Director, Operational Test and Evaluation

Digital Twin Assessment, Agile Verification Processes, and Virtualization Technology

July 2022

Nickolas H. Guertin
Director

This page intentionally left blank.

Executive Summary

This report summarizes the assessment of the state of digital twin practices in the Department of Defense (DOD) and the relevant verification, validation, and accreditation (VV&A) body of work, as well as a plan to use commercial virtualization technology in weapon systems and for deployed forces. The report is based on the survey that the office of the Director, Operational Test and Evaluation (DOT&E) administered to programs under DOT&E oversight and on the Software Acquisition Pathway. DOT&E validated the survey data through interviews with select program offices and DOT&E staff. This report is written in response to the House Report 117-118 to accompany the Report of the Committee on Armed Services House of Representatives on H.R. 4350, Public Law 117-81 National Defense Authorization Act for Fiscal Year 2022.

Approximately 14 percent of programs under DOT&E oversight are applying continuous integration/continuous delivery (CI/CD) methodologies, and approximately 7 percent have built or are planning to build digital twins. One of the eight programs under DOT&E oversight and on the Software Acquisition Pathway is using CI/CD methodologies and one is building digital twins.

Digital twins have not yet been used to support operational or live fire test and evaluation (T&E). While a body of work on the VV&A of digital twins is still being developed, the guidance that DOT&E, in coordination with the Office of the Under Secretary of Defense for Research and Engineering, is developing for verification and validation (V&V) of modeling and simulation (M&S) will apply to digital twins. Many of the same gaps that affect M&S also affect the credible use of digital twins. Additional case studies are needed to demonstrate and standardize adequate processes that would support more Agile VV&A of either M&S or digital twins.

The plan to use commercial virtualization technology in weapon systems and for deployed forces includes the requirement to evaluate the benefits of commercial virtualization, including energy savings, potential reliability improvements, and hardware savings while creating and maintaining more complex security boundaries. The plan also emphasizes the requirement to assess the dependencies of the system and its components on specialized real-time computer processing wherein virtualization may pose a performance or power consumption concern for tactical applications. Finally, the plan commits to developing tools and processes needed to adequately evaluate the operational performance of systems employing such technologies.

The complexity of the multi-domain operational environment and associated operational constraints are increasingly making digital technologies a critical aspect of T&E. For example, digital twins that can be subjected to repeated cyberattacks as the threats and the system itself evolve and will allow for continuous evaluation of cyber survivability for the mission to keep pace.

While digital twins create new opportunities for T&E to enable assurance of continuously evolving systems, dedicated investments and initiatives are needed to standardize and implement this approach. There is an opportunity to address the challenges of using of such capabilities as

well as integration of model-based engineering to optimize integrated T&E approaches from the inception of the program through the end of its lifecycle.

Assessment Adequacy

Due to the different interpretations of what is considered a digital twin and the fluid nature of implementing digital twins in acquisition programs, on April 5, 2022, DOT&E administered a survey to its own staff to support the required assessments. In parallel, DOT&E issued a survey to the Service's T&E Executive staff to validate the internal responses or adjudicate any differences. The DOT&E oversight list includes 72 Army, 67 Air Force, and 85 Navy or Marine Corps acquisition programs. The DOT&E oversight list also includes 19 acquisition programs managed by other organizations (e.g., Missile Defense Agency, National Security Agency, etc.). Of those 243 acquisition programs under DOT&E oversight, 8 programs (or component programs) are on the Software Acquisition Pathway. Combined, the internal and external surveys provided reportable details on 195 programs under DOT&E oversight including 6 programs on the Software Acquisition Pathway. Table 1 summarizes the details.

Table 1. Summary of Programs Under DOT&E Oversight List or on the Software Acquisition Pathway (SWP) and Their Coverage in This Report

Total (SWP)	Army (SWP)	Air Force (SWP)	Navy & Marine Corps (SWP)	Other (SWP)
Number of Programs Under DOT&E Oversight to Include Programs on Software Acquisition Pathway Enumerated in Parenthesis				
243 (8)	72 (2)	67 (3)	85 (1)	19 (2)
Survey Data Availability on CI/CD and the use of Digital Twins for Programs Under DOT&E Oversight to Include Programs on Software Acquisition Pathway Enumerated in Parenthesis				
195 (6)	55 (2)	65 (3)	62 (1)	13 (0)
Total number of DOD Programs on the Software Acquisition Pathway				
35	6	9	10	10
Survey Data Availability on CI/CD and the use of Digital Twins for Software Acquisition Pathway Programs				
6	2	3	1	0

Acronyms: CI/CD – Continuous integration/continuous delivery; DOD – Department of Defense; DOT&E – Director, Operational Test and Evaluation; SWP – Software Acquisition Pathway

The State of CI/CD and Digital Twin Practices in the DOD

Definitions

CI/CD is a component of the Development, Security, Operations (DevSecOps) software development method used to increase the speed of capability delivery.[1] Development (Dev) is normally done using the Agile process that delivers software in small and regular increments. CI/CD, in particular, is a set of software and hardware development practices that automate the

[1] There is an important distinction between "delivery" and "deployment;" continuous delivery enables frequent software releases to staging or various test environments once verified by automated testing, but does not necessarily entail deployment to fielded systems.

building and testing of new software releases. The DOD Enterprise DevSecOps Strategy Guide describes DevSecOps as an iterative process consisting of ten phases shown in Figure 1.

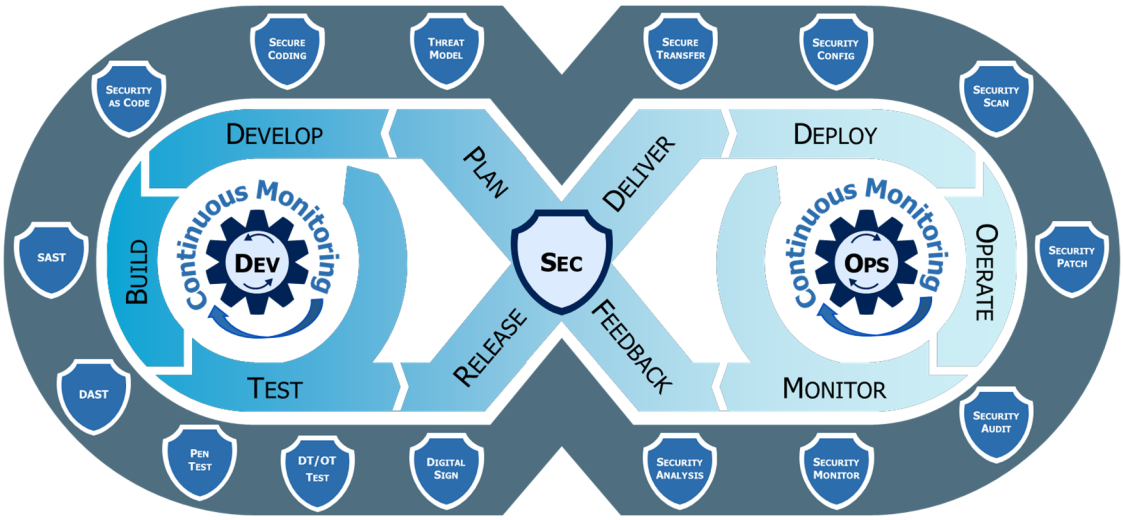

Figure 1. DevSecOps Distinct Lifecycle Phases and Philosophies.

Different organizations ascribe different meaning to the term "digital twin." For example, the Army Program Executive Office (PEO) for Ground Combat Systems defined the digital twin as "a virtual representation of a connected physical asset." The Navy T&E executive staff defined it as "[a] virtual model that is created to reflect an existing physical object. The model can represent more than physical characteristics, to include the operations/behavior of the physical object." The Air Force T&E executive staff quoted the National Institute of Standards and Technology (NIST) definition: "[a] digital twin is the electronic representation – the digital representation – of a real-world entity, concept, or notion, either physical or perceived."[2] This report uses the NIST definition provided above with the following clarifications:

- The defining feature of a digital twin is the ongoing data integration between the digital model and its physical unit counterpart.
- Digital models used for research and development can evolve into digital twins of specific units once they are produced and fielded, and these twins can continue to be updated as their underlying digital model is refined.

The Use of CI/CD Approaches in Programs under DOT&E Oversight or on the Software Acquisition Pathway

Approximately 28 percent of surveyed Air Force programs (18 of 65), 11 percent of surveyed Army programs (6 of 55), and 18 percent of surveyed Navy and Marine Corps surveyed programs (11 of 62) under DOT&E oversight or on the Software Acquisition Pathway are using CI/CD approaches. Table 2 provides additional details.

---

[2] NISTIR8356 (DRAFT) Considerations for Digital Twin Technology and Emerging Standard.

Table 2. Programs under DOT&E Oversight Using or Planning to Use CI/CD Methodologies (Software Acquisition Pathway Programs in Light Gray)

	Program	CI/CD Status
Air Force	Air Force Maintenance, Repair and Overhaul Initiative (MROi)	The program shifted to an Agile approach three years ago. The program switched their development environment to their production environment.
	Joint Cyber Warfighting Architecture (JCWA)	The program is developing a platform called DARK ASTER, an open-source system with shared common services for developing, integrating, testing, and deploying software capability. Currently, each subcontractor uses an on-premises instantiation of the current pipeline configuration to field capabilities.
	Air Force Next Generation Air Dominance	The program is using Agile approaches consistent with CI/CD.
	Air Operations Center Weapon System Modifications	The program is delivering capability incrementally, consistent with CI/CD approaches.
	Defense Enterprise Accounting & Management System (DEAMS)	The program is using the Scaled Agile Framework and continues to work toward improving their pipeline, which uses continuous exploration, integration, and delivery.
	Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Inc. 2B	The program has been delivering “micro-releases” consistent with CI/CD approaches.
	F-22 - RAPTOR Advanced Tactical Fighter Aircraft	The program has adopted Agile approaches. It releases new software builds to the fleet annually.
	Future Operationally Resilient Ground Evolution (FORGE) Rapid Prototype	The program is attempting CI/CD approaches and is working on defining its end state and objectives.
	GPS III; GPS III Follow-on Production; and GPS Next Generation Operational Control System Block 3F	The three programs are using a variety of development approaches, including both waterfall and Agile approaches with CI/CD. (Note that these three programs are accounted for separately in the total Air Force programs reflected in this report.)
	HH-60W Jolly Green II	The program is attempting Agile approaches. The program plans to settle into an annual cycle for software and minor hardware updates once it goes into full rate production.
	Integrated Strategic Planning and Analysis Network (ISPAN) Increment 5	The program is using CI/CD approaches and has a robust test environment that gets switched to production when ready.
	Next Generation Operational Control System	The program is using a variety of development approaches, including both waterfall and Agile approaches with CI/CD.
	Nuclear Planning and Execution System (NPES)	The program is planning to adopt the same Agile CI/CD approaches used by ISPAN upon delivery of initial operating capability.
	Protected Tactical Enterprise Service (PTES)	The program is using Agile CI/CD approaches in its development. The frequency of software releases with new operational capabilities is approximately once every eight months. The program additionally has monthly software releases that do not add substantial operational capability. These releases are currently targeting testbeds.
	Space Command and Control System	The program is using Agile DevOps and attempting CI/CD approaches. Challenges are related to the difference in classification between the development environment (unclassified) and the deployment environment (a multilevel security environment).
	Three-Dimensional Expeditionary Long-Range Radar	The program is new and plans to use Agile CI/CD approaches.

Army	Distributed Common Ground System - Army (DCGS-A)	The program shifted to Agile approaches and has been working towards CI/CD approaches following Increment 1. It is delivering capability developments (CDs). CD1 took 2 years to fully deploy and CD2 is expected to take around 2.5 years.
	Enterprise Business Systems Convergence	The program is new and plans to adopt Agile CI/CD approaches.
	Infantry Squad Vehicle (ISV)	The program is aligned with the objectives of CI/CD. Once software updates are approved, they are delivered to the fielded systems via an onboard software update.
	Joint Light Tactical Vehicle (JLTV) Family of Vehicles	The program manages software development in accordance with the tenets of CI/CD. The evolving software baseline continues to support added JTLV functionality. Changes are validated through a combination of Systems Integration Lab (SIL) and physical vehicle testing. The program is working to automate SIL testing and implement cloud distribution of software to expedite its availability to the field.
	Tactical Intelligence Targeting Access Node (TITAN)	The program is planning to use CI/CD approaches.
	Terrestrial Layer System (TLS)	The program uses the Agile methodology for continuous, rapid software development. Each contractor has an internal CI/CD pipeline that enables automatic building and testing of new software releases. New releases are not yet automatically deployed to fielded systems.
Navy and Marine Corps	Aegis Weapon System	The program founded a Prototype Software Factory "The Forge" to provide a virtual and physical ecosystem to foster Agile software development using CI/CD approaches. The Forge is initially focused on upgrades to the user interface and user experience of the Aegis Weapon System, introduction of mission planning and battle management aides, and foundational infrastructure changes.
	Consolidated Afloat Networks and Enterprise Services (CANES)	The program is using a CI/CD approach for hosted applications within the Over Match Software Armory that they intend to field on shipboard platforms.
	Distributed Common Ground System - Navy (DCGS-N)	The program uses the pre-production staging environment in the Over Match Software Armory as part of the CI/CD process and intends to move development and integration work to the software factory for complete CI/CD.
	E-2D Advanced Hawkeye	As the program progresses through Delta System Software Configuration-4 (DSSC-4) and into DSSC-5, software development has migrated to the Agile construct and incremental delivery.
	F/A-18E/F Super Hornet Aircraft; EA-18G Airborne Electronic Attack; and Infrared Search and Track (IRST)	These programs develop software using Agile concepts. While formal fleet software deployments remain roughly every two years, Early Operational Capability releases are being used to incrementally deliver capability as future plans for continuous delivery are matured. (Note that these three programs are accounted for separately in the total Navy programs reflected in this report.)
	MK 48 ADCAP Common Broadband Advanced Sonar System; and MK 54 torpedo/MK - 54 VLA/MK 54 Upgrades Including High Altitude ASW Weapon Capability (HAAWC)	These programs use Agile methods to develop software. Models of all software algorithms are used to test inputs and outputs as single entities or subsystems/systems in order to identify issues early in the software release cycle. Once performance of the model is proven, it is exercised in a hardware-in-the-loop simulator. (Note that these two programs are accounted for separately in the total Navy and Marine Corps programs reflected in this report.)
	MQ-25 Stingray	The program utilizes Agile software development practices consistent with CI/CD and auto-code technology where feasible. This approach is intended to continue into the production phase of the program.
	VH-92A Presidential Helicopter	The program employs the use of Agile SCRUM methodologies and Kanban for continuous and rapid software development.

The Use of Digital Twins as an Enabler to Extending the Efficacy and Efficiency of CI/CD Approaches in Programs under DOT&E Oversight or on the Software Acquisition Pathway

Approximately 11 percent of surveyed Air Force programs (7 of 65), 11 percent of surveyed Army programs (6 of 55), and 5 percent of surveyed Navy and Marine Corps programs (3 of 62) under DOT&E oversight or on the Software Acquisition Pathway are building or planning to build digital twins that could be used as an enabler to extending the efficacy and efficiency of CI/CD approaches. Table 3 summarizes the details.

Table 3. List of Programs under DOT&E Oversight or on Software Acquisition Pathway Building or Planning to Build Digital Twins (SWP Programs in Light Gray)

	Program	Digital Twin Status
Air Force	Air Force Next Generation Air Dominance (NGAD)	The program is using advanced digital engineering approaches consistent with the development of digital twins.
	B-52 Commercial Engine Replacement Program (CERP)	The program has been working to build digital twins but has exhibited challenges in articulating their use cases over the long-term. The amount of live test data needed for adequate verification and validation (V&V) of the underlying digital models presents a challenge. It may be less resource intensive in the short-term to conduct live tests for the purposes of system evaluation rather than rigorous model V&V.
	F-22 (F-22 in a box)	The program is attempting to build digital twins but has not yet successfully demonstrated them due to a lack of integration with fielded physical aircrafts.
	F-35 (F-35 in a box)	The program is attempting to build digital twins but has not yet successfully demonstrated them due to a lack of integration with fielded physical aircrafts.
	GPS III and GPS III Follow-on (GPS IIIF)	These two programs have developed complex satellite simulators that incorporate the actual satellite hardware and software. These simulators can be configured as a digital twin with substantial data integration between it and its assigned orbiting satellite, to assist in investigating and resolving on-orbit anomalies, for instance. (Note that these two programs are accounted for separately in the total Air Force programs reflected in this report.)
	LGM-35A Sentinel (Ground Based Strategic Deterrent)	The program is working to develop highly-sophisticated digital twins as part of its Digital Engineering System (DES). DES is being designed to integrate engineering diagrams, requirements, and software/hardware architectures into a unified modeling environment. Some of these integrations have proven challenging. DOT&E, Air Force Operational Test and Evaluation Center, and Northrup Grumman are working together on the highly complex endeavor of DES VV&A.
Army	Future Long Range Assault Aircraft (FLRAA)	This program is working on delivering a digital model of this future aircraft as well as an emulator of its cockpit. The Army will then transition FLRAA to the Major Capability Acquisition pathway to develop the physical aircraft. The Army intends to use digital twins throughout the acquisition process.
	Improved Turbine Engine Program (ITEP)	The program recently completed building their first engine from a digital model, and plans to develop digital twins of the engines as they enter production.
	Indirect Fire Protection Capability (IFPC)	The program plans to build digital twins of these vehicles, but the program is in an early stage of development.
	Optionally Manned Fighting Vehicle (OMFV)	The program plans to build digital twins of these vehicles, but the program is in an early stage of development.
	Robotic Combat Vehicle-Light (RCV-(L))	The program plans to build digital twins of these vehicles, but the program is in an early stage of development.

	Tactical Intelligence Targeting Access Node (TITAN)	This new Middle Tier of Acquisition program is planning to use a digital twin.
Navy and Marine Corps	DDG 1000	The program is exploring a digital twin for DDG 1000 Electrical System Monitoring.
	MQ-25 Stingray	The program is developing digital twins of each aircraft as well as the Static Test Article and Fatigue Test Article.
	VH-92A Presidential Helicopter	The program leverages an emulation model used to plan aircraft network upgrades and implement necessary ground changes to reduce timeline and risk to operations.

The Adequacy of Digital Twins for T&E Purposes

The digital twins used in programs under DOT&E oversight or on the Software Acquisition Pathway have not yet been used to support operational performance evaluations. Programs are using digital twins to help with engineering. We have observed some potential for using digital twins in developmental tests. For example, the Improved Turbine Engine Program (ITEP) has a digital twin of their engine, which is useful for determining the effects of fixes and tweaks to the engine. The level of fidelity to accomplish some engineering tasks with models is not the same level that would be required to support an evaluation of operational performance. This is partially because a complete evaluation will require not only a digital twin of the system under test, but also a high-fidelity simulation of the operational environment, to include representative threat systems and any other mission-relevant aspects that can affect mission performance. These are all critical elements that need to be aggressively pursued to support the integration of T&E in model-based system engineering, optimize the use of integrated T&E, and support adequate and continuous evaluation of operational performance as systems are built to more dynamically evolve over time. In addition to the potential for using digital twins in T&E as high-fidelity digital models also exhibit potential use in training (e.g., realistic cyber warfare training for operational forces).

The Existing VV&A Body of Work

Digital twins have not yet been verified and validated to the extent needed to contribute to operational or live fire T&E. Of the programs that have reported the use of digital twins, many are only used for contractor-level testing in support of engineering and manufacturing development, rather than government testing. Other programs such as Future Long-Range Assault Aircraft (FLRAA), Optionally-Manned Fighting Vehicle (OMFV), and Next-Generation Air Dominance (NGAD) plan to use digital twins, but these programs are early in development. The first program to use a digital twin that might contribute to an operational test evaluation is LGM-35A Sentinel (Ground Based Strategic Deterrent), but testing has yet to begin.

The same principles and challenges of traditional M&S apply to the V&V of digital twins. Effective V&V requires early planning and adequate resourcing to support a rigorous "test, predict, refine" feedback loop approach. In this approach, programs must iteratively collect data from live, operational testing, as well as predictions from the digital twin on the outcomes of the live test. The predictions and the live data must be analyzed to determine where differences between the digital twin and the real system lie, so refinements to the simulation can be made to move the digital twin closer to validation. Additional investments and case studies are needed to develop and validate the process needed to adequately leverage Agile development methods in V&V.

Recommendations on How Adequacy Can Be Developed and Determined in a More Agile Process as the Digital Twin Evolves, Instead of Through a Waterfall Process Enacted at the End of the Digital Twin Development

An adequate assessment of a digital twin requires an assessment of the boundaries within which the digital twin should be considered representative of the live system and the limits of that representation. When digital twins are used in T&E, an adequate assessment also requires a statistically based, quantitative comparison of "live data" to "simulation output." V&V needs to be planned and resourced early, and executed iteratively. V&V plans should continuously evolve over the system lifecycle, and should capture: (1) the number of events/data required to support an adequate comparison, (2) range of conditions for comparison, (3) a plan for collecting data from live testing and predictions from simulations, (4) analysis of statistical risk, and (5) the validation methodology. The V&V process should quantify the uncertainty in the representation of the digital twin and assess the risk of that uncertainty to an evaluation of operational performance.

As noted in Table 3 for the B-52 Commercial Engine Replacement Program, the amount of live test data needed for adequate V&V of the underlying digital models presents a challenge. In the short-term, it may be less resource intensive to conduct live tests for the purposes of system evaluation rather than conducting a rigorous V&V. Nevertheless, the complexity of the multi-domain operational environment and related open air testing constraints are increasingly making digital technologies a necessity for adequate T&E.

Validation not only requires a sound experimental design for the live data (ideally matched with the model output), but also a sound design strategy for covering the model domain. This is consistent with the National Research Council observation that validation activities can be separated into two general categories: (1) external validation (i.e., comparison to live test data), and (2) parametric analysis (i.e., investigation of model outcomes across the model input domain).[3] These strategies can be applied in an Agile development process, but adequate resources need to be allocated to continuously verify and validate digital twins. Successful Agile V&V will require effective communication and coordination between developmental and operational testers, and enough "live" test data to make robust conclusions about model performance. Additional case studies are needed to validate and standardize the process needed to optimize Agile V&V.

Commercial Virtualization

Definition

Commercial virtualization consolidates computing resources by using software technologies to containerize the software or simulate the hardware of a system. The National Institute of Standards and Technology (NIST) Special Publication 800-125 defines virtualization as:

---

[3] National Academy of Sciences Report (ISBN 0-309-06551-8), "Statistics, Testing, and Defense Acquisition, New Approaches and Methodological Improvements," 1998.

> The simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM). There are many forms of virtualization, distinguished primarily by computing architecture layer[...] In full virtualization, one or more operating systems (OS) and the applications they contain are run on top of virtual hardware. Each instance of an OS and its applications runs in a separate VM called a guest operating system. The guest OSs on a host are managed by the hypervisor, which controls the flow of instructions between the guest OSs and the physical hardware, such as CPU, disk storage, memory, and network interface cards. The hypervisor can partition the system's resources and isolate the guest OSs so that each has access to only its own resources, as well as possible access to shared resources such as files on the host OS. Also, each guest OS can be completely encapsulated, making it portable. Some hypervisors run on top of another OS, which is known as the host operating system.

One advantage of virtualization is that resources can be dynamically allocated among containers or virtual machines, which increases flexibility in deploying capability and may result in a smaller hardware footprint. In one example, it may be possible to virtualize several "guest" operating environments within one physical computer, rather than needing to purchase several physical computers. Also containerization facilitates modularity, portability, improved security and flexibility while lowering technical risk. Thus, some tasks that have traditionally been accomplished with several computers could be accomplished with one. Usage of virtualization technology brings several potential benefits to DOD programs, including:

- Ease of deploying software updates;
- Ease of managing and configuring the virtual environment;
- Energy and hardware savings;
- Ease of reverting software updates;
- Reliability improvements; and
- Increased adaptability to changing program requirements.

Programs will need to systems engineer their computing needs to ensure the optimum virtualization technology is implemented and to occasionally revisit architecture decisions as these technologies evolve and open up alternative efficiencies. For example, as containerization technologies have advanced, more and more cloud computing solutions can natively implement virtualization and emphasize end-user interaction through web-based applications.

Of note, the Persistent Cyber Training Environment has gained substantial value from its extensive and large-scale deployment of virtualization.[4]

Navy Aegis

The Navy's PEO of the Aegis program, PEO Integrated Warfare Systems, has conducted successful experimentation wherein Aegis Weapon System (AWS) software has been enabled to

---

[4] https://www.peostri.army.mil/persistent-cyber-training-environment-pcte

operate on virtual machines running on transportable commercial off-the-shelf (COTS) computer servers and then integrated with the shipboard tactical system. The PEO demonstrated during a live fire engagement that they can operate the shipboard tactical system from this virtualized version of the AWS software. The PEO is now focused on decoupling the AWS software baseline from the tactical shipboard hardware so that the software runs on virtual machines established by the hypervisor. The PEO envisions that this transition to virtualized machines will allow the AWS software baseline to be decoupled from shipboard hardware updates, as the need for processor upgrades will be reduced due the ability to more efficiently use the available computing power. In addition to easing the deployment of new software versions and capabilities, this will enable Aegis ships with this upgrade to have two AWS software environments running in parallel on the same tactical system: the first running the tactical baseline connected to the tactical system, and the second as a "sandbox" for training, testing, and experimentation.

Plan to Use Commercial Virtualization Technology in Weapon Systems and for Deployed Forces

Acquisition programs should plan to use virtualization, especially as part of their CI/CD and T&E processes. However, as discussed in a report by NIST, virtualization can have negative security implications.[5] In particular, the report highlights that virtualization adds layers of technology, which can increase the security management burden by necessitating additional security controls. Combining many systems onto a single physical computer can cause a larger impact if a security compromise occurs. While some virtualization systems make it easy to share information between the systems, this convenience can turn out to be an attack vector if it is not carefully controlled. In some cases, virtualized environments are quite dynamic, which makes creating and maintaining the necessary security boundaries more complex. Consequently, the plan to use commercial virtualization technology in weapon systems and for deployed forces must emphasize that systems' software be safely run on commercially available computer hardware and that this safety be proven through T&E. The plan must also require an assessment of the value added of using such technologies given the safety implications. For example, the assessment should quantify the value added of consolidating the applications to run on centralized computer servers instead of individual desktops or consoles (i.e., energy usage savings) and the value added of hastening software deployment by delivering products to a virtualized environment. A key best practice in virtualization is to conduct a careful assessment of the system's operating and information technology environment and related needs.

The plan to use commercial virtualization technology in weapon systems and for deployed forces must also account for the suitability of software virtualization for real-time tactical applications, especially those that are memory- or processing-intensive, subject to power consumption restraints, or must be certified based on demonstrated behavior to be fully deterministic (e.g., nuclear surety). The plan should require an assessment of the dependencies of the system and its components on specialized real-time computer processing, wherein virtualization may pose a performance or power consumption concern. Industry is advancing the usage of virtualization for real-time data-processing-intensive applications such as vehicles.

---

[5] NIST Special Publication 800-125, https://www.govinfo.gov/content/pkg/GOVPUB-C13-ad063940b2ba8fcf2e891bc658e6ef3e/pdf/GOVPUB-C13-ad063940b2ba8fcf2e891bc658e6ef3e.pdf

Many commercially available central processing units (CPUs) now natively support virtualization, but the suitability of virtualization for specialized mission-critical, real-time-processing applications must be a careful consideration in the implementation plan. Of note, timing issues wherein the correct sequence of events get out of order have been encountered in commercial CPU virtualization that have proven challenging – or in some cases, impossible – to resolve.

DOD Instruction 5000.82 *Acquisition of Information Technology* includes requirements for DOD's Information Enterprise Architecture and cloud computing. The plan to use commercial virtualization technology in weapon systems and for deployed forces should ensure that the use of common COTS computer hardware, to include cloud computing, be optimized for virtualization.

DOD Instruction 5000.90 *Cybersecurity for Acquisition Decision Authorities and Program Managers* includes requirements relating to cybersecurity. The plan to use commercial virtualization technology in weapon systems and for deployed forces should ensure that these cybersecurity requirements are met.

The plan to use commercial virtualization technology in weapon systems and for deployed forces must emphasize the need to follow a Modular Open Systems Approach (MOSA), in accordance with Title 10 United States Code, Section 805, 2446a.(b). MOSA employs a modular design that uses major system interfaces between a major system platform and a major system component, between major system components, or between major system platforms. MOSA is subjected to verification to ensure major system interfaces comply with standards, and uses a system architecture that allows severable components at the appropriate level to be incrementally added, removed, or replaced throughout the life cycle of the platform to afford opportunities for enhanced competition and innovation.

Lastly, the plan to use commercial virtualization technology in weapon systems and for deployed forces commits to developing T&E tools and processes required to adequately evaluate the operational performance of systems applying such technologies.