizations lacked a CXO or equivalent, but by 2019, only 11% lacked a c-level customer officer.[56]

Additionally, most of the large corporations the Subcommittee interviewed have clear senior leaders identified (often at the vice president level, reporting to the corporate CIO) to own the IT user experience. So, again, this is strong supporting evidence for DoD.

---

55 Omale, Gloria. Garner, Inc. "Gartner Says Nearly 90% of Organizations Now Have a Chief Experience Officer or Chief Customer Officer or Equivalents." February 20, 2020. www.gartner.com/en/newsroom/press-releases/2020-02-10-gartner-says-nearly-90--of-organizations-now-have-a-c.

56 Ibid.

The CXO will help create and drive a user-experience culture in the information technology and IT acquisition organizations. The CXO will be responsible for the following:

- Counseling senior leaders in developing, implementing, and maintaining enterprise IT technologies.
- Defining the top-down scope-specific user-experience challenges, quantifying them where possible, and defining approaches, tools, and budget needs to address them.
    - Conduct a high-level meta-analysis of the current state of the IT user experience;
    - Develop an enterprise understanding of the most critical IT user experience touchpoint, journeys, and gaps;
    - Document and communicate the "case" for change as applicable; and
    - Serve as key software program advisor and facilitator.
- They are influencing the deployment and improvement of the most widely used applications and IT services, which significantly impact IT user experience within the Department.
    - Serve as advisor and facilitator to the specific program managers, specifically to assist in requirements and milestone setting and tracking of program progress against metric targets and budgets;
    - Improve the IT experience by identifying IT pain points and opportunities via the synthesis of data from multiple metrics areas; and
    - Implement digital-user experience approaches, processes, tools, patterns, etc.
- Serve as a facilitator among the relevant programs to assist in identifying gaps and closing them in programs owned by other MILDEPs or components.
    - Identify the most common user journeys that involve interactions with multiple systems and
    - Analyze these experiences via applicable methods to identify pain points and opportunities.

From interviews and research, the Subcommittee believes the CXO model within the Air Force is a strong example of where such a role has been created and is making clear progress towards delivering on this recommendation. Other MILDEPs, components, and agencies should consider adopting a similar position and model and, at a minimum, identify someone no lower than the GS-15 level to fulfill these duties for the team's CXO role at headquarters and within the component agencies.

December marks the one-year anniversary of President Joe Biden's executive order detailing the need for agencies to prioritize and to improve the customer experience. The Department of Homeland Security (DHS) is in the final stages of responding to the president's technological hiring initiative by making job offers before the end of 2022 from almost 1,000 applicants.[57]

DHS Set to Hire 50-100 in CX Office at HQ, from 1,000 Applicants, to Start January 2023

December marks the one-year anniversary of President Joe Biden's executive order detailing the need for agencies to prioritize and to improve the customer experience.

"Our Government must recommit to being 'of the people, by the people, [and] for the people' in order to solve the complex 21st century challenges our Nation faces. Government must be held accountable for designing and delivering services with a focus on the actual experience of the people whom it is meant to serve"

~ President Joe Biden, 13 December 2021

The Department of Homeland Security (DHS) is in the final stages of responding to the president's technological hiring initiative by making job offers before the end of 2022 from the almost 1,000 applicants for the team's CXO role at headquarters and within the component agencies. With several hundred positions to fill across the Department, DHS seeks qualified candidates at the GS-14 or GS-15 grade levels with skill sets comparable to senior product manager, human-centered designer, software engineer, and data science.

An overarching goal for this hiring initiative is to help DHS create a more consistent, standard approach to and accountability for customer experience. As a result of establishing a dedicated customer experience office in headquarters, the organization would encourage a customer experience culture change and collaboration across the Department, serving as a valuable training resource.

With a plan in place, DHS is committed to removing administrative barriers, increasing equity, building trust, and strengthening security. The CX team will help achieve these essential goals.[58]

57 Miller, Jason. Federal News Network. "DHS on cusp of hiring as many as 100 CX experts." December 13, 2022. www.federalnewsnetwork.com/hiring-retention/2022/12/dhs-on-cusp-of-hiring-as-many-as-100-cx-experts.

58 U.S. General Services Administration. "GSA Survey Satisfaction Results." March 2022. www.gsa.gov/reference/reports. The White House. "Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government." December 13, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/.

Rec #6: Centralize Acquisition and Vendor Negotiations Where Possible

Rec #6 Summary:

- DoD should **conduct an assessment** by DBB or a Federally Funded Research and Development Center (FFRDC), under the auspices of the Deputy Secretary of Defense (and shared across the MILDEPs, components, and agencies budget and acquisition communities) **of the technical and cost benefits of migrating to a single or reduced number of Office 365 (O365) tenants**. The assessment, which should be repeated and reported every few years, should include metrics addressing each performance-related item annotated on Recommendation #2 and cost.
- The data generated by this assessment should become **a core tool in associated resource planning and decisions**.
- Align all hardware/computer/device requirements to **a common set of performance and operational standards**, including security protocols, interoperability, and other mission-critical elements.

Rec #6 Details:

Set a Path to a Single or Reduced Tenancy Model: Whether the Department should shift to a "single tenancy" model for basic IT services is among the most difficult the Subcommittee has tried to address. There is little doubt that such a shift could achieve measurable performance and cost improvements if done right. **In the commercial sector, it is considered a best practice.** At the same time, within the Department, for reasons of size, trust, control, and more, achieving a single tenancy state would likely be far more complex. This, therefore, requires the Department to take explicit, continued action to ensure that it is optimizing its IT operations and acquisitions.

O365 is the dominant desktop operating environment in DoD. As in most corporate, public, and private enterprises, DoD users are familiar with and use Office 365's applications and services daily, such as Word, Outlook, Excel, PowerPoint, Teams, etc.

Less visible than the applications themselves, but no less critical to user functionality, operability, and security, is Office 365's concept of "tenants," which refers to the virtual "containers" within O365 which hold customers' information such as users, domains, and configurations.

Presently, DoD operates under a multi-tenant architecture, meaning several O365 tenants support various MILDEPs, components, and agencies. This architecture is expensive, is vulnerable to cyber-attack (owing to the existence of multiple access points), lacks uniform backup processes, promotes inefficient restoration of data and files, and offers less administrative control.

Moreover, as noted elsewhere in this report, among the key user complaints with the current IT constructs are 1) the challenges associated with moving data from location to

location as the result of a permanent change of station move or other geographic change and 2) the challenges of collaborating across multiple components or domains. In an era where interoperability, agility, and flexibility are critical, these challenges too often sub-optimize performance, responsiveness, and mission effectiveness.

Transitioning to a single tenant (or a limited number of tenants) could mitigate several issues and provide the following benefits:

- Increased data security;
- Increased reliability;
- More straightforward system restoration when necessary;
- Easier system/data migration;
- Improved user collaboration; and
- Improved control over software updates and customization.

Moreover, it is the Subcommittee's view that the Department's **current siloed approach to hardware/computer/device, vendor, solution negotiations, and management may deny the benefits that would likely derive from an enterprise-wide acquisition and licensing strategy**.

That said, the Subcommittee acknowledges that inter-service dynamics, and political realities, may preclude the realization of a "single-acquisition" strategy for software buys. Nonetheless, services, components, and agencies may benefit from approaching vendors with a "unified negotiation" strategy to obtain the best pricing. **Minimally, DoD must align all hardware/computer/device requirements to a common set of performance and operational standards, including security protocols, interoperability, and other mission-critical elements.**

Rec #7: Streamline, Standardize, and Consolidate Help Desks Across the DoD

Rec #7 Summary:

- Well-performing help desks are critical for monitoring, delivering, and enabling end-user experience.
- DoD today has a multitude of tiered help desks with inconsistent service levels, metrics, tools, and data collection methods.
- DoD should streamline and consolidate help desk operations for basic unclassified IT support to improve user experience and effectiveness and to overtime spending efficiencies.
- DoD should mandate specific and standardized data collection for all help desks and ensure IT leaders across the enterprise have access to all such data.
- DoD should ensure seamless interoperability between all help desks to maximize the use of available resources across the enterprise.

Rec #7 Details:

As noted above, due to the disjointed organizational structure of DoD IT operations, numerous "help desks" have been created throughout the Department, which includes 13 alone for DISA.

Having multiple help desks utilizing different standards, vendors, systems, and data collection limits the Department's ability to establish enterprise-level trends and improvements; to anticipate and proactively counter technology gaps and potential outages; and to prepare for and react to threat vectors across the portfolio.[59]

Help Desk Impacts: 91% of customer service teams agreed with the statement "our help desk system increases productivity."[60]

Accordingly, the Subcommittee recommends the following:

Consolidate Help Desks: Depending on the IT structural and governance model DoD implements, the Department should consolidate help desk operations; provide specific data collection requirements across the Department; and ensure seamless interoperability between all help desks. Specifically, the Subcommittee recommends considering the following consolidation for basic unclassified IT support: **one help desk for OSD and the 4th Estate, one for each service, and one for the COCOMs combined. Coupled with the features recommended below, this consolidation could dramatically improve the user experience, productivity and garner cost savings which can applied to other underfunded IT initiatives** .

---

59 Trust Radius. "Help Desk Statistics and Trends for 2022." April 21, 2022. www.trustradius.com/buyer-blog/help-desk-statistics.

60 Amaresan, Swetha. Hubspot.com. "Help Desk Management: 13 Key Steps to Follow for Success." June 24, 2022. https://blog.hubspot.com/service/help-desk-management.

To enable this consolidation to succeed, DoD should mandate that each help desk meet a certain level of capabilities (e.g., Tiers 1-3, etc. of user issues) and have a common set of standards/requirements for data collection. Additionally, each help desk must be "interoperable" so that the most appropriate and readily available help desk can resolve the user's problem. When one help desk is unable to rapidly address the user's issue (or has extended wait times), the user is referred to a help desk with appropriate availability or expertise worldwide. Finally, regarding **data collection, each help desk must immediately transmit user information to a central repository to determine enterprise-level user experience trends and rapidly identify systemic issues or threats.**

> ***Customer Perceptions: Sixty-six percent (66%) of customers expect companies to understand their unique needs and expectations, yet 66% say they're generally treated like numbers.***
>
> ***~ Salesforce, 2020***
> www.trustradius.com/buyer-blog/help-desk-statistics

Additionally, this consolidation, coupled with aggressive interoperable cloud services, will provide more enterprise-level effectiveness in the areas of accountability, efficiency, and security:

- **Accountability (Data Standards/Sharing):** If MILDEPs or other components need to own their individual help desk implementations, data standardization and data sharing should be required to ensure proper collection of help desk metrics and accountability.
- **Efficiency (Driven by Cloud Access):** The cloud will allow DoD to consolidate its extensive data center assets further. The Department has started to rationalize and reduce data centers, but significant work still needs to be done to standardize capabilities and practices. Embracing the cloud will provide an opportunity to accelerate and extend those consolidation opportunities and to achieve efficiencies through the rapid deployment of common user services.
- **Security (Cloud Offers Broader Security Options):** An enterprise cloud perspective will enable more centralized management and the wider availability of security service options for cloud adoption by DoD to also include those DoD components with smaller implementation staff and smaller IT budgets.

This federated consolidation approach could eliminate redundancy and provide a more holistic and rapid resolution to user issues while giving DoD better tracking, visibility, and resolution capabilities.

Rec #8: Centralize Reference Architecture, Network, and Security Standards Under DoD CIO and Federate Delivery and User Experience Accountability to the MILDEP CIOs

DoD owns the best single IT enterprise practice in the world, with the implementation of Microsoft Teams due to COVID-19 pandemic pushing millions to telework. Microsoft said this was the largest and fastest estate implemented in the world with 25-50K users transitioned per night. This initiative was directly led by the DoD CIO while ensuing MILDEP, components, and agencies CIOs were held accountable to get necessary sign offs from their superiors. *Hon Dana Deasy*

Rec #8 Summary:

- The current decentralized model leads to a lack of end-to-end ownership of user experience. Currently, each MILDEP is taking a different approach, leading to a fractured user experience across the DoD. The Subcommittee recommends the DoD **move to a Federated model** with the MILDEPs, components, and agency CIOs reporting solid lines to their respective branches and strong dotted lines to the DoD CIO. The DoD CIO should have significant input into the performance evaluation of the MILDEP and agency CIOs.
- This group should **create a chartered DoD CIO Council** composed of MILDEPs, components, and agency CIOs, chaired by the DoD CIO with some level of budgetary O365 authority. This group would collectively own setting standards across the DoD under the leadership of the DoD CIO. That standards setting should include decisions like how many disparate Office 365 tenants to deploy; the potential move to a single sign-on; multi-factor authentication domain; endpoint refresh schedule; and which best practices among those of existing departments should be leveraged as a DoD standard. The DoD CIO should serve as the final vote in the event the DoD CIO Council cannot reach alignment on issues.
- The CIO Council should utilize the CXOs to report on key metrics and to assist in evaluating, planning, implementing, and reporting on IT key initiatives under the Council's purview.
- The Subcommittee recommends centralizing the reference architecture, security stack, and transport layer in an organization with direct line reporting to the DoD CIO.

- Currently, each of the MILDEPs is undertaking a different strategy to improve end-user experience, ranging from VDI to using the internet as a WAN backbone for NIPR traffic. The Subcommittee recommends the **DoD CIO move quickly to understand the merits of the different approaches and to establish one as the de facto standard** for the DoD to prevent a fractured user experience.

Rec #8 Details:

The Subcommittee further recommends MILDEPs, components, and agency CIOs have the ultimate ownership and accountability for user experience, with the CIO Council serving as the alignment vehicle across those groups.

The MILDEP CXOs will be key contributors and advisors to the CIO Council. CXOs will help share metrics, initiative planning and implementation roadmaps, and foster the sharing of best practices and common approaches across the MILDEPs and components as it relates to providing IT service and to meeting the user experience needs within the organization.

- The Subcommittee recommends this group drive some immediate short-term decisions, including:

    1. Charter for the CIO Council, including aligning decisions at the group level versus which decisions are entirely at the discretion of the services, components, and agency CIOs;
    2. Move to a single O365 tenant or federation between the existing tenants;
    3. Move to a single sign-on, multi-factor authentication domain across the DoD;
    4. Select an endpoint monitoring solution, and deploy it across ALL DoD endpoints to measure actual user experience;
    5. Align on a dashboard of measures that are critical to user experience, and review as a group monthly;
    6. Align on which approach, Navy's VDI or Army's Internet as WAN best meets user experience, and set as a North Star to migrate all of DoD over some time; and
    7. Create a set of standard images and a lab to measure any impact on performance when adding new software to the images. This approach should include alignment on the security stack across the endpoints, network, and perimeter.

Rec #9: Clearly Define DISA's Role in the Unclassified User Experience

Rec #9 Summary:

- For the basic unclassified user experience, DoD **should review the required use of DISA services, focusing on balancing the benefits of enterprise-wide oversight** against MILDEPs, components, and agency needs to meet user effectiveness and service-unique requirements.
- DoD should inventory all unclassified IT functions to eliminate duplication, thereby, allowing scarce funding for other pressing needs.
- DoD should assess the costs, benefits, and potential drawbacks of directing increased use of DISA engineering and system management services and DISA-managed acquisition vehicles by MILDEPs, components, and agencies.

Rec #9 Details:

DISA is one of the largest IT organizations in the world, with a massive and complex global mission set. It is composed of over 7,000 military and civilian employees.[61] DISA is responsible for enabling, securing, and improving the communications backbone for our global command and control, providing quality and timely access to information by all US forces worldwide, and implementing and maintaining classified and unclassified IT system architectures.[62]

The job is immense. It requires massive amounts of data, network monitoring, and security capabilities; a highly skilled workforce; and consistent access to new technologies. Thus, the Subcommittee believes that in any DoD IT structure, some DISA-like organization is necessary. In addition, DISA provides valuable engineering, design, acquisition, implementation, security, and system management services to the Department, the duplication of which within MILDEPs, components, and agency would be needlessly expensive and impact the ability to use scarce funds elsewhere.

Nevertheless, when it comes to basic unclassified IT effectiveness, DISA, in its current form, simply does not have the necessary user-level monitoring/access or directive authorities to drive significant improvements in the individual user's experience enterprise-wide.

---

61 Defense Information Systems Agency. Careers. Retrieved November 4, 2022. https://www.disa.mil/careers.

62 Defense Information Systems Agency. Mission. Retrieved November 4, 2022. https://www.disa.mil.

It is important to note that calls to repair the Agency are not new. Since its establishment in 1960 as the Defense Communications Agency (renamed in 1991), DISA's customers at multiple levels have called for its reform, restructure, revamping, re-scoping, reengineering, and otherwise "re-doing." "In 2018, Rep. Mac Thornberry, then Republican chairman of the House Armed Services Committee, proposed draft legislation Tuesday that would eliminate the Defense Information Systems Agency by 2021."[63] These calls are often inherent in any organization that provides services that can never be delivered acceptably "fast, good, and cheap" enough. It is also aggravated by a pricing structure in which DISA must recover operating costs from its customers for services that can be obtained at lower cost directly from vendors. Additionally, individual user problems may involve multiple issues (e.g., redundant security layers, available bandwidth, hardware obsolescence, etc.). As a result, DISA is often the focus of frustration, even though, in many cases, the Agency has little visibility or oversight of the entire "IT chain" down to the user level.

DISA, like any large organization, requires consistent review and would benefit from ongoing process improvement and periodic restructuring. However, it is beyond the scope of this Study to provide comprehensive change recommendations. Moreover, it is clear that there is no uniform policy mandating the use of the broad range of DISA's offerings or permitting it to monitor the user level. This situation appears to have the following significant impacts:

- There is no DoD entity responsible for the individual user experience, enterprise-wide;
- DoD is denied the benefits of enterprise-wide system management, including accurate end-to-end performance monitoring down to all users in the Department;
- DoD is likely acquiring IT systems and services sub-optimally, not benefitting from cost economies of scale that could come with the more enterprise-wide acquisition;
- DoD is complicating its naming and other domain management processes by allowing multiple authorities to establish standards and conventions; and
- DoD may be harming its cybersecurity posture by allowing the implementation of multiple domains along MILDEPs, components, and agency lines.

63 Mitchell, Billy. Fedscoop. "Mac Thornberry wants to eliminate DISA." April 18, 2018. https://www.fedscoop.com/eliminate-disa-legislation-mac-thornberry.

Implementation Roadmap

The following is a notional guide to implement the Recommendations to better posture the DoD IT enterprise capabilities addressing the current and future gaps in the IT user experience of DoD stakeholders. The Subcommittee recommends the Deputy Secretary of Defense direct the Chief Information Officer to identify an Office of Primary Responsibility (OPR) for each of the Recommendations below to begin implementation. OPRs will develop a plan of action and milestones to brief the Deputy Secretary of Defense via the Deputy's Management Action Group (DMAG). The steps are ordered based on logical sequencing as well as the assumed magnitude of the change/length of time to enact. While there are some dependencies across these roadmap items, some steps can be implemented in parallel or started, and timeline optimized, depending on resources and final implementation schedules and review and sign-on.

1. **Rec #8**: **Form DoD CIO Council with DoD CIO, MILDEP CIOs, and Charter**
    a) Draft DoD CIO Council member list and charter (3 months)
    b) Final member list and charter approved by DoD CIO and DepSecDef (6 months)
2. **Rec #5 & #8**: **Establish/Designate Permanent Chief Experience Officers and Engage in the Work of the DoD CIO Council (modeled after AF CXO)**
    a) All MILDEPS and OSD CXOs identified or hired (all by 12 months, some sooner)
3. **Rec #1**: **Implement Endpoint Monitoring Across ALL Devices, and Prioritize DoD IT Funding to Consistently Monitor and to improve End-user Experience (subset and over time towards goal and all endpoints)**
    a) 10% of end points monitored across DoD (6 months)
    b) 25% devices are monitored across DoD (12 months)
    c) 90+% of devices are monitored across DoD (24 months)
4. **Rec #2: Leverage Metrics for IT User Experience to Drive Accountability from Service Providers and to Deliver Acceptable Quality of Service**
    a) Key IT Metrics defined (3 months)
    b) Key Metrics monitored and dashboard available (9 months)
    c) Action plan created based on actual and target key metrics (12 months)

5. **Rec #3**: **Review and Upgrade Device Replacement Strategy and Device Life Cycle Management**
    a) Revise Device Replacement Strategy (4 months)
    b) Upgrade all devices based on new strategy (budget dependent) (36 months, subset device upgrade sooner)
6. **Rec #8: Define Common Standards and Policies through DoD CIO Council:**
    a) Define Network and Security Standards (9 months)
    b) Define Standard Endpoint Configurations (12 months)
    c) Define Reference Architecture (15 months)
7. **Rec #4: Simplify Security Layers, Move Faster to Zero Trust/Application-Level Security**
    a) Simplify endpoint anti-malware deployment (12 months)
    b) Implement new Security standard (14 months)
    c) Implement Zero Trust for key applications (24 months)
8. **Rec #7: Streamline, Standardize, and Consolidate Help Desks Across the DoD**
    a) Timeline for DISA to consolidate to 1 Help Desk (15 months)
    b) Timeline for all DoD to consolidate to 1 Help Desk (24 months)
9. **Rec #9: Clearly Define DISA's Role in the Unclassified User Experience**
    a) Review and confirm DISA's responsibilities (6 months)
10. **Rec #6: Centralize Acquisition and Vendor Negotiations Where Possible**
    a) Review and consolidate acquisition and vendor negotiations for Basic IT Services (Microsoft, Security, Monitoring) (12 months)

Conclusion

DoD must shift its perspective and approach towards enterprise-wide IT user experience to one that understands efficient and reliable technology is essential to every single operation, from day-to-day support tasks all the way to the warfighters and the civilians that support them and the mission.

- The private sector applies industry best practices to prioritize enterprise IT end-user experience focused on this Study's eight Key Findings and Recommendations. The Subcommittee understands that all recommendations cannot be implemented overnight but is confident that establishing a CXO for the MILDEPs, components, and agencies will facilitate enhanced implementation of the remainder of the recommendations.
- It is critical to define the key metrics to determine user experience, measure those metrics broadly and down to the device endpoints, publish and review the results internally, and use them to drive improvement and accountability.
- IT Security is critical; however, the current way security is layered and deployed redundantly down to the endpoints needs to be reviewed, simplified, and move faster to zero trust to simplify the security even further. The current pilots within DISA and other parts of the Department are showing promise and should help to accelerate this direction further.
- Upgrade devices that exceed the recommended 36-48 months of usage guidance with clear budget support.
- Through research and commentary from IT industry executives, organizations conveyed that prioritizing the IT end-user experience significantly benefits employees by decreasing downtime and work-stoppage issues, which results in happier employees and aids in the retention of skilled employees. With the war on recruiting and retaining talent, the DoD must ensure employees have the proper resources to conduct their routine work.

Lastly, the Subcommittee recommends further investigation or future studies on the following topics:

- Modernize or replace the Defense Property Accounting System and the process for accounting for IT inventory;
- Update current budgeting and planning process for IT capabilities and resources;
- Technical and cost benefits of migrating to a single tenant across all of DoD; and
- Enterprise vendor management to provide transparency and accountability across DoD.

Signatures

David Beitel
Subcommittee Chair

Safroadu Yeboah-AmanKwah
Subcommittee Co-Chair

Anand Bahl
Subcommittee Member

COL Gregory Bowman USA (Ret)
Subcommittee Member

Sally Donnelly
Subcommittee Member

Marachel Knight
Subcommittee Member

Brig Gen Bernard Skoch USAF (Ret)
Subcommittee Member

Stan Soloway
Subcommittee Member

GEN Joseph Votel USA (Ret)
Subcommittee Member

Appendices

Appendix A - Terms of Reference

Appendix B - Presentation to the Board

Appendix C - Subcommittee Member Biographies

Appendix D - Contributors List

Appendix E - Bibliography

Appendix F - Questionnaire and Survey Forms

Appendix G - Public Comments

Appendix H - Acronyms

Appendix A: Terms of Reference

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY - 9 2022

MEMORANDUM FOR DEFENSE BUSINESS BOARD

SUBJECT: Terms of Reference — Recommendations to Improve User Experience on the Department of Defense's Non-Classified Internet Protocol Router Network

Information Technology (IT) is the building block of any modern organization, whether commercial or governmental. An organization's IT is one of its most critical components. When these capabilities fail, are degraded, or have extreme performance issues, there are disturbances to everything from basic administration, finance, communications, and contracting to mission-critical applications supporting warfighters around the globe.

The Department of Defense (DoD) understands its IT infrastructure and systems are essential to maintaining its warfighting superiority, and the DoD has invested substantial resources and effort into building this critical capability. In order to continue to maintain our information superiority and to provide the tools our workforce needs to innovate, DoD personnel must have access to reliable, secure, responsive, and rapid IT.

Despite ongoing efforts, DoD IT has not historically provided a consistent high quality user experience. Additionally, the COVID-19 pandemic forced millions of military and civilian personnel into some degree of teleworking, further stressing DoD's IT infrastructure and systems. The DoD has significantly increased network capacity to accommodate this surge and is actively pursuing modernization efforts (updating hardware, pursuing Zero Trust network architecture, etc.), but IT issues are still regularly cited as barriers to DoD personnel productivity and ability to contribute.

Therefore, I direct the Defense Business Board ("the Board"), through its Board Business Operations Advisory Subcommittee ("the Subcommittee"), to provide recommended approaches to the DoD for rapidly improving IT user experience without negatively impacting security or resiliency. Specifically, the Board, through its Subcommittee, will focus on the following actions:

- Identifying industry organizational and technical best practices, and user experience frameworks to maintain a positive user experience that facilitates productivity;
- Evaluating the current state of DoD user experience for basic IT services across the Department;
- Providing case studies and distilling best practices from relevant private sector companies on how they maintain and enhance their employees' IT user experience;
- Developing recommendations to manage and improve DoD user experience for basic IT services across the Department;

- Any related matters the Board determines relevant to this task.

I direct the Subcommittee to submit its independent recommendations to the full Board for its thorough consideration and deliberation at a properly noticed public meeting, unless it must be closed pursuant to one or more of the Government in the Sunshine Act exemptions.

In conducting its work, the Board and its Subcommittee have my full support to meet with Department leaders, and all requests for data or information shall be honored that may be relevant to its fact-finding and research under these Terms of Reference, consistent with applicable law and regulations. As such, the Office of the Secretary of Defense and DoD Component Heads are requested to cooperate and, within five business days, facilitate requests by Board staff regarding access to relevant personnel and information deemed necessary, as directed by paragraphs 5.1.8. and 5.3.4. of DoD Instruction 5105.04, "Department of Defense Federal Advisory Committee Management Program," and in conformance with applicable security classifications.

Once material is provided to the Board, it becomes a permanent part of the Board's record. Components are reminded that all data/information provided is subject to public inspection unless the originating Component office properly marks the data/information with the appropriate classification and Freedom of Information Act exemption categories before the data/information is released to the Board. The Board has physical storage capability and electronic storage and communications capability on both unclassified and classified networks to support receipt of material up to the Secret level. Each Component should remember that Board members, as special government employee members of a DoD federal advisory committee, will not be given any access to the DoD network, to include DoD email systems.

The Subcommittee shall not work independently of the Board's charter. The Board and the Subcommittee will operate in conformity with and pursuant to the Federal Advisory Committee Act, the Government in the Sunshine Act, and other applicable federal statutes and regulations. The Subcommittee and individual Board members do not have the authority to make decisions or provide recommendations on behalf of the Board nor report directly to any federal representative. The members of the Subcommittee and the Board are subject to certain Federal ethics laws, including 18 U.S.C. § 208, governing conflicts of interest, and the Standards of Ethical Conduct regulations in 5 C.F.R., Part 2635.

Thank you in advance for your cooperation and support to this critical undertaking to inform subsequent decisions on how the Department addresses national security challenges in the coming decades. My points of contact for this effort are CAPT Daryl M. Wilson, USN, Senior Military Representative to the Board at (808) 594-3324 or daryl.m.wilson4.mil@mail.mil, and Jennifer Hill, Executive Director of the Board at (571) 342-0070 or jennifer.s.hill4.civ@mail.mil.

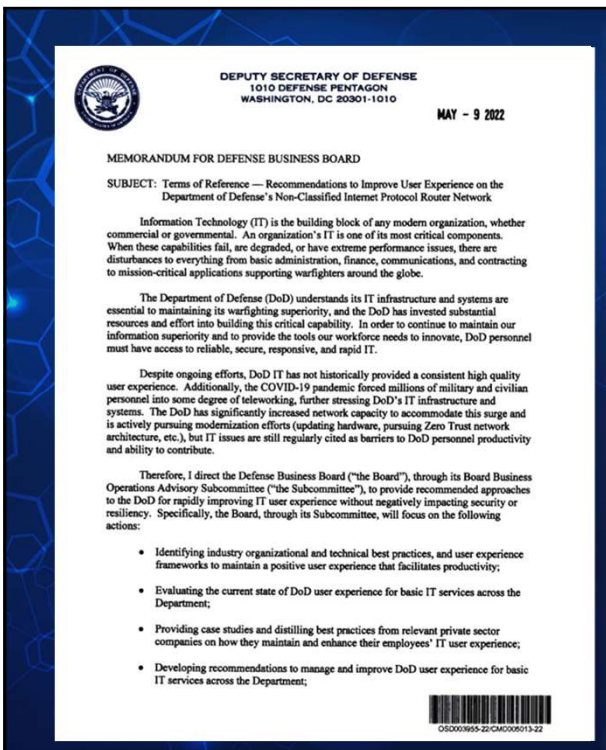
This page left intentionally blank

Appendix B: Presentation to the Board

DEFENSE BUSINESS BOARD

EVALUATION OF DOD IT USER EXPERIENCE

February 02, 2023 — *FY-23-02*



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY - 9 2022

MEMORANDUM FOR DEFENSE BUSINESS BOARD

SUBJECT: Terms of Reference — Recommendations to Improve User Experience on the Department of Defense's Non-Classified Internet Protocol Router Network

Information Technology (IT) is the building block of any modern organization, whether commercial or governmental. An organization's IT is one of its most critical components. When these capabilities fail, are degraded, or have extreme performance issues, there are disturbances to everything from basic administration, finance, communications, and contracting to mission-critical applications supporting warfighters around the globe.

The Department of Defense (DoD) understands its IT infrastructure and systems are essential to maintaining its warfighting superiority, and the DoD has invested substantial resources and effort into building this critical capability. In order to continue to maintain our information superiority and to provide the tools our workforce needs to innovate, DoD personnel must have access to reliable, secure, responsive, and rapid IT.

Despite ongoing efforts, DoD IT has not historically provided a consistent high quality user experience. Additionally, the COVID-19 pandemic forced millions of military and civilian personnel into some degree of teleworking, further stressing DoD's IT infrastructure and systems. The DoD has significantly increased network capacity to accommodate this surge and is actively pursuing modernization efforts (updating hardware, pursuing Zero Trust network architecture, etc.), but IT issues are still regularly cited as barriers to DoD personnel productivity and ability to contribute.

Therefore, I direct the Defense Business Board ("the Board"), through its Board Business Operations Advisory Subcommittee ("the Subcommittee"), to provide recommended approaches to the DoD for rapidly improving IT user experience without negatively impacting security or resiliency. Specifically, the Board, through its Subcommittee, will focus on the following actions:

- Identifying industry organizational and technical best practices, and user experience frameworks to maintain a positive user experience that facilitates productivity;
- Evaluating the current state of DoD user experience for basic IT services across the Department;
- Providing case studies and distilling best practices from relevant private sector companies on how they maintain and enhance their employees' IT user experience;
- Developing recommendations to manage and improve DoD user experience for basic IT services across the Department;

OSD003955-22/CMD005013-22

On May 9,2022, the Deputy Secretary of Defense tasked the DBB to provide recommendations to improve IT End-user Experience:

- The current state of DoD user experience for basic Non-Classified Internet Protocol Router Network (NIPR) IT services across the Department
- Best practices from relevant private sector companies on how they maintain and enhance their employees' IT user experience
- Industry organizational and technical best practices and user experience frameworks to maintain a positive user experience that facilitates productivity
- Recommendations to manage and to improve DoD user experience for basic IT services across the Department

SUBCOMITTEE MEMBERS

- David Beitel, **Chair**
- Safroadu Yeboah-Amankwah, **Co-Chair**
- General Joseph L. Votel (ret)
- Sally Donnelly
- Anand Bahl
- Colonel Gregory Bowman (ret)
- Marachel Knight
- Brigadier General Bernard Skoch (ret)
- Stan Soloway

ITSC EXPERTISE

- **Industry Tech**: Anand Bahl, David Beitel, Marachel Knight, Safroadu Yeboah-Amankwah, General Joseph L. Votel (ret), Brig. Gen. Bernard Skoch, (ret) COL Greg Bowman (ret)
- **Military**: General Joseph L. Votel (ret), COL Greg Bowman (ret), Brig. Gen. Bernard Skoch (ret)
- **DoD & Federal Policy Advisors**: Sally Donnelly, Stan Soloway

Approach& Methodology

DEFENSE BUSINESS BOARD
OFFICE OF THE SECRETARY OF DEFENSE

- **Six Month Study**
- **Interviewed 29+ DoD Leaders and IT Industry Professionals**
- **Conducted Survey w/ Results from ~20,000 Participants**
- **Received Quantitative and Qualitative IT user Experience Feedback from JSP Users**
- **Analyzed Data from a Literature Review Grounding Assumptions to Provide Context for Findings**

Background

The Department of Defense:

America's Largest Government Agency

- 3.4 million military and civilian personnel
- $816 billion annual budget

Organization of this Magnitude Must Provide

- The requisite IT infrastructure
- Fully equipped personnel to accomplish jobs and execute DoD'smission

IT Networks Need to be Mobile Enough to Support

- Missions around the world
- Collaboration with any partners as mission requires, 24/7/365

IT infrastructure and services must address

- Frustration with the state of IT and work-stoppage issues
- Poorly-rated customer experience

Invested resources and improvements in building critical IT capabilities have yet to provide a consistent high-quality user experience across the enterprise

Key Findings

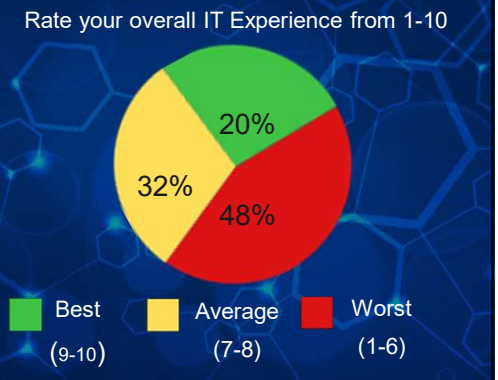
- Lack of actionable performance metrics for enterprise-wide IT user experiences
- 80% of survey respondents rate user experience average or below
- Insufficient infrastructure to proactively isolate performance Issues
- Broad end-point disparities in and among user groups
- Varying and siloed IT policies cause inefficiencies across the DoD
- Redundant deployment of security and cybersecurity tools
- Insufficient IT funding & lagging acquisition implementation
- MILDEPs approach IT user experience & effectiveness differently

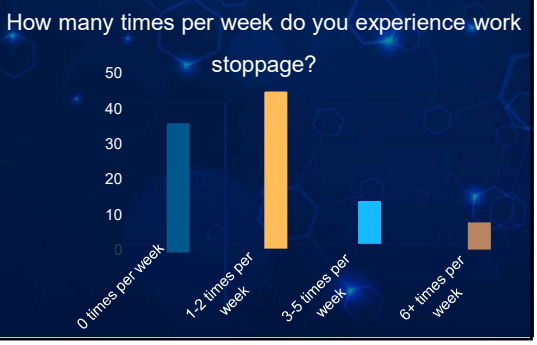
Lack of Actionable Performance Metrics for Enterprise IT User Experiences

- Successful IT services must have:
  - Complete set of metrics to measure the successful delivery and usefulness of service
  - Clear understanding of the needs of those being served and who is providing the service
- Customer experience maturity model
  - Each federal agency fits into one of five levels of user/customer experience maturity
    - Reactive, Tactical, Strategic, Foundational, Customer-Centric
      - DoD is currently in the Reactive Stage, a rudimentary understanding of customer experiences
- Industry Best Practice: Net Promoter Score (NPS) Metric
  - 2/3 of Fortune 1000 companies utilize NPS to measure customer sentiment

80% of Survey Respondents Rate User Experience Average or Below

- Survey results of 20,000 Joint Services Provider customers reveal
  - Consistent problems with log-on times, ticket frequency, IT-driven work stoppages, and re-authentication frequency, independent of onsite vs remote work
- Missing user experience common metrics
  - No enterprise-wide readily identifiable, consistent, transparent, and comprehensive user-satisfaction assessments across the DoD
- Sub-optimal IT services
  - Work-stoppages negatively impact productivity & morale
  - JSP Survey indicates sizeable productivity losses
  - DoD employees and uniformed service members appear to accept sub-optimal IT services as the norm;
  - In industry, this would be recognized as a significant recruitment and retention challenge



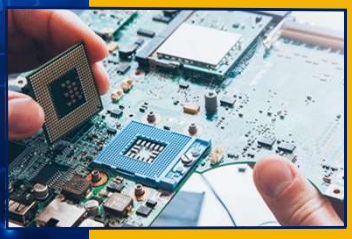


Insufficient Infrastructure to Proactively Isolate and Resolve Performance Issues

- Inconsistent or lack of Endpoint Monitoring on devices
  - Monitoring software deployed inconsistently across end user devices, or in many cases not at all due to budget constraints
  - Lack of data on actual user endpoint experience: System crashes, application crashes, slow performance due to excessive CPU or memory utilization
  - Lack of real-time data makes it challenging for helpdesks to troubleshoot user issues
- Siloed Help Desks/Cumbersome DISA JSP Ticketing Process
  - Service not managed end to end from endpoint, through the network, and out to the internet
  - Multiple help desks that each own their portion of the user experience
  - Inefficient and costly to staff, operate, and maintain multiple helpdesks
- Lack of Standard Images/configurations
  - Multitude of images/configuration make every issue resolution a unique investigation

Broad End-Point Disparities in and Among User Groups

- Antiquated Hardware for modern applications
  - Personnel conducting critical work on substandard devices
  - Modern applications (e.g. VC, cloud productivity, security) not supported by many end-points
- Sub-standard Life Cycle Replacement (LCR)
  - Accurate/holistic accounting of age/configuration of end-devices unavailable
  - Hardware replacement of approx 48 months vs. industry practice of 36 months
- Significant IT management challenges resulting
  - Lack of standard images and efficient application testing
  - High complexity for help desks
  - Increased security exposure



Varying and Siloed IT Policies Cause Inefficiencies Across DoD

- DoD CIO
  - Responsible for implementing standards and policy across DoD but has no authority over MILDEP CIOs
  - Ad hoc CIO council not chartered to review user experience metrics and produce performance based results
- DoD Governance Structure
  - Siloed and inconsistent DoD IT policies, ownership, and services deployment
  - Current model is highly decentralized with the majority of decision making authority with the MILDEP CIOs
  - Examples of good direction in each of the MILDEPs but no overall alignment on best practices or vision to move to common standards across the MILDEPS

Redundant Deployment of Security and Cybersecurity Tools

- Layered and Redundant Cyber Security
  - Reports of multiple/redundant security applications installed on devices negativity impacting usability by competing for local CPU, memory and disk resources
  - Lack of critical lab testing for interactions of layers, security patches, and software updates results in needlessly high CPU utilization
- Work Stoppage
  - Lengthy login times produced by authentication scripts contribute to widespread loss of productivity within DoD
- Zero Trust Framework
  - Complete user authentication across all work flows to ensure impenetrable security
  - Will not be available to agencies until 2027

Insufficient IT Funding & Acquisition Implementation

- IT Funding
  - Inadequately funded IT resulting in outdated hardware, software and IT infrastructure
  - IT funding not “fenced;” often used as “bill payer” for other mission-related requirements
  - Advent of IT Modernization fund could help but funding levels fluctuate greatly
- Lagging Behind Industry Best Practices
  - Modernizing current hardware and software across DoD
  - Identifying the future skills needed for cloud-based services
  - Conducting regular evaluations of customer experiences and user needs
- It’s about more than just IT
  - Current DoD IT procurement processes are not clearly or consistently aligned with either end user needs or common standards that enable efficiency, performance, and interoperability
  - Procurement silos exacerbate the ability of components to ensure high UX

MILDEP Approach the IT User Experience & Effectiveness Differently

- DoD has a “Title 10-driven” IT organizational structure
  - Decentralized budget authority
  - Consent-based governance
- MILDEPs have embarked on separate paths to achieve their organizational goals and user needs
  - Department of the Army
    - Bring Your Own Device (BYOD) using VDI (20,000 users)
    - Moving away from DISA and testing a network concept called “internet as WAN”
    - Deployed a single, world-wide help desk to provide technical support
  - Department of the Air force
    - Created a Chief of User Experience Position
    - Utilizes User Satisfaction Surveys to the entire force
      - Tracks each respondent’s key demographics
      - Understand specific users IT issues
    - Endpoint monitoring for 6500 users with funding for 25K additional users
    - Enterprise performance management system conducting holistic network monitoring across 50 bases
  - Department of the Navy
    - Implementation of a VDI with a cloud-delivered desktop
    - A BYOD program w/o uses of CAC
    - Plans to employ over 200,000 virtual desktops

Recommendations

"Government must be held accountable for designing and delivering services with a focus on the actual experience of the people whom it is meant to serve"

- Centralize Reference Architecture, Network and Security Standards Under DoD CIO and Federate Delivery and User Experience Accountability to the MILDEP CIOs
- Establish/Designate Permanent Chief Experience Officer
- Implement End-Point Monitoring across ALL Devices and Prioritize DOD IT Funding to Consistently Monitor and Improve End-User Experience
- Leverage Metrics for IT User Experience to Drive Accountability from Service Providers and Deliver Acceptable Quality of Service
- Review and Upgrade Device Replacement Strategy and Device Life Cycle Management
- Simplify Security Layers, Move Faster to Zero Trust/Application-Level Security
- Streamline, Standardize, and Consolidate Help Desks Across the DoD
- Clearly Define DISA's Role in the Unclassified User Experience
- Centralize Acquisition and Vendor Negotiations Where Possible

Centralize Reference Architecture, Network and Security Standards Under DoD CIO and Federate Delivery and User Experience Accountability to the MILDEP CIOs

- Move to a Federated model with the MILDEPs, components, and agency CIOs
  - Create a DoD CIO Council of the above groups to align on common standards and best practices to leverage as a DoD standard
  - Continue to hold the MILDEP CIOs accountable for delivery and give decision making authority within the best practices defined by the Council
  - The DoD CIO should serve as the tie breaking vote and final decision maker
- Centralize the reference architecture, the security stack, and transport layer in an organization with direct line reporting to the DoD CIO
- DoD CIO to evaluate the merits of the different technical approaches of improving user experience across the MILDEPs
  - Establish a single technical standard and approach for the DoD to prevent continued fractured user experience

Establish/Designate Permanent Chief Experience Officers

- MILDEP to designate a permanent Chief Experience Officer (CXO) who is responsible for:
  - Measuring User Experience
  - Identifying key gaps in delivery of service
  - Counseling senior leadership on improvements, etc.
- CXOs Performance Plans Designed for Specific Targets
  - Service standardization initiatives
  - Customer experience numbers, etc.
- MILDEPs, components, and agency Chief Experience Officers, in collaboration with their respective CIO leaders, should:
  - Share results and best practices to improve DoD-wide results and to drive transparency and best practices

Implement End-Point Monitoring across ALL devices and prioritize DOD IT funding to consistently monitor and improve End-User Experience

- Consistently and accurately measure end point performance and health
  - Fund and deploy endpoint monitoring solution on **ALL** DoD endpoint devices
  - Provide data for end-to-end user experience metrics
  - Use experience improvement targets as critical objective for annual DoD-level IT investment/budget prioritization
- Recognize and prioritize IT capabilities to ensure productivity and employee engagement
- Establish the structure and expertise to resolve IT-related work stoppage issues
  - Must adopt a culture of continuous improvement in IT service measurement and delivery
  - Establish accountability for resolving issues including cross-enterprise collaboration to address critical issues
  - Mandate and accelerate the adoption of **interoperable** enterprise cloud services

Leverage Metrics for IT User Experience to Drive Accountability from Service Providers and Deliver Acceptable Quality of Service

- Define, log, report transparently, and measure against appropriate targets
  - Define the critical metrics that capture end user experience
  - Metrics should be reviewed regularly by CIO Council with the MILDEP CIOs, CXOs, and DepSecDef
  - Utilize metrics and end user survey data to drive accountability from internal team and vendor service providers
- CDAO to provide a centralized data warehouse and dashboards for metrics data in ADVANA
- Prioritize User Experience at the same level as Return on Investment(ROI) in determining IT roadmaps and future budget investments decisions
- Conduct IT Experience and Satisfaction surveys across all levels of DoD IT on a regular basis
  - Ensure consistency across survey questions so improvement can be measured

Review and Upgrade Device Replcement Strategy and Device Life Cycle Management

- Issue policy that mandates an endpoint refresh cycle timeline of 3-4 years
  - Requirements must be in all endpoint contracts
  - Must be specifically defined and protected in departmental and component budgets
- Include specific line items for IT modernization in each budget submission
  - Must define the desired/expected end-state
  - Must define how progress toward the end-state is to be measured and reported
- Review and update DPAS IT requirements to reflect current nature of IT hardware systems

Simplify Security Layers, Move Faster to Zero Trust/Application-Level Security

- Establish DoD-wide security standards to be adhered to by all MILDEPs, components, and agencies throughout DoD
  - End-to-end framework, from endpoint through network to perimeter
  - DoD CIO should establish standards centrally
- Establish lab testing to identify performance impacts of applications to endpoints, including layered security packages
- Accelerate deployment of Zero Trust

Streamline, Standardize, and Consolidate Help Desks Across the DoD

- Well-performing help desks are a critical element
  - Monitoring, delivering, and enabling end-user experience.
- DoD, today, has a multitude of tiered help desks with inconsistent service levels, metrics, tools, and data collection methods
- Streamline and consolidate help desk operations for basic unclassified IT support to:
  - Improve user experience and effectiveness
  - To over time derive spending efficiencies
- Mandate specific and standardized data collection for all help desks
  - Ensure IT leaders across the enterprise have access to all such data
- Ensure seamless interoperability between all help desks to maximize use of available resources across the enterprise

Clearly Define DISA's Role in the Unclassified User Experience

- DISA's role in user experience must be specifically defined based on its actual capabilities

- DISA, like any large organization, requires consistent review and would benefit from ongoing process improvement and periodic restructure. Accordingly, DoD should
  - Review the use of DISA services to balance the benefits of enterprise-wide oversight against MILDEPs, components, and agency needs (as well as ongoing efforts).
  - Assess the costs, benefits, and potential drawbacks of directing increased use of DISA engineering and system management services
  - Assess DISA-managed acquisition vehicles by MILDEPs, components, and agencies

Centralize Acquisition and Vendor Negotiations Where Possible

- Conduct an assessment by DBB or a Federally Funded Research and Development Center (FFRDC)
  - Evaluate technical and cost benefits of migrating to a single or reduced number of Office 365 (O365) tenants. This would include both performance implications as well as implications/reality of increasingly centralized procurement

- Data generated by this assessment as well as assessment of device ages, must become a core tool in resource planning and decisions

- Align all hardware/computer/device requirements to a common set of performance and operational standards including:
  - Security protocols
  - Interoperability
  - Other mission critical technical elements

RECOMMENDATIONS	IMPLEMENTATION	TIMELINE IN MONTHS
Form DoD CIO Council with DoD CIO, MILDEP CIOs, and Charter		
	Draft DoD CIO Council Member List and Charter	3 Months
	First Member List and Charter Approved by DoD CIO and DepSecDef	6 Months
Establish/Designate Permanent Chief Experience Officers and Engage in the Work of the DoD CIO Council		
	All MilDeps and OSD CXOs identified or hired	12 Months
Implement Endpoint Monitoring Across ALL Devices and Prioritize DoD IT Funding to Consistently Monitor and to Improve End-user Experiences		
	10% of end points monitored across DoD	6 Months
	90+ % of devices are monitored across DoD	12 Months
	All devices are monitored across DoD	24 Months
Leverage Metrics for IT User Experience to Drive Accountability from Service Providers and Deliver Acceptable Quality of Service		
	Key IT Metrics defined	3 Months
	Key Metrics monitored and dashboard available	9 Months
	Initial Action plan created based on actual and target key metrics	12 Months
Review and Upgrade Device Replacement Strategy and Device Life Cycle Management		
	Revise Device Replacement Strategy (see recommended threshold	4 Months
	Upgrade all devices based on new strategy (budget	36 Months

RECOMMENDATIONS	IMPLEMENTATION	TIMELINE IN MONTHS
Define Common Standards and Policies through DoD CIO Council		
	Define Network Standards	9 Months
	Define Security Stan	9 Months
	Define Standard Endpoint Configuration	12 Months
	Define Reference Architecture	15 Months
Simplify Security Layers, Move Faster to Zero Trust/Application-Level Security		
	Simplify end point anti-malware deployment	12 Months
	Implement new Security standard	14 Months
	Implement Zero Trust for key applications	24 Months
Streamline, Standardize, and Consolidate Help Desks Across the DoD		
	Timeline for DISA to consolidate to 1 Help Desk	15 Months
	Timeline for all DoD to consolidate to 1 Help Desk	24 Months
Clearly Define DISA's Role in the Unclassified User Experience		
	Review and confirm DISA's responsibilities	6 Months
Centralize Acquisition and Vendor Negotiations Where Possible		
	Review and consolidate acquisition and vendor negotiations for Basic IT	12 Months

Future Studies

- Modernize or replace the Defense Property Accounting System (DPAS) and the process for accounting for IT inventory
- Update current budgeting and planning process for IT capabilities and resources
- Technical and cost benefits of migrating to a single Microsoft O365 tenant across DoD
- Enterprise vendor management to provide transparency and accountability across DoD


Questions and Discussion

This page left intentionally blank

Appendix C: Subcommittee Member Bios

DEFENSE BUSINESS BOARD

DAVID BEITEL (Chair)

CHIEF TECHNOLOGY OFFICER, ZILLOW GROUP

As Chief Technology Officer of Zillow Group, David Beitel oversees the internal and external technical engineering, product development, and technology operations teams.

David joined Zillow in 2005 as a member of the founding team and is one of the company's first executive leaders. In addition to his role as CTO, David helped develop and build Zillow from a small startup to a household name and was named the region's Most Innovative CTO by the Puget Sound Business Journal in 2012. He also received the Large Enterprise Seattle CIO ORBIE Award for 2021.

Prior to Zillow, David was CTO of Expedia, where he joined as one of its earliest team members and spent 12 years. David started his career at Microsoft in the handheld computing group.

David earned a Bachelor of Science in Computer Science and Master of Engineering in Computer Science from Cornell University. He is a board trustee and advisor with a number of advocacy, education and charitable organizations, including Cornell University CIS, University Prep, and T4A.org.

DEFENSE BUSINESS BOARD

SAFROADU YEBOAH-AMANKWAH (Co-chair)
SENIOR VP & CHIEF STRATEGY OFFICER, INTEL

Safroadu "Saf" Yeboah-Amankwah is senior vice president and chief strategy officer (CSO) at Intel Corporation. Yeboah-Amankwah leads Intel's Global Strategy Office, including Intel Capital, and works with the executive team on developing and driving growth-oriented strategies.

Yeboah-Amankwah joins Intel from McKinsey & Company, where he was most recently a senior partner and global head of the Transformation Practice for the Telecom, Media and Technology (TMT) practice, based in Washington, D.C. He is also the global lead of Client Capabilities for the TMT practice. Previously he served as managing partner for South Africa and head of McKinsey's TMT and Digital practice for Africa, among other roles.

Yeboah-Amankwah received both his bachelor's and master's degrees in electrical engineering and computer science from the Massachusetts Institute of Technology. He is a former board member of the United Negro College Fund.

Education: MIT Electrical Engineering and Computer Science 1993, Master's Engineering 1994

Experience:

McKinsey & Company (26 yrs 3 mos)
Senior Partner Sep 2018 – Nov 2020; Washington, DC
Senior Partner Sep 1994 – Nov 2020

During his time in Africa, Saf was one of McKinsey's experts on doing business in Africa and he led the firms work in digital and telecommunications across Africa. While in that role, he supported the turnaround of a leading local telecom operator led a three-year transformation program at one of Africa's largest retail banks. He also supported a global private-equity firm in turning around an Africa multinational focused on the agricultural value chain.

His other efforts helped a high-tech multinational develop a growth strategy for its African operations that led to a 3X improvement in sales and he co-led a three-year transformation for one of the largest telecom OEMs, encompassing operations in North America, Europe and Asia.

DEFENSE BUSINESS BOARD

ANAND BAHL

CHIEF INFORMATION OFFICER, MICRON

Anand Bahl is Chief Information Officer, CVP at Micron Technology, Inc. where he oversees the global technology teams supporting manufacturing and engineering solutions, enterprise applications and analytics, global security, infrastructure and operations, and other business-facing IT services and capabilities. Anand is focused on driving an enterprise wide digital transformation at Micron to enable speed at scale.

He has more than 20 years of international and domestic experience in both IT and Finance in the chemical, textile, and technology industries. Immediately prior to joining Micron in July 2018, Anand led Vivint Smarthome' s Finance and Supply Chain IT organization. He has also held various IT and Finance leadership positions at Symantec, Advanced Micro Devices, Koch Industries, and Dow Chemical (Rohm & Haas).

Anand received a Master of Business Administration in Finance and Operations and a Master of Inorganic Chemistry from Vanderbilt University.
http

DEFENSE BUSINESS BOARD

GREG BOWMAN

VICE PRESIDENT OF CORPORATE DEVELOPMENT & CHIEF INNOVATION OFFICER SIEMENS GOVERNMENT TECHNOLOGIES TECHNOLOGY, INC.

Gregory L. Bowman is the Vice President of Corporate Development & Chief Innovation Officer of Siemens Government Technologies (SGT), Inc., the separate but affiliated U.S. government arm of technology powerhouse Siemens. With project teams across the U.S. and internationally, SGT is a cleared provider of Siemens products, technologies and software to solve some of the most complex government challenges in energy, automation and digitalization.

Prior to joining SGT, Mr. Bowman served in the U.S. Army for more than 25 years—culminating his career as the Strategic Military Law and Policy Advisor/Legislative Counsel to the Secretary of the Army. Chosen to establish that position, he served two Secretaries and two Acting Secretaries of the Army for over seven years. At SGT, Mr. Bowman has served as Director of Large Integrated Programs (OCONUS), then Deputy/Chief Operating Officer of Energy & Infrastructure and most recently as Vice President of Strategy, Growth and Partnerships. In his current role, he is focused on driving strategic growth by leveraging innovations from across the Siemens global portfolio to support U.S. government customers around the world.

A graduate of Longwood University, Mr. Bowman was commissioned in the Army in 1990 and graduated summa cum laude in Pre-Law and was the Distinguished Military Graduate. Following graduation, he was selected for the "Educational Delay" Program to attend the University of Virginia School of Law. He received his Juris Doctorate in 1993, and later received a Master of Military Law and Government Contracting (Honor Graduate) from the U.S. Army Judge Advocate General's Legal Center & School, and a Master of Military Arts and Sciences (Strategy) from the U.S. Army Command & General Staff College. He is a member of the Virginia State Bar and is admitted to practice law before both the Supreme Court of Virginia and the Supreme Court of the United States.

Mr. Bowman's military positions included Strategic Military Law and Policy Advisor and Legislative Counsel to the Secretary of the Army; Legislative Counsel, Office of the U.S. Army Chief of Legislative Liaison; Deputy Staff Judge Advocate, U.S. Army Armor Center and Fort Knox, Kentucky; Military Personnel Law Attorney, Administrative Law Division, Office of The Judge Advocate General; Senior Legal Advisor, Governorate Support

Team (1st Armored Division-Baghdad); Military Member Judicial Review Committee of Iraq; and served as the first Administrator/Amicus Central Criminal Court of Iraq.

DEFENSE BUSINESS BOARD

SALLY DONNELLY

FOUNDING PARTNER, PALLAS ADVISORS

Sally Donnelly is a Founding Partner of Pallas, a strategic advisory firm specializing in navigating complex national and international security dynamics. Her public service included roles as Senior Advisor to the Secretary of Defense, Director of the Washington Office for the Commander of U.S. Central Command, and Special Assistant to the Chairman of the Joint Chiefs of Staff.

In the private sector, Ms. Donnelly was the Founder and Chief Executive Officer of SBD Advisors, a Washington, D.C.-based consulting firm advising technology and corporate clients as well as non-governmental organizations on strategic positioning, communications and policy issues.

Previously she spent more than 20 years at Time Magazine serving as the magazine' s correspondent for the Iraq War, the Moscow bureau, and on the aviation and airline beat. She was the head researcher of the 1988 book Mikhail S. Gorbachev: An Intimate Biography and worked on the 1989 book Massacre in Beijing.

Ms. Donnelly serves on the Board of the Quincy Institute for Responsible Statecraft. Additionally, she is a non-resident senior fellow at the Rockefeller Brothers Fund and on the Leadership Council for the Bob Woodruff Foundation. Ms. Donnelly holds a Bachelor of Arts in History from Hollins College and a Master' s degree in Russian politics from London School of Economics.

DEFENSE BUSINESS BOARD

MARACHEL KNIGHT

SENIOR VICE PRESIDENT, STRATEGIC PROGRAM REALIZATION, AT&T COMMUNICATIONS, INC

As Senior Vice President of Strategic Program Realization, Marachel's responsibilities include delivering strategic initiatives, products and services that span across the enterprise and managing prioritization of AT&T's multi-billion-dollar portfolio to optimize customer experience and maximize value.

Marachel has served in a variety of technology leadership positions at AT&T. Her areas of expertise include technology architecture and development, technology engineering, network construction, technology operations, technology realization and program management, P&L, business operations, capital and expense budget management, and project management. Marachel led the architecting, development and building of the first U.S. standards-based 5G wireless network, launched AirGig technology trials, advanced the transformative software-defined networking initiative, and led business development and project management for AT&T's customized venue antenna solutions. Marachel has two patented inventions: Systems for Use with Multi-Number Cellular Devices and Messaging Forwarding System.

Marachel serves on the board of directors for Marvell Technology, Inc., a publicly traded leader in data infrastructure semiconductor technology. She also serves on the board of directors for the National Action Council for Minorities in Engineering and is a member of the Federal Reserve Bank of Dallas Business and Community Advisory Council. Marachel co-established and is a national advisor for Advocates for Women in Technology, an AT&T employee resource network. She is a former chair of Carnegie Mellon University' s Information Networking Institute Alumni Leadership Council and formerly served on the advisory board of After School Matters.

Marachel earned a master' s degree in information networking from Carnegie Mellon University and a bachelor' s degree in electrical engineering from Florida State University.

BRIG. GEN. BERNARD SKOCH (USAF, RET.), EXECUTIVE LEAD, AFA STRATEGIC EVENTS AIR FORCE ASSOCIATION

Brigadier General Bernie Skoch (USAF, Ret.) graduated from the University of Arkansas with a bachelor's degree in industrial engineering. Upon graduation he was commissioned as a second lieutenant in the Air Force. His 29-year Air Force career took him throughout the United States, Europe, Asia, the Pacific, and the Middle East on permanent and temporary duty until retiring at the rank of brigadier general.

Skoch has more than 25 years of experience in leadership positions developing, managing and implementing communications and information systems at the wing, major command, and Air Staff levels of the United States Air Force as well as at the Defense Information Systems Agency (DISA). During his time at DISA he served as the Principal Director for Customer Advocacy and as the Principal Director for Network Services. At Headquarters USAF, he served as Director of Mission Systems, Director of Communications Operations, and Director of Chief Information Officer Support where he was responsible for aligning information technology systems with business process improvements. He has developed policies for global voice, video, radio, data, and satellite systems.

While on the Joint Staff, Skoch led transformation of the mainframe-based DoD-wide Worldwide Military Command and Control System to the distributed Global Command and Control System, substantially improving system support to Combatant Commands.

As Director of Communications at Pacific Air Forces, he led the creation of the COPE SPARK family of initiatives which significantly improved warfighter communications and data support throughout the Pacific.

Upon retirement from active duty, Skoch was a consultant to numerous IT-sector companies and to the federal government. In 2010, following an unsuccessful run for the U.S. House of Representatives, Skoch was appointed National Commissioner of the National Youth Cyber Education Program, CyberPatriot, a program operated by the not-for-profit Air and Space Forces Association. Skoch oversaw the planning and implementation of CyberPatriot and provided leadership and support for the program's development. Under his leadership the program grew into the largest cyber defense STEM education competition in the world, reaching

over 250,000 K-12 students, stimulating their interest in science, technology, engineering and mathematics related studies, as well as increasing their awareness of cybersecurity threats.

Skoch is a graduate of Air Command and Staff College, Air War College, and the Program for Senior Officials in National Security at Syracuse University and Johns Hopkins University. He holds a master's degree in management and supervision from Central Michigan University.

Bernie is a certificated Commercial Pilot and FAA certificated drone pilot, and is an amateur astronomer and a ham radio operator. Bernie and Debbie, his wife of 50 years, have six children, twenty-one grandchildren, and one great grandchild, all residing in Northwest Arkansas.

DEFENSE BUSINESS BOARD

STAN SOLOWAY

PRESIDENT & CEO, CELERO STRATEGIES, LLC

Stan Soloway is President & CEO of Celero Strategies, LLC, a full-service strategic consultancy focused on the federal market. Celero Strategies is Soloway's latest step in a career during which he has become widely regarded as one of the nation's leading experts on the federal market, the factors and dynamics that drive it and how to translate that expertise into meaningful strategies and action. With Celero, Soloway's goal is to combine two core passions: helping good companies bring innovative solutions to government and helping government significantly improve its performance and delivery of service. Stan also serves as a member of the Defense Business Board, and is a Fellow of both the National Academy of Pubic Administration (where he also serves on the Board of Directors) and of the National Contract Management Association.

Prior to founding Celero Strategies in January 2016, Stan served for 15 years as the President & CEO of the Professional Services Council, the largest and most influential national association of government technology and professional services firms. While at PSC, Soloway was the industry's leading voice, policy strategist and resource for both government and the private sector. He regularly testified before Congress, was a prolific writer, appeared often on radio and television; and was routinely sought out by both corporate and government organizations to discuss current market trends, dynamics and strategies. He has also been a contributing author for books published by Cambridge University, Harvard Law School and the University of Pennsylvania, and in 2021 co-authored "Other Transactions at 60: Hitting Their Stride or Hitting the Wall?" which was published by the IBM Center for the Business of Government.

Stan was the recipient of the 2016 Consumer Electronics Show (CES) Government Technology Leadership Award and was named the IT Industry Executive of the Year in 2013 by Government Computer News, He has also been cited as one of the 100 most influential business leaders in Washington (Washington Business Journal) and one of the 100 most influential figures in national defense (Defense News and Gannett). He is a four-time winner of the Federal 100 Award for his leadership in federal information technology and is a principal at the Partnership for Public Service where he serves as a Senior Advisor to Government Executives (SAGE).

During the second half of the Clinton Administration, Stan served as the Deputy Undersecretary of Defense and was responsible for wide-ranging reforms to defense acquisition and technology policy and practices, and broader department-wide re-engineering. In recognition of his leadership in the department, Stan was awarded both the Secretary of Defense Medal for Exceptional Public Service and the Secretary of Defense Medal for Distinguished Public Service.

As passionate believer in the importance and value of public service, Stan also served from 2007 to 2013 as a Senate-confirmed member of the Board of Directors of the Corporation for National and Community Service (now known simply as AmeriCorps). Earlier in his career he was a public policy and public affairs consultant for nearly 20 years. He also co-produced the acclaimed PBS television series "Great Confrontations at the Oxford Union." He is a graduate of Denison University, where he was elected to the National Men's Leadership, National Journalism, and National Political Science honorary societies.

DEFENSE BUSINESS BOARD

GENERAL JOSEPH L. VOTEL, USA (RET)

PRESIDENT & CEO FOR BUSINESS EXECUTIVES FOR NATIONAL SECURITY

General Joseph L. Votel is a retired U.S. Army Four-Star officer and most recently the Commander of the U.S. Central Command – responsible for U.S. and coalition military operations in the Middle East, Levant and Central and South Asia. During his 39 years in the military, he commanded special operations and conventional military forces at every level. His career included combat in Panama, Afghanistan and Iraq. Notably, he led a 79-member coalition that successfully liberated Iraq and Syria from the Islamic State Caliphate. He preceded his assignment at CENTCOM with service as the Commander of U.S. Special Operations Command and the Joint Special Operations Command.

Votel was recognized with the Distinguished Military Leadership Award from the Atlantic Council, the U.S. – Arab Defense Leadership Award from the National Council on U.S. - Arab Relations, the Patriot Award from the Congressional Medal of Honor Society, the SGT James T. Regan Lifetime Achievement Award from the "Lead the Way" Foundation and the Freedom Award from the Intrepid Sea, Air and Space Museum.

In January of 2020, General Votel became President & CEO of Business Executives for National Security (BENS). He is a Strategic Advisor for Sierra Nevada Corporation as well as a member of the Board of Trustees for Noblis Corporation. Votel is a non-resident Distinguished Fellow at the Middle East Institute and the Belfer Center at the John F. Kennedy School of Government and advises the Combating Terrorism Center at West Point. He sits on the Executive Board of Freedom House and the Center for Ethics and the Rule of Law (CERL). He serves on the Board of Directors for Service to School, Minnesota Wire, Digital Force Technologies and Owl Cyber Defense. He is a member of the Council on Foreign Relations.

Votel is a 1980 graduate of the United States Military Academy and earned master's degrees from the U.S. Army Command and Staff College and the Army War College. He is married to Michele; and they have two grown sons, a daughter-in-law and two grandchildren. The Votels reside in Lake Elmo, Minnesota.

This page left intentionally blank

Appendix D: Contributors List

The Defense Business Board would like to thank the following individuals and organizations for their time in contributing knowledge and information supporting this study. Their help is greatly appreciated.

Mr. Sajeel Ahmed, Director of JSP
Mr. Wes Anderson, Vice President Defense, Microsoft
Mr. Christopher Barnhurst, Deputy Director, DISA
Mr. Nicholas Chailan, Chief Technology Officer, Prevent Breach
Mr. Paul Crumbliss, DISA Deputy Chief Compute Operations
Hon. Dana Deasey, DoD CIO (previous)
Mr. Motti Finkelstein, Intel CIO
Mr. Guy Fruda, Chief Technology Support Leader, Deloitte
Mr. Roger Greenwell, DISA Enterprise Integration & Innovation Center, CIO, Director
Mr. Brian Herman, DISA Cyber Security & Analytics Directorate
Mr. Raj Iyer, Army CIO
Ms. Lauren Knausenberger, Air Force CIO
LTG Susan Lawrence (Ret), CEO AFCEA
Mr. Anthony Leraris, Managing Director Accenture
Ms. Tinisha Mcmillan, DISA, Endpoint & Customer Service Director, 4th Estate
Ms. Danielle Metz, OSD CIO (ODA&M)
Mr. Bobby Mills, Customer Service Chief, DISA JSP
Mr. Frederick Moorefield, DoD DCIO C3
Mr. Chad Montgomery, Duty CIO and Chief Operations Officer ITS, Deloitte
Mr. Mark Murphy, Ops Research Analyst OSD CAPE
Mr. Joseph Nogueira, Principal Deputy Director CAPE
Mr. Chris Paczkowski, DISA Transport Services Executive Senior Technologist
Mr. David Shaddrix, JSP CoS/Customer Service Director
Mr. Raju Shah, Director of Enterprise Engineering and Governance Directorate
Mr. John Sherman, DoD CIO
Ms. Julia Shmirkin, Survey Methodologist, WHS Facilities Services Directorate
Mr. Jon Summer, CIO AT&T
Mr. Rodney Turner, Customer Engagement Division Chief, DISA JSP
Mr. Steve Wallace, DISA Director of Emerging Technology
Mr. Joseph Wassel, DISA Cyberspace Operations Director
Mr. Aaron Weis, DoN CIO
Mr. David Wennergren, CEO ACT-IAC
Mr. Colt Whittall, Air Force Chief IT User Experience Officer

Appendix E: Bibliography

Amaresan, Swetha. Hubspot.com. “Help Desk Management: 13 Key Steps to Follow for Success.” June 24, 2022. https://blog.hubspot.com/service/help-desk-management.

Barnett, Jackson. Fedscoop.com. “IT Consolidation for Military’s Fourth Estate Agencies is Coming Next Year, officials say.” Page 19. December 1, 2020. www.fedscoop.com/dod-fourth-estate-modernization-initiative-disa.

Batchelder, Grossman, Martin, Newcomb, Rockart & Yetter. *Harvard Business Review*. “The End of the Delegation? IT and the CEO.” September-October 1995. Retrieved hbr.org on October 27, 2022. https://hbr.org/1995/09/the-end-of-delegation-information-technology-and-the-ceo.

Boyd, Aaron. Nextgov.com. “Air Force CXO: We Don’t Have to Delight the User.” Retrieved January 4, 2023. https://www.nextgov.com/emerging-tech/2019/10/air-force-cxo-we-dont-have-delight-user/160373.

CentreofExcellence.com. “Customer Maturity Model.” Page 13. Retrieved December 22, 2022. https://www.centreofexcellence.com.

Chief Information Officers Council. Policies, Priorities & Resources. “CIO. Handbook.” Retrieved January 7, 2023. https://www.cio.gov/cio-handbook.

Colvin, Geoff. Fortune.com. “The Simple Metric That’s Taking Over Big Business.” Page 11. June/July 2020. https://fortune.com/longform/net-promoter-score-fortune-500-customer-satisfaction-metric.

Curry, Koch, Milic, Yan, and Zhang. Information Systems Management. “How Consumer Technology is Changing the IT Function: A Multi-Case Study of Three Fortune 500 Companies.” 2019. Vol 36, No. 4, Page 336-349. Retrieved January 18, 2023. https://doi.org/10.1080/10580530.2019.1652443.

Das, Tamaghna. SectHub.com. “Endpoint Monitoring: A Comprehensive Guide.” Retrieved December 6, 2022. www.selecthub.com/endpoint-security/endpoint-monitoring.

Defense Business Board. “Recommendations for the Next Generation of Business Health Metrics.” November 10, 2022. https://dbb.defense.gov.

Defense Information Systems Agency. Careers. Retrieved November 4, 2022. https://www.disa.mil/careers.

Defense Information Systems Agency. Global Service Desk. “GSD Help Desk for JSP and DoDNET/4th Estate Optimization (4ENO).” Retrieved December 18, 2022.

Department of Defense Information Resource Management Strategic Plan FY19-23. “DOD Digital Modernization Strategy 2019.” Page 7. July 12, 2019. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

Department of Veterans Affairs. “VA on Track to Improve Veteran Customer Experience.” June 25, 2019. www.va.gov/VE/pressreleases/2019062501.asp.

Director of Administration & Management. “Department of Defense Strategic Management Plan.” August 8, 2022. https://dam.defense.gov.

Douglas, Robert. Planet Magpie. “How Often Should You Replace Your Company PCs?” August 7, 2018. www.planetmagpie.com/news/woof-newsletter/2018/08/07/how-often-should-you-replace-your-company-pcs.

Freedberg, Sydney. Breaking Defense. “Exclusive: Pentagon Not Prepared for Software Updates at the Speed of Ware, Report Finds.” December 14, 2022. https://breakingdefense.com/2022/12/exclusive-pentagon-not-prepared-for-software-updates-at-the-speed-of-war-report-finds.

Gill, Jaspreet. Breaking Defense. “Army Launches New Bring-Your-Own-Device Pilot as It Aims to Leverage Commercial Capabilities. August 22, 2022. https://breakingdefense.com/2022/08/army-launches-new-bring-your-own-device-pilot-as-it-aims-to-leverage-commercial-capabilities.

Gill, Jaspreet. Breaking Defense. “OSD Gets New IT Directorate, Own CIO After Study Found ‘Degradation’ of Services.” October 14, 2022. https://breakingdefense.com/2022/10/osd-gets-new-it-directorate-own-cio-after-study-found-degradation-of-services.

Gold, A. J. & Associates. Research. “Value of Replacing Company Computers Every Three Years.” Retrieved November 21, 2022. https://jgoldassociates.com/research.

Haxxess Enterprise Corporation. “How Often Should We Replace Our Business Computers?” Retrieved January 16, 2023. www.haxxess.com/how-often-replace-business-computers.

Help Net Security. News. “The True Costs Incurred by Businesses for Technology Downtime.” April 24, 2020. https://www.helpnetsecurity.com/2020/04/24/technology-downtime.

Hicks, Kathleen H. U.S Department of Defense. “Next Generation of Business Health Metrics Terms of Reference.” [Memorandum]. November 10, 2022. https://dbb.defense.gov.

Higgins, Ryan. Chief Information Officers Council. “The Importance of Multifactor Authentication. October 26, 2022. The Importance of Multifactor Authentication | CIO.GOV.

InsightCDCT.com. “The State of IT Modernization 2020.” Retrieved November 21, 2022. https://solutions.insight.com/getattachment/a67b34bd-1a9a-42fe-a408-7afe180b96d8/Complete-IDG-survey-results.aspx).

Joint Interoperability Testing Command (JITC). About. Retrieved January 18, 2023. https://jitc.fhu.disa.mil.

Kannan, Michael. Linkedin.com. “Michael Kannan’s Post.” February 2022. https://www.linkedin.com/posts/michaeljkanaan_technology-future-innovation-activity-6891726752759074816-2qCv.

Legislative Board of Texas. “Review of Replacement Schedule for Information Technology Equipment.” Retrieved December 27, 2022. www.lbb.texas.gov/Documents/Publications/Issue_Briefs/257_IT%20Replacement%20Schedule.pdf.

Liu, Nancy. SDx Central. “DoD Discloses Zero-Trust Strategy, Roadmap. “November 23, 2022. https://www.sdxcentral.com/articles/news/dod-discloses-zero-trust-strategy-roadmap/2022/11/#.

Microsoft NZ News Centre. “True Cost of Not Replacing Computers.” Retrieved November 22, 2022. news.microsoft.com/en-nz/2018/10/16/true-cost-of-not-replacing-computers-revealed-in-microsoft-study-more-than-4000-each.

Miller, Jason. Federal News Network. “DHS on Cusp of Hiring as Many as 100 CX Experts.” December 13, 2022. www.federalnewsnetwork.com/hiring-retention/2022/12/dhs-on-cusp-of-hiring-as-many-as-100-cx-experts.

Mitchell, Billy. Fedscoop.com. “Mac Thornberry Wants to Eliminate DISA.” April 18, 2018. https://www.fedscoop.com/eliminate-disa-legislation-mac-thornberry.

Office of Personnel Management. Policy, Data, Oversight. Retrieved January 8, 2023. https://www.defense.gov/News/Releases/Release/Article/2430245/dod-guidance-on-extension-of-maximum-telework-flexibilities.

Office of Personnel Management. Policy, Data, Oversight. “Fact Sheet: Computing Hourly Rates of Pay Using the 2,087-Hour Divisor.” Retrieved January 8, 2023. https://www.opm.gov/policy-data-oversight/pay-leave/pay-administration/fact-sheets/computing-hourly-rates-of-pay-using-the-2087-hour-divisor.

Omale, Gloria. Garner, Inc. “Gartner Says Nearly 90% of Organizations Now Have a Chief Experience Officer or Chief Customer Officer or Equivalents.” February 20, 2020. www.gartner.com/en/newsroom/press-releases/2020-02-10-gartner-says-nearly-90--of-organizations-now-have-a-c.

Payscale.com. “Average Salary for U.S. Department of Defense Employees.” Retrieved January 19, 2023. https://www.payscale.com/research/US/Employer=U.S._Department_of_Defense/Salary.

Reddit.com. “Fix our computers!” March 2022. https://www.reddit.com/r/Military/comments/sdlvk7/fix_our_computers.

Sanders, Andrew. AppNeta. “4 Critical KPIS for Internal Help Desks to Improve End-User Experience.” November 13, 2017. www.appneta.com/blog/4-critical-kpis-internal-help-desks-improve-end-user-experience.

Serbu, Jared. Federalnewsnetwork.com. “DoD Establishes New CIO to Unify IT Efforts in Office of the Secretary of Defense.” October 14, 2022. https://federalnewsnetwork.com/defense-news/2022/10/dod-establishes-new-cio-to-unify-it-efforts-in-office-of-the-secretary-of-defense.

Smith, Karl. Defense Information Systems Agency. “DISA Launches Cybersecurity Awareness Campaign.” March 3, 2022. https://www.disa.mil/en/NewsandEvents/2022/DISA-Cybersecurity-Awareness-Campaign.

The Office of Cost Assessment & Program Evaluation. “FY2020 DoD Budget Request (Base and OCO Funding).” Retrieved January 7, 2023. https://cape.osd.mil.

The White House. “Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government.” December 13, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government.

The World Bank. “GDP (current US$) Data.” Retrieved December 3, 2022. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

Trust Radius. “Help Desk Statistics and Trends for 2022.” April 21, 2022. www.trustradius.com/buyer-blog/help-desk-statistics.

U.S. Department of Defense. About. Retrieved November 7, 2022. https://www.defense.gov/About.

U.S. Department of Defense. “DOD Guidance on Extension of Maximum Telework Flexibilities.” Retrieved November 30, 2020. https://www.defense.gov/News/Release/Release/ Article/2430245/dod-guidance-on-extension-of-maximum-telework-flexibilities.

U.S. Department of Defense. “Federal Data Center Consolidation Initiative.” November 8, 2011. https://dodcio.defense.gov/Portals/0/Documents/FDCCI-Final-2011.pdf.

U.S. Department of Defense. Mission Statement. Retrieved November 5, 2022. https://www.defense.gov/About/#.

U.S. Department of Defense. Press Release. November 30, 2020. “DOD Guidance on Extension of Maximum Telework Flexibilities.” https://www.defense.gov/News/Releases/Release/Article/2430245/dod-guidance-on-extension-of-maximum-telework-flexibilities.

U.S Department of Defense. “2022 National Defense Strategy of the United States of America.” October 27, 2022. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

U.S. General Services Administration. “GSA FY 2022-2026 Strategic Plan.” Retrieved December 12, 2022. www.gsa.gov/reference/reports/budget-performance/gsa-fy-20222026-strategic-plan.

U.S. General Services Administration. “GSA Survey Satisfaction Results.” March 2022. www.gsa.gov/reference/reports.

U.S. House of Representatives. (n.d.). 10 USC 142: Chief Information Officer. Office of the Law Revision Counsel United States Code. Retrieved January 11, 2023. https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title10-section142&num=0&edition=prelim#sourcecredit.

U.S. House of Representatives. (n.d.). 44 USC 3506: Federal Agency Responsibilities. Office of the Law Revision Counsel United States Code. Retrieved January 11, 2023, https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title10-section142&num=0&edition=prelim#sourcecredit.

Vbsitservices.com. “How Often Should Your Company Replace Computers?” Retrieved December 5, 2022. www.vbsitservices.com/2016/02/how-often-should-your-company-replace-computers.

Washington Headquarters Services. “JSP, Interactive Customer Evaluation IT Satisfaction Survey.” November 17, 2022.

Appendix F: Questionnaire and Survey Forms

This page left intentionally blank

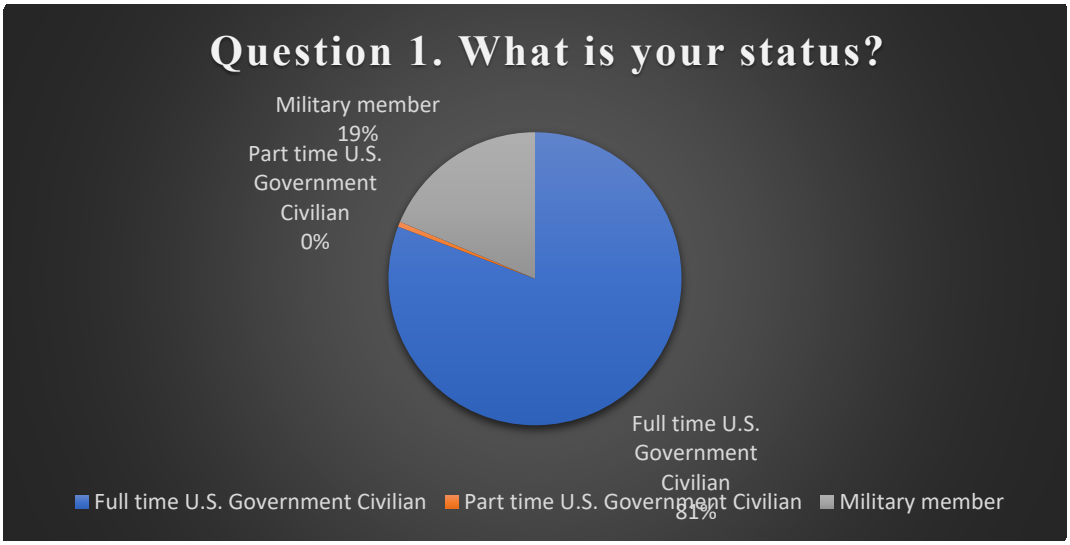
Background:

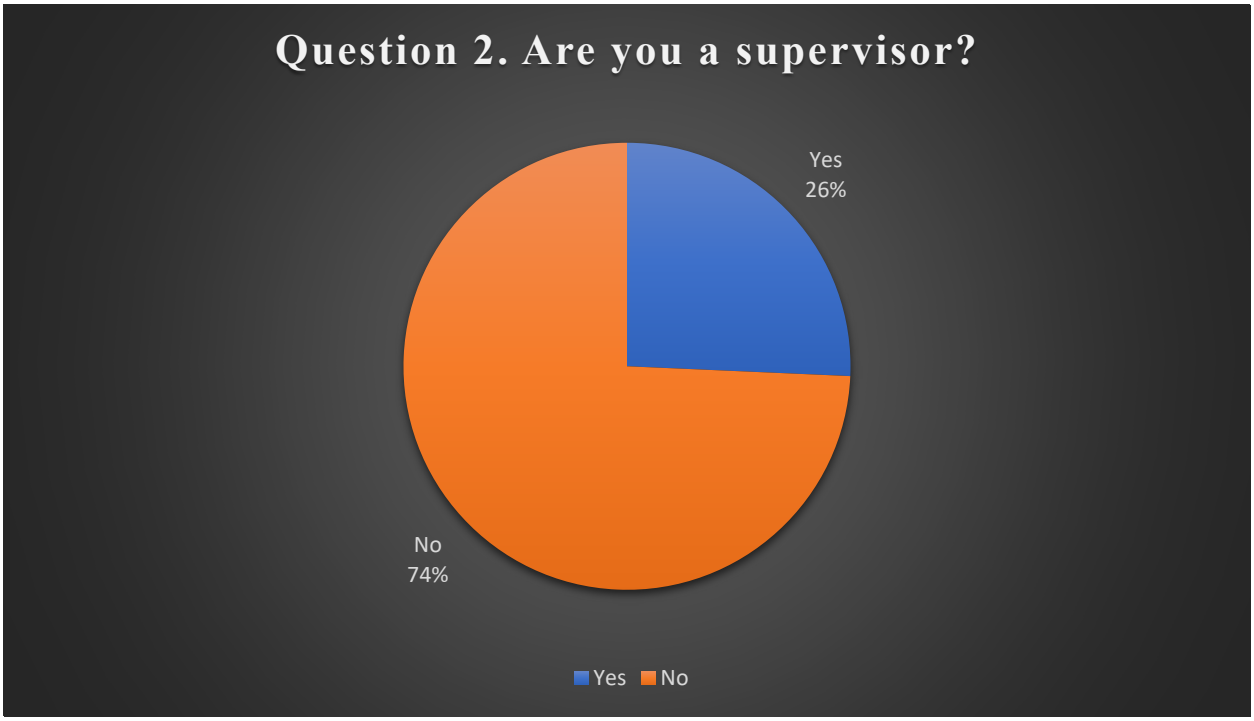
The Deputy Secretary of Defense assigned the Defense Business Board a study to provide "Recommendations to Improve the IT User Experience." An organization's IT is one of its most critical components. The DoD understands its IT infrastructure and systems are essential to maintaining its warfighting superiority, and the DoD has invested substantial resources and effort into building this critical capability. However, despite ongoing efforts, DoD IT has not historically provided a consistently high-quality user experience. To maintain our information superiority and provide the tools our workforce needs to innovate, DoD personnel must have access to reliable, secure, responsive, and rapid IT. This survey will provide valuable insights to improve Joint Service Provider customers' IT user experience without negatively impacting security or resiliency.

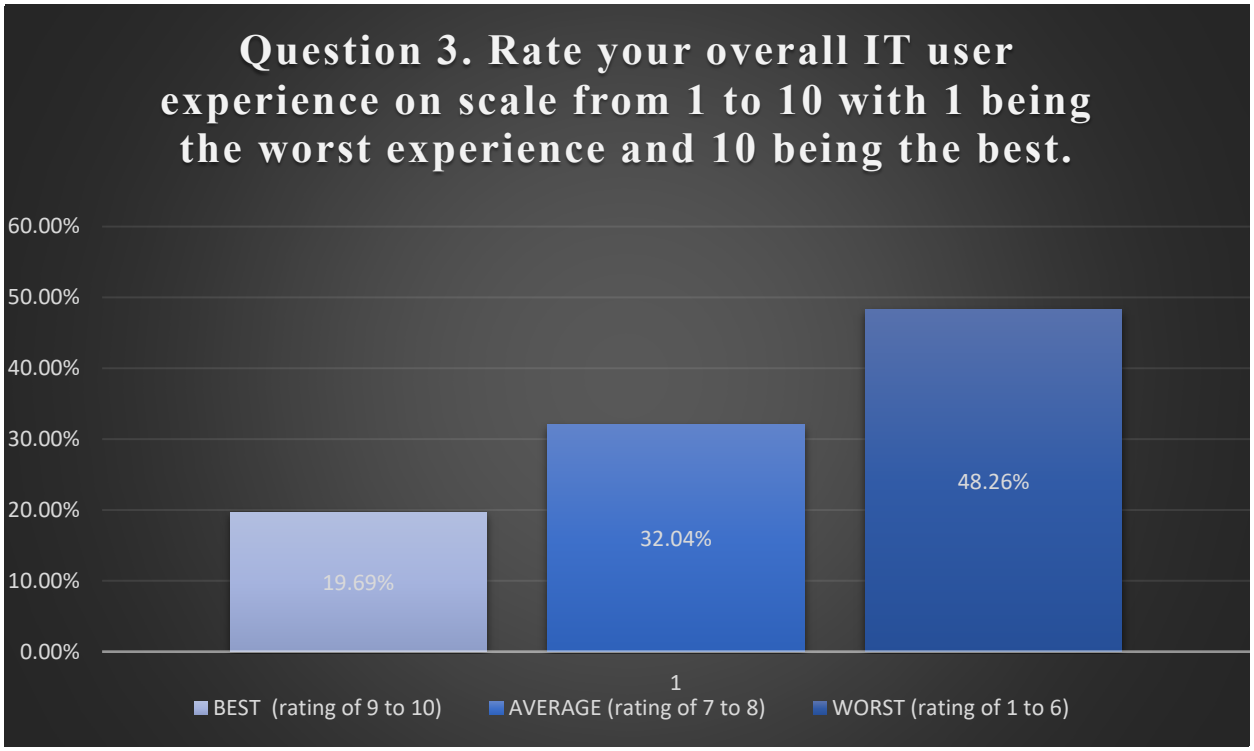
The Subcommittee surveyed approximately 22,000 Federal Employees who use IT services within the National Capital Region under the responsibility of the JSP. The survey ran for approximately two weeks with more than 3,500 respondents.

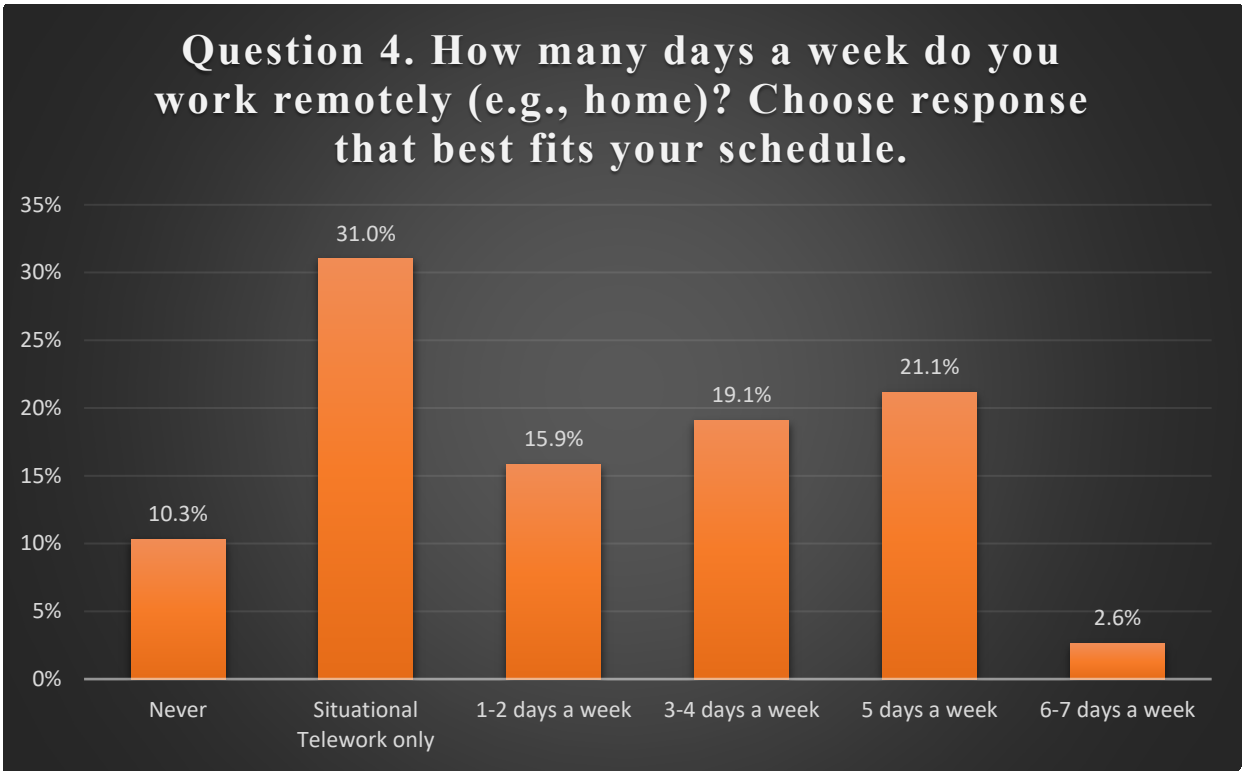
Note: The Subcommittee did not include a full breakdown of long-form answers in this report for brevity. If required, the DBB IT Study team can provide them.

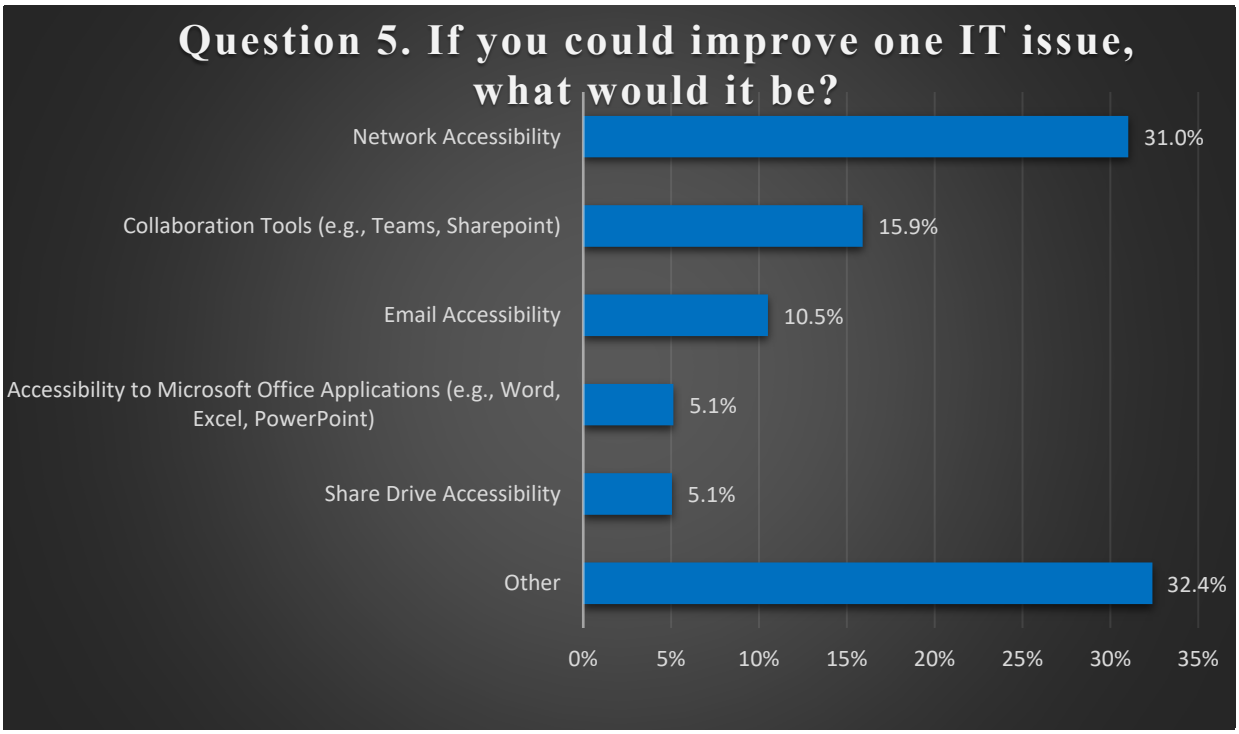
Survey:

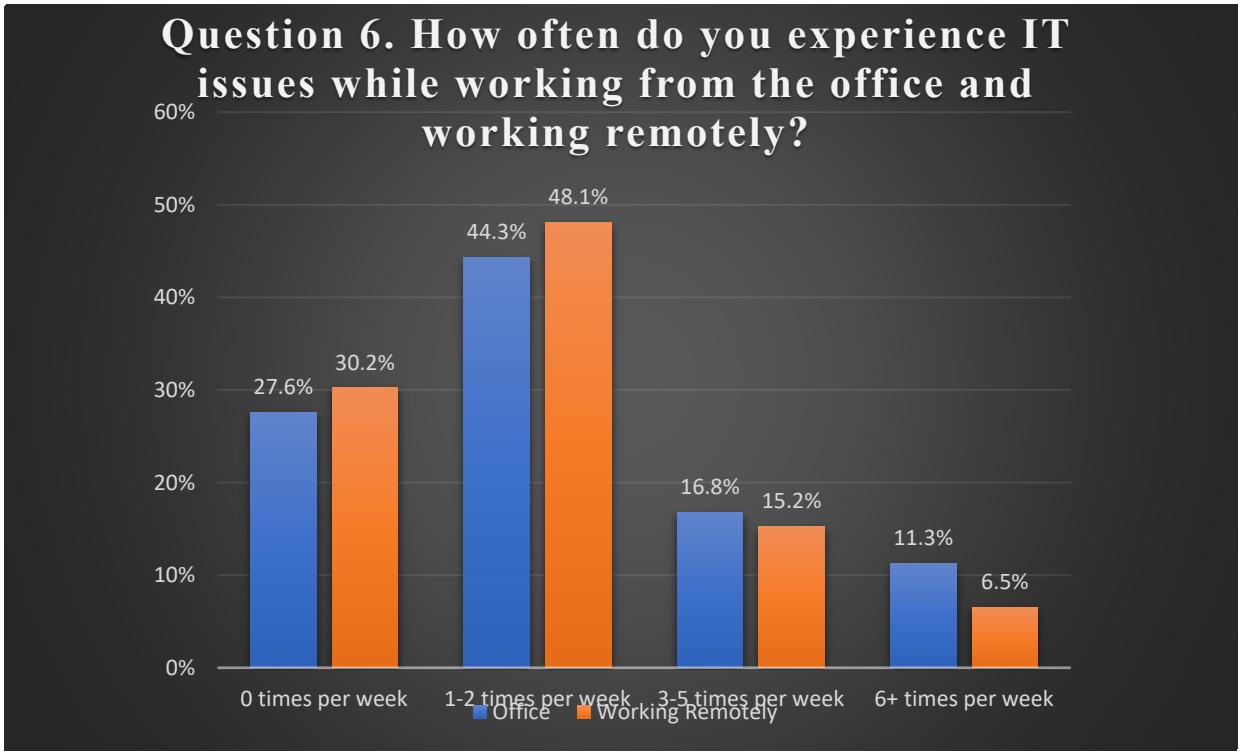


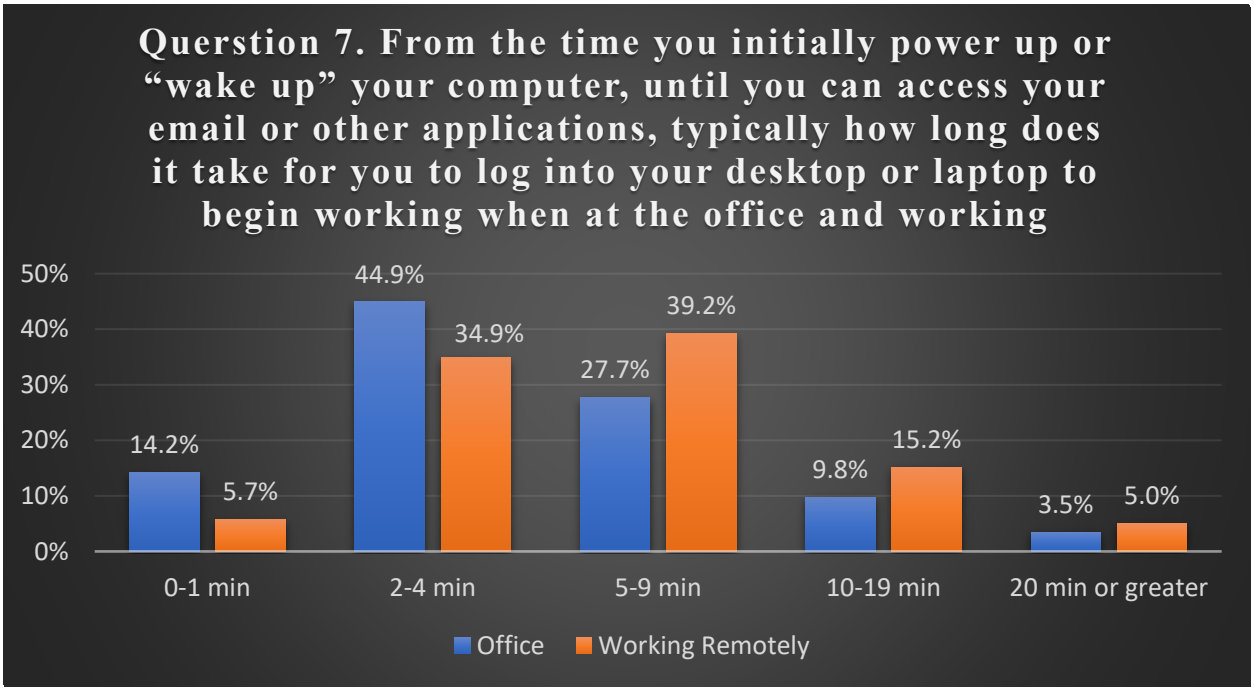

Question 2. Are you a supervisor?
Yes
26%
No
74%
Yes
No

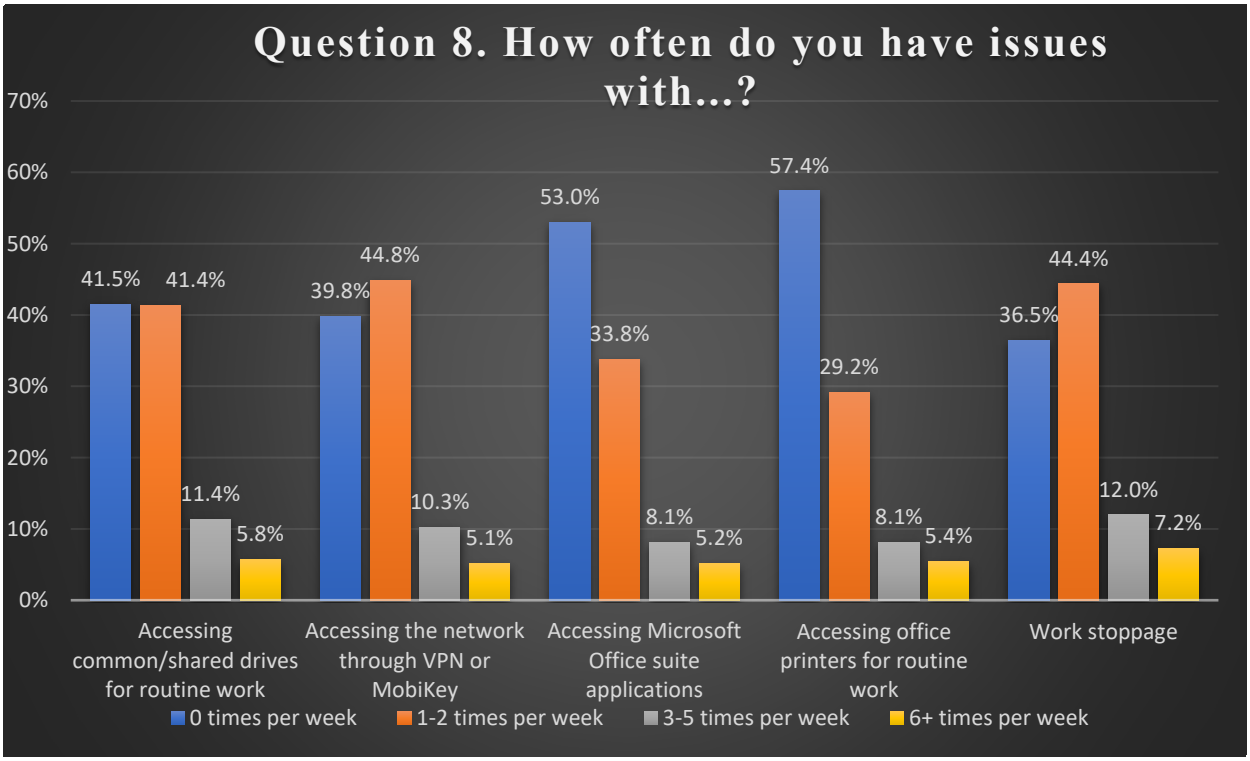

Question 3. Rate your overall IT user experience on scale from 1 to 10 with 1 being the worst experience and 10 being the best.
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
19.69%
32.04%
48.26%
1
BEST (rating of 9 to 10)
AVERAGE (rating of 7 to 8)
WORST (rating of 1 to 6)

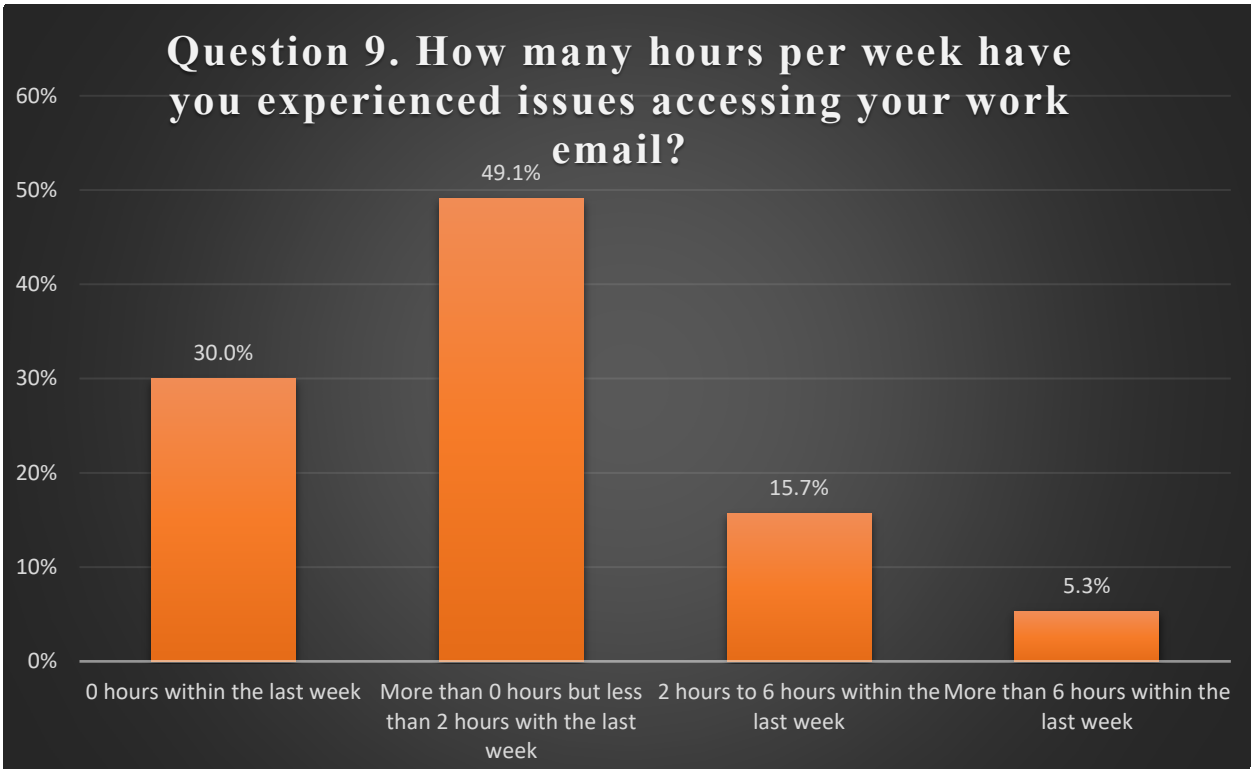

Question 4. How many days a week do you work remotely (e.g., home)? Choose response that best fits your schedule.
35%
30%
25%
20%
15%
10%
5%
0%
10.3%
31.0%
15.9%
19.1%
21.1%
2.6%
Never
Situational Telework only
1-2 days a week
3-4 days a week
5 days a week
6-7 days a week

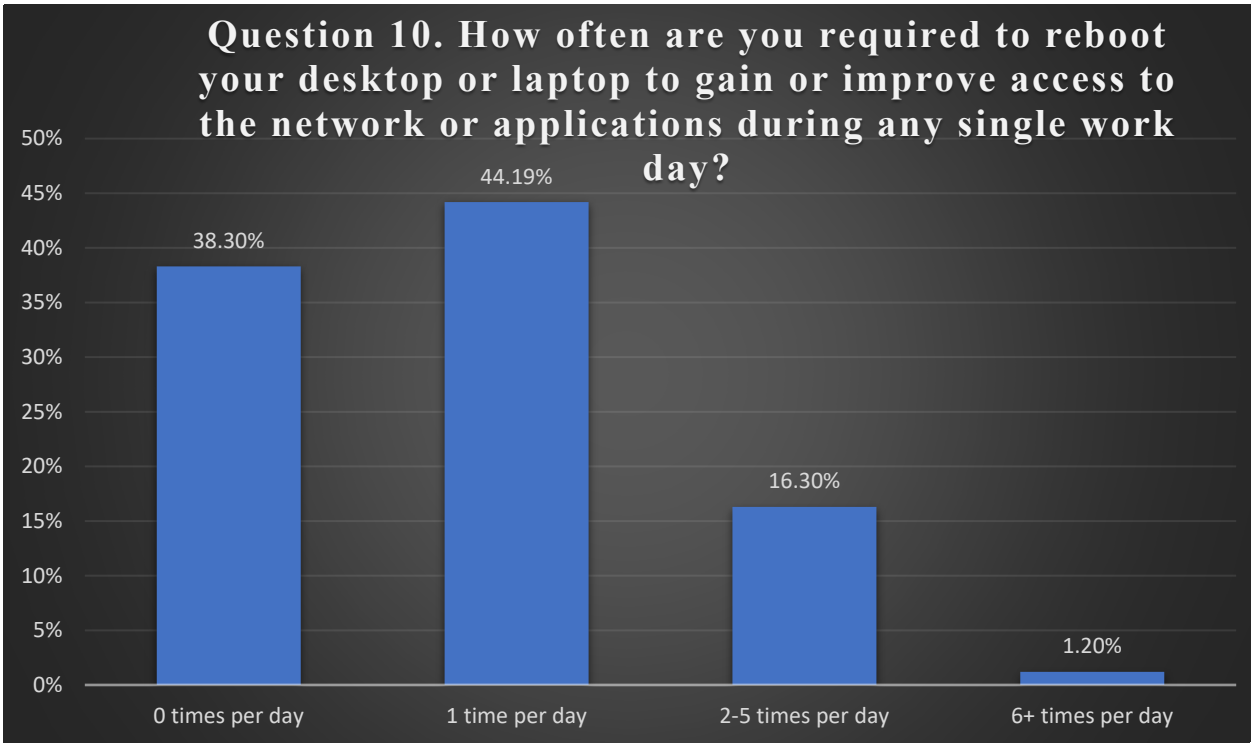

Question 5. If you could improve one IT issue, what would it be?
Network Accessibility
31.0%
Collaboration Tools (e.g., Teams, Sharepoint)
15.9%
Email Accessibility
10.5%
Accessibility to Microsoft Office Applications (e.g., Word, Excel, PowerPoint)
5.1%
Share Drive Accessibility
5.1%
Other
32.4%
0%
5%
10%
15%
20%
25%
30%
35%

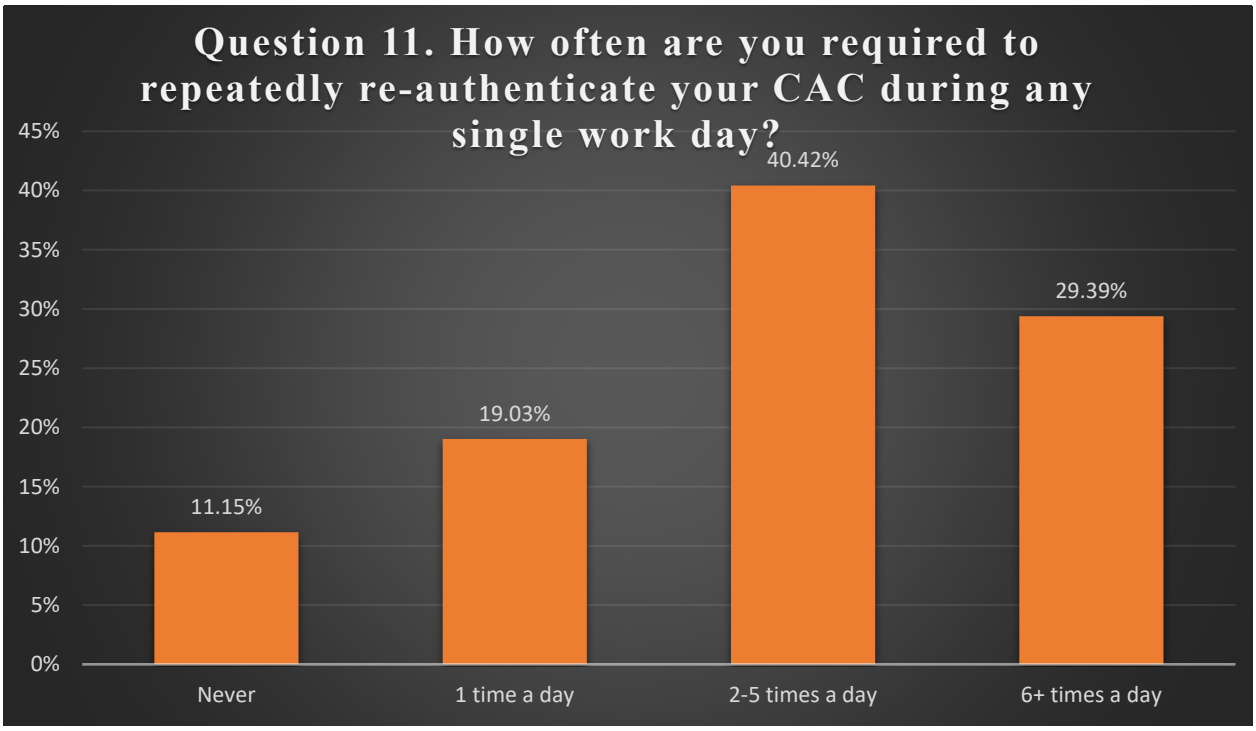

Question 6. How often do you experience IT issues while working from the office and working remotely?
60%
50%
40%
30%
20%
10%
0%
27.6%
30.2%
44.3%
48.1%
16.8%
15.2%
11.3%
6.5%
0 times per week
1-2 times per week
3-5 times per week
6+ times per week
Office
Working Remotely

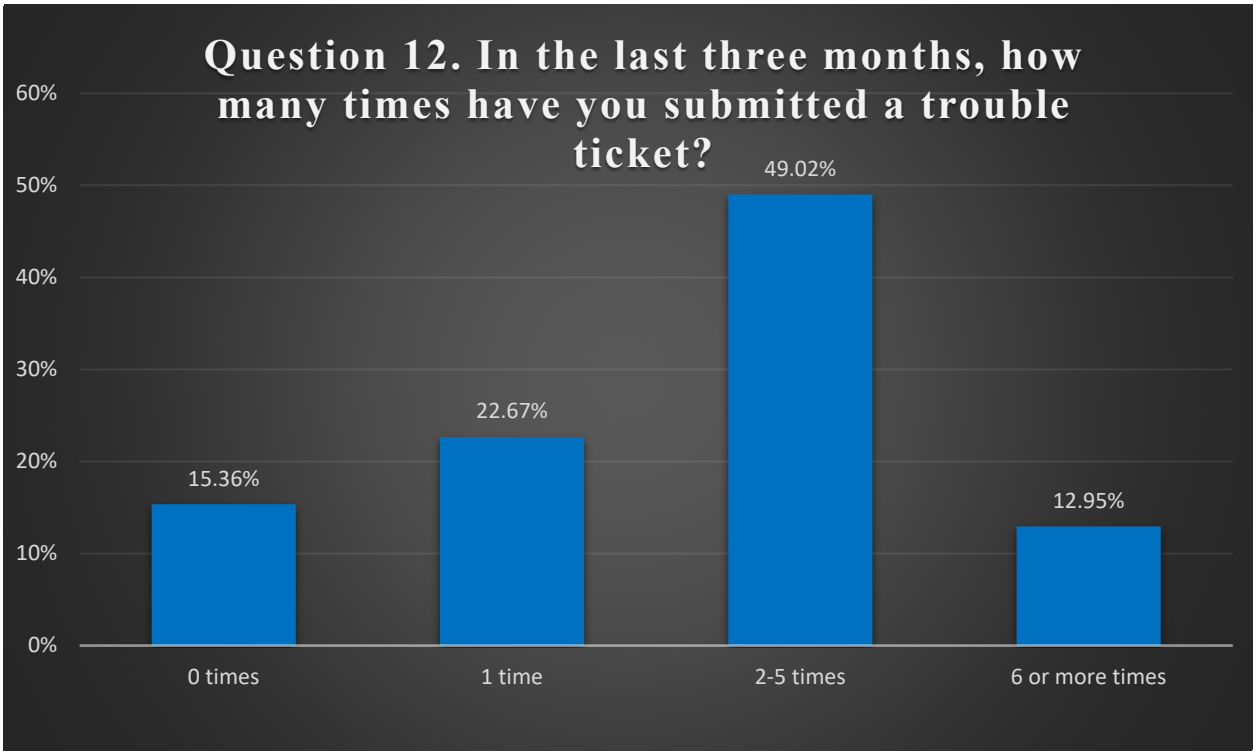

Querstion 7. From the time you initially power up or "wake up" your computer, until you can access your email or other applications, typically how long does it take for you to log into your desktop or laptop to begin working when at the office and working
50%
40%
30%
20%
10%
0%
14.2%
5.7%
44.9%
34.9%
27.7%
39.2%
9.8%
15.2%
3.5%
5.0%
0-1 min
2-4 min
5-9 min
10-19 min
20 min or greater
Office
Working Remotely

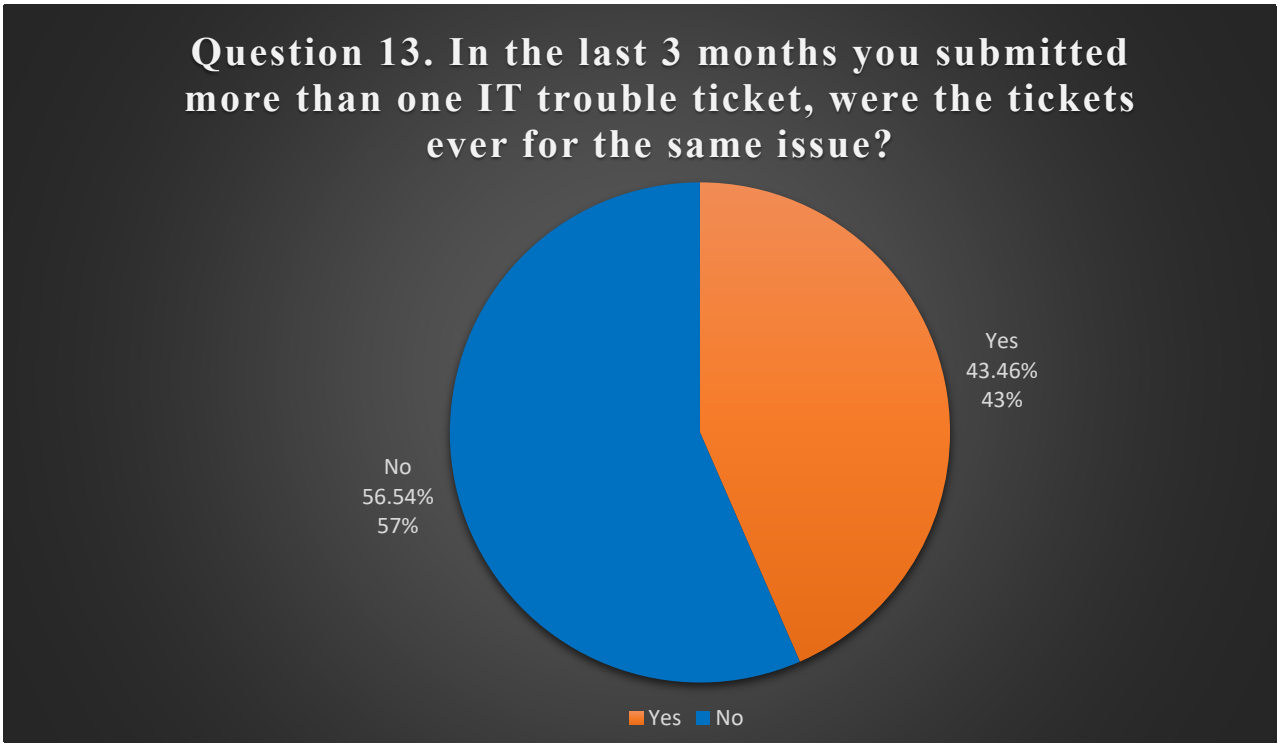

Question 8. How often do you have issues with...?
70%
60%
50%
40%
30%
20%
10%
0%
41.5%
41.4%
11.4%
5.8%
39.8%
44.8%
10.3%
5.1%
53.0%
33.8%
8.1%
5.2%
57.4%
29.2%
8.1%
5.4%
36.5%
44.4%
12.0%
7.2%
Accessing common/shared drives for routine work
Accessing the network through VPN or MobiKey
Accessing Microsoft Office suite applications
Accessing office printers for routine work
Work stoppage
0 times per week
1-2 times per week
3-5 times per week
6+ times per week

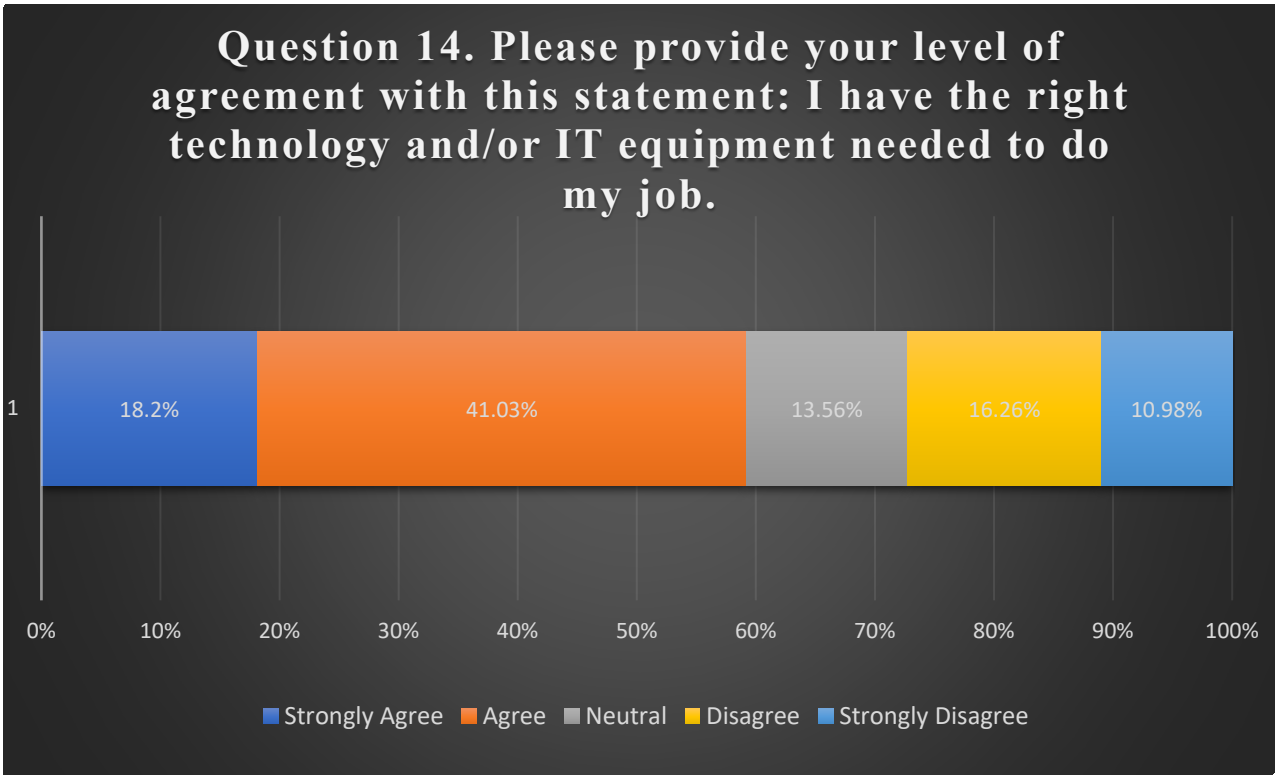

Question 9. How many hours per week have you experienced issues accessing your work email?
60%
50%
40%
30%
20%
10%
0%
30.0%
49.1%
15.7%
5.3%
0 hours within the last week
More than 0 hours but less than 2 hours with the last week
2 hours to 6 hours within the last week
More than 6 hours within the last week

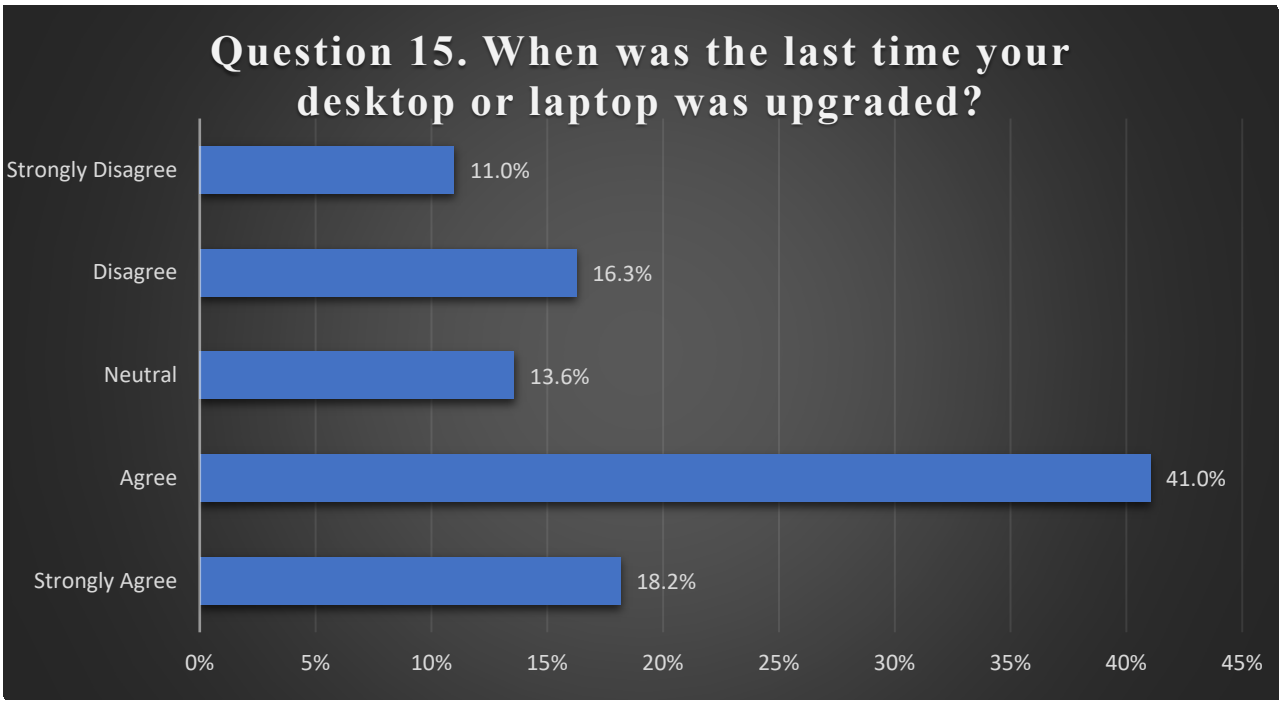

Question 10. How often are you required to reboot your desktop or laptop to gain or improve access to the network or applications during any single work day?
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
38.30%
44.19%
16.30%
1.20%
0 times per day
1 time per day
2-5 times per day
6+ times per day


Question 11. How often are you required to repeatedly re-authenticate your CAC during any single work day?
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
11.15%
19.03%
40.42%
29.39%
Never
1 time a day
2-5 times a day
6+ times a day


Question 12. In the last three months, how many times have you submitted a trouble ticket?
60%
50%
40%
30%
20%
10%
0%
15.36%
22.67%
49.02%
12.95%
0 times
1 time
2-5 times
6 or more times


Question 13. In the last 3 months you submitted more than one IT trouble ticket, were the tickets ever for the same issue?
Yes
43.46%
43%
No
56.54%
57%
Yes
No


Question 14. Please provide your level of agreement with this statement: I have the right technology and/or IT equipment needed to do my job.
1
18.2%
41.03%
13.56%
16.26%
10.98%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
Strongly Agree
Agree
Neutral
Disagree
Strongly Disagree


Question 15. When was the last time your desktop or laptop was upgraded?
Strongly Disagree
11.0%
Disagree
16.3%
Neutral
13.6%
Agree
41.0%
Strongly Agree
18.2%
0%
5%
10%
15%
20%
25%
30%
35%
40%
45%

Appendix G: Public Comments

No public comments received as of February 2, 2023.

This page left intentionally blank

Appendix H: Acronyms

This page left intentionally blank

4ENO	4th Estate Network Optimization
ADVANA	Advancing Analytics
BYOD	Bring Your Own Device
CAC	Common Access Card
CAPE	Cost Assessment and Program Evaluation
CDAO	Chief Digital and Artificial Intelligence Office
CDO	Chief Data Officer
CEMM	Customer Experience Maturity Model
CEO	Chief Executive Officer
CIO	Chief Information Officer
COCOM	Combatant Commanders
COO	Chief Operating Officer
COVID-19	Coronavirus Disease
CPU	Central Processing Unit
CX	Customer Experience
CXO	Chief Experience Officer
DA&M	Director of Administration and Management
DBB	Defense Business Board
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMAG	Deputy's Management Action Group
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DPAS	Defense Property Accountability System
DSD	Deputy Secretary of Defense
EIE	Enterprise Information Environment
FAR	Federal Acquisition Regulation
FFRDC	Federally Funded Research & Development Center
GSA	General Services Administration
GSD	Global Service Desk
ICE	Interactive Customer Evaluation
IT	Information Technology
IT UX	IT User Experience
JCIDS	Joint Capabilities Integration Capabilities & Development System
JITC	Joint Interoperability and Test Command
JSP	Joint Service Provider
LAN	Local Area Network
LCR	Life Cycle Replacement
MILDEP	Military Department
NCR	National Capital Region
NPS	Net Promoter Score
NIPR	Non-Classified Internet Protocol Router

NIPRNET	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
O365	Office 365
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
PC	Personal Computer
QoS	Quality of Service
ROI	Return on Investment
SIPR	Secret Internet Protocol Router
SLA	Service Level Agreement
TMF	Technology Modernization Fund
ToR	Terms of Reference
USAF	United States Air Force
VDI	Virtual Desktop Infrastructure
VHA	Veterans Health Administration
WAN	Wide Area Network
ZTRA	Zero Trust Reference Architecture

This page left intentionally blank

Defense Business Board
1155 Defense Pentagon
Room 5B1008A
Washington, DC 20301-1155

https://dbb.defense.gov

DBB Staff

Jennifer S. Hill, Executive Director
Dr. Sherri Malace, Sr. Advisor to the Executive Director
CAPT Daryl Wilson, USN, Military Representative
Lt Col Kyle M. Harrington, USAF, Military Representative
MAJ Jamaal Kirkland, USA, Military Representative
Janice McLaury, Research Analyst & Writer
Kayla Cross, Management Analyst
Gwyneth Murphy, Analyst
Leah R. Glaccum, Operations Manager
Ademola Oduyebo, Administrative Support
Cheyenne Rodriguez, Administrative Support