# FY 2018 Annual Report

The freedom and security of our nation depends on the lethality and readiness of our military. Our warfighters must be prepared for combat, equipped with secure, credible weapon systems, and trained to employ those systems effectively and decisively. As the Director of Operational Test and Evaluation (DOT&E), I ensure that our weapon systems are systematically tested across a range of operational conditions that warfighters are likely to encounter in combat. Establishing combat credibility through realistic testing gives warfighters the confidence their weapons and equipment will work when they need them. I have been in this position for just over one year and, during this time, have informed 92 acquisition and 25 fielding decisions for the Department. When I was appointed to this position, I committed to increasing collaboration between DOT&E and other agencies within the defense community. Looking back, I have been most impressed with the "spirit of cooperation" between OSD and the military Services. With an attitude of teamwork, we are working towards the ability to field combat credible systems at the speed of relevance.

During the past year, my office collaborated with other OSD offices and the test and evaluation (T&E) community to increase combined approaches to testing programs. We worked with the OSD Director of Developmental T&E (DT&E) and the Services' Operational Test Agencies (OTAs) to develop streamlined guidance for Test and Evaluation Master Plans (TEMPs). We are constructing a risk assessment policy to determine the level of oversight that DOT&E will exercise for middle-tier and traditional acquisition programs. I reviewed the existing DOT&E oversight list and retained oversight of those capabilities that are most critical to our current and future national security needs. My goal in each case was to facilitate more rapid development and deployment of weapon systems without sacrificing the integrity or independence of the T&E community. Following this review, I established policy to clarify criteria to both place and remove a program on the oversight list.

Building on the work of the past year, my initiatives for this next year center on several key focus areas. Software-intensive systems and their cybersecurity implications remain a high priority. Collaborating with DT&E to conduct operational T&E (OT&E) earlier in the system development and acquisition process, adapting T&E for emergent technologies, improving our testing environments, and enhancing the workforce required to support T&E are other key focus areas.

## SOFTWARE-INTENSIVE SYSTEMS AND CYBERSECURITY

Most of the capabilities of current weapon systems are defined by software. This trend will continue as more complex and capable software platforms and algorithms make their way into the battlespace. However, as more software is incorporated into weapon systems, their vulnerability to cyber-attacks increases. Also, the cyber-attack surface of our systems increases as they become more interconnected and interdependent. Therefore, it is important to evaluate both the performance and cybersecurity of software-intensive capabilities within systems of systems as these drive operational effectiveness, suitability, and survivability.

### Effectiveness and Suitability

Software-intensive systems cannot rely solely on manual, platform-focused testing to evaluate performance. T&E strategies need to integrate accredited modeling and simulation (M&S) and automated testing of software wherever possible to achieve continuous evaluation of software code and system capabilities. M&S of systems allows greater platform testing across a variety of operational and threat scenarios. Also, accredited automated testing and M&S can overcome some of the limitations of manual testing by evaluating systems across multiple operational contexts faster than real-time processes.

Repeatable automated testing will reduce man-hours required for testing system changes and enable delivery of software at the speed of relevance. It will enable evaluating the effect system changes or failures have on the safety and capabilities of the warfighter. Repeatable automated testing will improve system sustainability and cost through early detection and resolution of deficiencies. To facilitate these improved software development considerations, the DOD should implement an iterative, incremental approach to acquisition and T&E, such as Development Security Operations (DevSecOps). During DevSecOps, stakeholders (i.e., system developers, acquirers, developmental and operational testers, cybersecurity experts, and warfighters) collaborate across the entire system lifecycle, from development and test to operations and sustainment.

### Cybersecurity Survivability

Any data exchange with a software-intensive system opens avenues for cyber-attacks that could adversely affect the confidentiality, integrity, or availability of the data. Cyber is a challenging man-made domain that requires seamless integration of technology with the cyber warrior to identify and defeat cyber adversaries. My office continues to emphasize the need to test all systems having

data exchanges for the resilience to complete missions in a cyber-contested environment. Also, I will continue to help improve the cybersecurity of mission-critical networks and systems through our Congressionally mandated Cybersecurity Assessment Program.

It is important that programs continue to conduct Cooperative Vulnerability and Penetration Assessments and Adversarial Assessments to fully characterize the cybersecurity of weapon systems. To aid this effort, I am advocating for improved training for cyber warriors and the development and use of automated tools for cybersecurity T&E. These tools should include the ability to examine deployed network and system configurations and identify flaws in software code. My office will continue to explore and advocate for cyber vulnerability assessment technologies that expand cybersecurity test scope while reducing test time. Concurrently, we will advocate for personnel with the skills needed to apply these tools effectively.

**Human-System Interaction (HSI)**

As systems become increasingly software intensive, the warfighter continues to be the most critical component in accomplishing the mission. We depend on our warfighters to be adaptable and find ways to accomplish the mission even when the systems we field have deficiencies. However, weapon systems that are difficult to use or that increase operator workload could reduce mission effectiveness or cause physical harm. As recently as 2017, the Navy's Fleet Forces Command cited poor HSI as a key factor in two U.S. Navy ship accidents, including the loss of 17 sailors.

I plan to update existing DOT&E guidance to encourage credible, systematic evaluations of HSI, consistent with Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) Section 227, Human Factors Modeling and Simulation Activities. I will encourage programs to incorporate warfighter feedback into the full system lifecycle from development and testing to operations and sustainment. I will align operational test of HSI with modern industry and scientific standards.

---

## CONDUCT OT&E EARLIER IN SYSTEM DEVELOPMENT

To deploy combat credible systems at the speed of relevance, I recommend a DevSecOps approach for software and the host hardware systems. This approach enables the OT&E community to engage with program managers early in system development to construct testable, operationally relevant requirements. I am encouraging the T&E community to adopt a combined testing approach in order to collect operationally relevant test data as early as possible during system development for both traditional and Middle Tier Acquisition (MTA) programs. Combined testing encourages developmental and operational testers to collaboratively plan and execute test events whenever possible to support their independent T&E goals and use resources efficiently. By performing operationally representative T&E early and often in the acquisition process, developers will identify performance shortfalls and cyber vulnerabilities when they are significantly cheaper and easier to fix.

Implementing a DevSecOps approach and combined T&E will be key to achieving the goals of the MTA approaches defined in FY16 NDAA Section 804. The overall goal of MTA is to expedite the development and fielding of capabilities to the warfighter. A combined test approach that incorporates the use of M&S is necessary to demonstrate and evaluate the performance of systems that pursue the MTA pathways. The operational demonstrations (OpsDemos) required by the NDAA provide programs the opportunity to establish combat credibility while keeping pace with rapid acquisition timelines. The size and scope of the OpsDemos should vary based upon the acceptable risk of the system to the mission and to the warfighter. The goal should continue to be delivering new capabilities rapidly without sacrificing performance of those capabilities that are most critical to the warfighters.

My office is working with the military Services to establish policy on OpsDemos that is tailorable to the speed and risk of the program. We have also initiated efforts to identify methods to tailor live fire test and evaluation (LFT&E) survivability and lethality assessment methods in support of MTA programs. The level of test for OpsDemos and LFT&E will vary in complexity and speed; from analysis of existing data primarily from prior test events, to an evaluation of a demonstration event, to a dedicated operational or live fire test. The level of test will be tailored to the program based on a risk analysis conducted by the lead OTA. I encourage all programs, middle tier and traditional, to use warfighter risk in determining the appropriate level of test.

---

## ADAPTING T&E FOR EMERGENT TECHNOLOGIES

As we conduct OT&E earlier in system development, the accelerating pace of emergent technologies will challenge T&E in new ways. The DOD has placed a renewed emphasis on advancing the capabilities of weapon systems using a range of new technologies, including hypersonic capabilities, directed energy, autonomy and artificial intelligence, and quantum systems. The T&E community must be prepared to evaluate these new systems and characterize their operational performance across a range of potential concepts of operations. This will require improvements in T&E infrastructure, novel T&E methods, and new skills in our T&E workforce.

As these technologies are incorporated into weapon systems, I will provide guidance on how to evaluate their unique capabilities during operational testing. While new technologies may present challenges, T&E of some have been ongoing. For example, the

Department has developed, tested, and fielded systems incorporating autonomous functions for several decades. In accordance with DOD Directive 3000.09, *Autonomy in Weapon Systems*, DOT&E is developing OT&E standards for autonomy in weapon systems. As military Services develop operational employment concepts for these emerging technologies, DOT&E will provide guidance on considerations for adequate OT&E.

## IMPROVING OUR TESTING ENVIRONMENTS

The closer our OT&E emulates the warfighters' combat environment, the better we can anticipate how the integrated warfighter system will perform. Creating operationally realistic conditions requires T&E infrastructure that can represent current and future capabilities. Often, existing T&E infrastructure provides limited replication of current threats or ineffective integration of currently fielded friendly capabilities. This problem is especially significant for threats to space systems. I witnessed this first-hand as I visited a number of our test ranges including the Pacific Missile Range Facility in Hawaii, Pacific Alaska Range Complex, White Sands Missile Range in New Mexico, Aberdeen Proving Ground in Maryland, and the Nevada Test and Training Range. These ranges were developed to test our systems against legacy threats, but are now inadequate to test against current and emerging threats.

Such shortfalls make it difficult to determine how systems will perform in the face of existing near-peer threats or in the context of integrated Joint Force or coalition operations. Fixing T&E infrastructure deficiencies and emulating a modern battlespace will require innovative approaches and a greater use of accredited M&S. My office continually works to improve the fidelity of OT&E and LFT&E M&S tools to enable virtual T&E of the effectiveness, suitability, lethality, and survivability of systems. Physical ranges and actual systems assure the evaluation of real-world effects during T&E, but can be limited in the variety of threats and capabilities or scale of operations. M&S mitigates some of these limitations, but must be continuously verified, validated, and accredited against real systems' and environmental performance data.

To overcome these challenges, programs must prioritize M&S validation early in development. Developers, acquirers, testers, and operators should fully understand the capabilities and limitations of any M&S. Early collaboration between all stakeholders and combined testing will support a more efficient and effective model-test-model process.

## WORKFORCE

In addition to adequate evaluation tools and methodology, credible T&E requires the right personnel to plan, execute, and analyze the tests. As OTAs maintain a skilled workforce through relevant training opportunities, knowledge is needed for systems that incorporate emerging technologies. We will continue to enhance workforce readiness and proficiency by developing and delivering training to the OTAs that focuses on current and future T&E needs.

Additionally, I am working to recruit and retain the most skilled personnel within the DOD for cybersecurity. I am looking to incorporate expertise from outside the DOD, including making use of our connections with the National Laboratories, University-Affiliated Research Centers, and Federally Funded Research and Development Centers. Expanding these partnerships can help us achieve the correct technical talent mix even in a highly competitive environment. I am committed to working with the OTAs to develop solutions to these challenges.

## CONCLUSION

Over the past year, I have been honored to be on the DOD team and support our warfighters. Through objectivity and independence, DOT&E will continue to evaluate the combat credibility of our weapon systems and equipment our men and women will use to accomplish the mission. As the authoritative source for DOD weapon systems' operational capabilities, I provide the unvarnished truth to DOD leaders and the Congress to ensure the taxpayers' investment in our nation's security is well spent. I look forward to continuing this important contribution to our national defense and stand ready to provide any additional information requested by members of the Congress or Congressional defense committees.

Robert F. Behler
Director