The Honorable Margaret Wood Hassan
Ranking Member
Federal Spending Oversight and Emergency Management Subcommittee
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Ranking Member Hassan:

Thank you for the letter dated 3 June regarding modernizing the Department of Defense's (DoD) information technology (IT) systems. The Department shares your concerns regarding security, efficiency, and spending related to legacy IT. To address this, the Deputy Secretary of Defense signed the Department of Defense Digital Modernization Strategy in June 2019 (attached). This strategy provides a clear vision and roadmap for achieving the goals within the National Defense Strategy across five key pillars: Enterprise Cloud; Artificial Intelligence (AI); Cybersecurity; Command, Control, and Communication (C3); and Data Management.

To address your second question related to the Department's modernization priorities and status, below is the high level plan for each of the five priority components. Included is the expected cost and any anticipated cost savings, if known; expected completion date; and the reason for any schedule delays.

Enterprise Cloud

The DoD Cloud Strategy drives the Department's cloud modernization efforts with the objective of establishing a DoD Enterprise Cloud Environment, a multi-cloud, multi-vendor ecosystem. As of June 2020, the current focus is on 1) enterprise acquisitions offering cloud services across security classifications and to the tactical edge and with terms and conditions that benefit DoD as an enterprise and 2) DoD's accelerated adoption of cloud and modern software capabilities such as Development, Security and Operations (DevSecOps) to deliver better software faster. We expect cost to shift from legacy hosting and data center models to modern cloud based digital infrastructure, with a target of 9% of total IT spending dedicated to cloud services by FY2025, up from 3% in FY2022. The Department continues to pursue this approach not exclusively for cost savings, but also for mission impact and the need to be more competitive in a highly-digital and data-rich world. DoD has experienced delays in deployment of its enterprise cloud due to acquisition protest and litigation. The Department now expects the enterprise cloud contract to be awarded in 4QFY20. As modernization of cloud and software capabilities is a continual process, this evolution must happen to ensure that the Department realizes the full potential of new technologies and maintains an advantage over a growing number of digitally-sophisticated adversaries.

Artificial Intelligence

The Joint Artificial Intelligence Center (JAIC) was designated as the Department's focal point for driving the delivery of artificial intelligence (AI)-enabled capabilities, outlined in the

DoD AI strategy. Through this strategy, the JAIC is developing the Joint Common Foundation (JCF), an AI development environment platform that enables application development and experimentation for teams across the DoD. The JCF will be at full operational capability in Q4FY21 due to cloud contract award protests and delays. This platform will contribute to phasing-out legacy systems by consolidating multiple infrastructure environments, creating interoperability and reducing redundancy across Services and components. In addition, the JAIC is advancing a broad portfolio of AI-enabled applications and capabilities to meet diverse mission needs, such as predictive maintenance, joint warfighting and business process transformation (BPT). As an example, under the BPT initiative, JAIC is developing and has deployed a prototype product called GAMECHANGER, which replaces current manual, labor-intensive practices for back office functions, such as policy research, administrative updates to guidance, and enhanced response to Congressional reporting requirements. This direct upgrade of legacy systems to be "AI-enabled" allows for tremendous cost savings and operational efficiency across the Department. The JAIC is taking an outcome-based, risk-informed approach, designing a holistic performance framework for DoD AI by which to measure the return on investment for AI-enabled applications and pivoting in cases where we assess that the return on investment to the Department is not optimized.

Cybersecurity

DoD CIO is leading the Department's effort to modernize its cybersecurity infrastructure. CIO has defined the cyber landscape consisting of ten focus areas for reducing cyber risk, with cost savings as a byproduct. As an example, our Comply to Connect (C2C) effort is enabling the automation of labor intensive and error prone activities associated with security management of endpoints as well as automating the process by which persons gain access to the right resource at the right time for the right reason. The Department is also in the process of implementing programs such as C2C and Automated Continuous Endpoint Monitoring (ACEM), which will work together with Enterprise Patch Management System (EPMS) to provide enterprise-wide automated patching and endpoint monitoring capability. This will enable the provisioning of trusted patches in a timely manner, enhance situational awareness, and provide improved visibility tools. These three capabilities will be deployed across the enterprise over the next several years. The FY2020-2024 funding included $526M for C2C and associated programs such as EPMS and $389M for ACEM. These capabilities will automate labor-intensive patching activities, and are expected to reduce overall operating costs for the DoD. Cost saving projections will be determined once each of these capabilities is operational. The Department anticipates ACEM to be operationalized by the end of CY2020. C2C will be implemented in stages, starting in FY2022 with an estimated completion by the end of FY2024, on both unclassified and classified networks. The EPMS will reach initial operational capability on classified networks by Q3 FY2021.

Command, Control, and Communications

The Department of Defense Command, Control and Communications (C3) Strategy provides direction for bridging the gap between today's legacy C3 enabling capabilities and Joint All Domain Command and Control (JADC2). It describes how the Department will innovate for competitive advantage while building the foundation for a fully networked communications transport layer and advanced C2 enabling capabilities to synchronize joint all domain operations against 21st century threats. The C3 strategy focuses on protecting and preserving current C3

capabilities; ensuring U.S., allies, and key partners have reliable access when needed; and providing seamless, resilient, and secure C3 transport infrastructure enabling a more lethal Joint Force across the full range of military operations. Three key foundational C3 modernization goals received funding and are underway: Enhancing the Delivery, Diversity, and Resilience of Position, Navigation, and Timing Information; Strengthening National Leadership Command Capability; and Providing Integrated and Interoperable Beyond-Line-of-Sight Communications Capabilities. These three capabilities will be deployed to the joint warfighter over the next several years. Modernization funding in the FY2021-2025 budget included $839M for GPS/PNT enhancements and programs such as Strengthening National Leadership Command Capability, which received $241M; $2.4B was provided for the modernization of Beyond-Line-of-Sight Communications Capabilities. The Department anticipates that GPS improvements will be fielded at 70% of the required operational capability by Q2FY27; improved National Leadership Command Capabilities will be operational by Q1FY26, and lastly, upgraded Beyond-Line-of-Sight Communications will fielded at 70% of the required operational capability by Q2FY26. Implementation of this strategy requires synchronizing near-term modernization efforts in and across operating domains, transitioning from stove-piped solutions to a highly-connected, agile, and resilient system.

Data Management

Data management is a fundamental component of the DoD Digital Modernization Strategy. A new DoD Chief Data Officer (CDO) organization has been established and will issue a DoD Data Strategy by Q1FY21. This strategy will provide a vision for DoD to be a data-centric organization that fully utilizes data at speed and scale for increased efficiency and operational advantage. The DoD Data Strategy is not focused on particular acquisitions or program investments, as the key enablers for data management are non-material. This includes a framework for data governance, commonly adopted data architectures, data standards for interoperability, and increased workforce data acumen. The newly-established Chief Data Officer is working to put those elements in place along with the necessary processes to support them. Over the longer term, strengthened data management will help the Department to better collect, share, analyze, and use its data. For example, the DoD is using the a data analysis platform to better integrate IT category management information across different DoD databases. While such efforts will lead to increased efficiency and reduced duplication in future information systems over the next few years, it is too early to quantify specific data-related savings or costs. The CDO organization will reach full operating capability over the next 12 months, as we build a supporting team of data subject matter experts.

To address your third question, the Department shares your concern regarding legacy IT systems that cost more to maintain annually than would be to simply modernize. System 1 which you referenced, also known as the Air Force's Integrated Maintenance Data System – Central Database (IMDS), was upgraded by the Air Force from the legacy programming language, COBOL, to the updated Visual COBOL.NET from September 2018 to June 2020. This update reduces the system's escalating sustainment costs by $19.4M. IMDS was also approved and funded for 're-hosting' of the application and database from a DISA Data Center to the Air Force's Microsoft Azure-hosted "Cloud One" cloud computing environment and is scheduled to go live on July 13, 2020. Our FY21 IMDS CDB DISA bill is expected to be ~$22M. The estimate of the Post Migration Costs that will be required to replace the DISA processing and
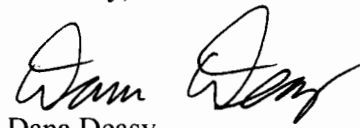
support in the Azure Cloud is about $2.588M in FY21. The delta of ~ $19.4M would represent the projected savings and the benefit of moving IMDS CDB from the DISA UNISYS Environment to the Azure Cloud.

On your fourth question, the Department needs to work to phase out legacy IT systems. In April 2020, the DoD CIO published a DoD-wide application rationalization guidance (attached) with the goal of better managing and modernizing the inventory of DoD systems and applications for improved effectiveness and efficiency. The guidance outlines a process that requires an assessment of DoD systems and applications to determine its relevance in alignment with mission need and advancements in technology. The Department will systematically drive out legacy systems through this process as a key goal. In May 2020, DoD CIO also released a memo on software license maintenance requiring programs to maintain up-to-date software and to plan for end-of-life transitions, which will ensure the Department maintains a resilient cybersecurity posture while benefiting from ever-evolving software features.

Regarding your fifth question, the DOD CIO coordinates closely with the Under Secretary of Defense Comptroller on IT matters, and also with the DoD Chief Management Officer and Under Secretary of Defense for Acquisition and Sustainment on IT acquisitions. Together, these offices ensure that IT investments and new IT acquisitions support the Department's Digital Modernization Strategy and the National Defense Strategy. The Federal Information Technology Acquisition Reform Act (FITARA) has reinforced the importance of senior leadership involvement in the decision-making process for DoD IT investments to ensure the Department is leveraging scarce resources on those IT capabilities that are most critical for the warfighter and in support of DoD business operations.

On your final question related to support from Congress, the Department is grateful for Congress' continued bipartisan backing to the DoD for its progress toward digital modernization. Fully funding the Department's priorities is the most valuable support that Congress can provide toward IT modernization. Modernizing government IT systems for future applications is critically dependent on having flexible and dependable resources, such as working capital funds, to sun-set legacy IT systems and practices in favor of modern, open-architecture, cloud-hosted systems. The Department will continue to strive towards modernization of its legacy IT systems to achieve greater reliability, security and efficiency.

Sincerely,

Dana Deasy

cc:
Thomas W. Harker
Performing the Duties of the Under Secretary of
    Defense (Comptroller)/Chief Financial Officer