Ellen M Lord - Opening Statement,
HASC Cyber, IT, and Innovation Subcommittee Hearing on Software
March 13, 2024

In an era of strategic competition among technologically advanced powers, software will shape the nature of deterrence and define national security advantage. The urgency to empower our defense and national security apparatus across all domains with both the best existing and emerging technology is critical to not only preserve our freedoms, but also those of our partners and allies. Our nation has developed and operationalized technology solutions that have transformed our commercial sector and in turn our everyday lives. Now we must harness and apply this ingenuity and innovation to bolster U.S. military superiority in the digital age. Given current geopolitical conditions, the stakes could not be higher.

Software development and implementation in support of our country's defense and intelligence infrastructure needs to meet the challenge of the moment. To fall short now would not be just a bureaucratic debacle, but a source of imminent risk to our ability to deter, fight, and win. The ability to quickly develop and deliver capability to close the gap between information discovery and mission response is a defining differentiator in emerging global competition.

Defense and intelligence agencies must develop, acquire, execute and maintain software to meet current mission needs while also having the agility to quickly respond to future threat environments. The statutory, regulatory, and budgetary framework for these agencies are ripe for streamlining to build and maintain the nation's software advantage.

Fostering a culture of buying readily available commercial software offerings

The Department of Defense (DoD) procurement process is one of the greatest challenges and opportunities to software acquisition. Often, software is purchased using the same approach that traditionally is employed for major hardware system purchases. Typically, this entails setting rigid requirements, conducting lengthy solicitation processes, and ultimately, years later, facing costly sustainment contracts to adapt software that is often obsolete on delivery. Although alternative acquisition pathways exist, they are only as effective as acquisition professionals' ability to implement them.

Funding professional training and development for acquisition professionals to ensure they have key skills for implementing the full spectrum of acquisition approaches will enable the best and most innovative software and technology are quickly provided to the national security workforce. DoD must operationalize policies and procedures to support the use of modern software development and delivery practices such as agile software development life cycle, software-as-a-service delivery, human-centered design, DevSecOps, and modern technology stacks.

The Defense Acquisition University (DAU) and other organizations maintain a series of credentialing programs supporting the continuing education of the defense acquisition workforce. While DAU has expanded their training programs to help align offerings with present-day defense capabilities, there needs to be more of an emphasis on developing a cadre of acquisition professionals who are familiar with the nuances and opportunities of procuring nontraditional and emerging technologies, such as software. Acquisition professionals must also be trained through use of case studies detailing how Program Executive Officers (PEOs) and Program Managers (PMs) can utilize multiple authorities to rapidly acquire software. There is a demand for experiential learning utilizing real-life examples explaining how procuring hardware is different than software and how working with small businesses differs from contracting with large primes. These efforts should fall under the Software Acquisition Credential Program and should include multiple courses. In short, training innovation must keep pace with software innovation.

Lower Barriers of Entry for Newer Innovative Companies to the National Security Space

DoD highlighted in its 2023 Software Modernization Implementation Plan that America's national security capabilities "will depend on DoD's proficiency to deliver resilient software capabilities rapidly and securely." When a new software application or information process is to be used by DoD, it must be compliant with The National Institute of Standards and Technology (NIST), meeting security and privacy controls. Approval of software systems is granted through the Authority to Operate (ATO) process. Obtaining ATOs can take months, if not up to a year, and often processes have to be replicated within programs, Services, and DoD entities. There is an opportunity to streamline and modernize the process of certifying software applications for security and resiliency to deliver the competitive advantage desired.

Rapid software delivery, in part, depends on a continuous Authority to Operate (cATO) process versus episodic Authority to Operate (ATO) issuance. A cATO process will provide continuous monitoring to detect cybersecurity activity, real-time cyber defense and adoption of an approved DevSecOps reference design.

DoD's guidance on cATO is gaining momentum, but additional steps are required for the cATO promise to be fully realized. A critical first step is to require an ATO joint standard or common definition ATO for DoD. Currently, some military departments have policies that require ATO reciprocity among their systems. The Department released updated July 2022 guidance for the "DoD Information Enterprise to use cybersecurity reciprocity" and for Authorizing Officers (AOs) to "promote reciprocity as much as possible." I strongly support continued efforts and implementation of these policies across Services and components to help improve the process and cycle time of lengthy sequential certification processes. Consistent institution and execution across DoD for the evolution from static ATO to cATO will catalyze consistency and portability as systems and software move into continuous evaluation and approval.

The arduous ATO process may prohibit small businesses and new entrants from overcoming the valley of death. Funding and policy changes are needed to increase resources for training and, if needed, additional support and staff for different parts of the DISA and ATO process to handle the bottlenecks in the approval process for the government. DoD should assess the potential for automation, including AI-enabled systems and software, to streamline the ATO certification process where appropriate with sufficient internal controls and appropriate oversight. DoD should reduce the number of approval gates in the ATO review process and determine how to grant more ATOs on an annual basis as DISA is mandated to approve up to only 12 systems a year.

Thanks to Congress for Sec. 1513 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 which required the CDAO to “develop and report on an actionable plan for the Deputy Secretary to reform the technologies, policies, and processes used to support accreditation and authority to operate decisions to enable rapid deployment into operational environments of newly developed government, contractor, and commercial data management, artificial intelligence, and digital solutions software.” I thank the Armed Services Committees in FY24, too, for their attention to ATO decisions and timelines and the related impacts to small businesses and nontraditional vendors. It was included as report language accompanying the conference report.

Resourcing Reforms

We need to strengthen available tools and establish new acquisition and budgetary tools that shorten the cycle time to develop and approve software projects, with automated reporting and review to enhance oversight.

The recently released final report from the Commission on Planning, Programming, Budgeting, and Execution (PPBE) Reform makes multiple recommendations that will support faster software fielding. These recommendations, if implemented, will have a broader impact than just software as they recognize the need for resourcing speed and agility given the reality of ever-increasing geopolitical threats coupled with the acceleration of emerging technologies.

PPBE recommendations recognize that PEOs and PMs need the agility to insert new technology and move modest amounts of funds in the year of execution, in addition to carrying over small amounts of budget at year end. The recommendations acknowledge that incorrect alignment of colors of money often delay program execution. Specifically, the Commission recommends allowing Procurement; Research, Development, Test and Evaluation (RDT&E); or Operations and Maintenance (O&M) to be used for the full cycle of software development, acquisition and sustainment. Current cost and schedules are pre-set to hardware-centered regulations and processes that are a mismatch for the speed of delivery needed for software to be relevant.

Building the Data Governance and Policies to Sustain AI Dominance

AI holds the promise of transforming industries and helping the Department tackle complex problems. Striking the right regulatory balance can incentivize companies, both large and small, to invest in research and development, driving advancements in AI technology. By protecting intellectual property rights and fostering an environment that encourages experimentation, Congress can empower all parts of the defense industrial base to assist the Department in maximizing the potential of AI while making sure governance guardrails are in place to foster safe development.

AI/ML software development relies on having data available for model training and validation. The quality and quantity of the data available for model development, together with a human(s) in the loop (HITL) determine the effectiveness and mission-meeting capability of the constructed software system ; as AI/ML software systems are built through tuning tailored algorithms on exquisite training data and interpretation and contextual assessment by Subject Matter Experts (SMEs,) based on use case and desired mission outcome.

Industry is evolving to provide benchmark data sets in order to better evaluate the reliability and value of AI/ML models. These benchmarks enable the comparison of existing and new models on a standardized set of performance criteria on a normalized set of data. This benchmarking of AI/ML models is essential for maintaining high standards of excellence and predictability when developing AI/ML-based software systems and solutions. These standards contribute to transparency and help build confidence and trust in AI/ML technologies. The Federal Government values the use of off-the-shelf solutions, such as Software-as-a-Service products, but does not have a standard methodology or framework across agencies for allowing both one-time and on-going access to the data that is used as the basis for growing a healthy ecosystem of next generation software companies leveraging generative AI/ML capabilities. To effectively train mission-oriented models, software developers must have access to both one-time and on-going access to libraries of mission-relevant data. This can be done in a secure manner, consistent with today's government security standards. Providing a readily available corpus of relevant data is a necessary condition in order to create a vibrant ecosystem of software providers and a key incentive for private capital, founders, and employees to enter the defense market.

Thank you to Congress for passing the pilot program in FY 2022 and codifying the DoD data libraries program in the FY 2023 NDAA to facilitate the development of AI capabilities. I look forward to seeing the Secretary of Defense delivering on congressional direction and developing data repositories with the right safeguards to substantially increase the speed with which companies can develop data analysis software and improve the ability of such products to produce accurate, meaningful analysis to inform mission decisions.

Pulling Together for Mission Needs

We have to get data out of silos so information is readily accessible and comprehensible to decision makers. The future of defense is about visibility and knowledge, empowered by software, so that our leaders can make better, faster decisions.

Sharing data under the right conditions, especially when we're using AI to help us make decisions to support service members being deployed, is paramount to the mission. That is because in national defense and within the battle space, where there is information and intelligence incoming from across air, land, maritime, space, and cyberspace domains, enabling similar data to be collated into the same place, providing a common operating picture with the best context and improving the ability to deliver advanced AI capabilities for mission success.

The United States today requires, and must invest in, software that offers interoperability and the ability to understand, decide, and respond to global threats at both speed and scale. We are years behind the commercial sector, and in some cases, our adversaries and we must bridge that gap in as short a time as possible.

Software enabled capabilities with AI-embedded features can be used to integrate a trustworthy view of best available assets across distributed commands, collaborative mission planning can occur within software and distributed users can impact the mission from any seat. And, there is commercially available, modern AI-enabled software capabilities available today that operators and decision makers can leverage to begin these activities.

In order to ensure the best technology is available at the time, scale, and speed our warfighters need, it will require a shift in how the Department acquires software. This shift includes building a skilled workforce to acquire and deploy the best mission-focused software; building a resourcing structure that allows the Department to respond securely and quickly to a digital battle space; lowering the cycle time and cost for newer innovators to support national security missions; and building the data governance and infrastructure needed.