The Cybersecurity and Acquisition Life-Cycle Integration Tool

Steve Mills ■ *Tim Denman*

Cybersecurity is a critical component of the systems engineering process for Department of Defense (DoD) acquisition systems. Failure to integrate cybersecurity into our systems across the entire acquisition life cycle introduces exceptional risk to the system and the warfighter. Cybersecurity plays an extremely important role in the user requirements, design, development, operations, sustainment and disposal of DoD Systems. Cybersecurity has many unique attributes when viewed from the acquisition lifecycle perspective.

Cybersecurity is first and foremost system engineering—system security engineering (SSE), to be exact. Too often, cybersecurity is viewed as an afterthought in the acquisition process. Secondly, cybersecurity has a specific process to address cybersecurity risk called the Risk Management Framework (RMF) for DoD Information Technology (IT). The RMF approach is a separate and complementary process to traditional DoD Risk Management as outlined by the January 2017 *Risk, Issues and Opportunity Management Guide*.

Next, cybersecurity testing is executed via a six-phase mission-focused process across the acquisition life cycle. Finally, an ever-changing cyber threat must be integrated into the systems engineering process. The complexity of managing all of these processes drives the need for an interactive and highly informative tool that helps users understand, visualize and begin to integrate cybersecurity across the acquisition life cycle to achieve better acquisition outcomes.

A team at the Defense Acquisition University has developed such a tool—the Cybersecurity and Acquisition Lifecycle Integration Tool (CALIT). CALIT went "live" in June 2016 and has been downloaded more than 5,000 times by members of the Defense Acquisition Workforce. CALIT has been used extensively by members of the DAU Cybersecurity Enterprise Team to deliver numerous cybersecurity related workshops to Defense Acquisition Workforce members. CALIT has also been used in development of the Cybersecurity and Acquisition Integration Workshop. This 1- to 2-day

Mills *is a professor of Program Management and is the Cyber Lead at the South Region's campus of Defense Acquisition University in Huntsville, Alabama.* **Denman** *is the DAU Cybersecurity Functional Learning director.*

workshop is currently being offered across all DAU regions to both government and industry partners several times a year.

Simple Approach to a Complex Challenge

CALIT was designed with simplicity and familiarity in mind. The Defense Acquisition Workforce is very familiar with the DoD acquisition life-cycle chart, often referred to as the "wall chart" or the "horse blanket." A cursory walk around a program management office or program executive office may result in seeing several versions of the wall chart in employees' work spaces. CALIT adopts this same approach, but depicts the key cybersecurity-related processes as "swim lanes" and orients them across the acquisition life cycle.

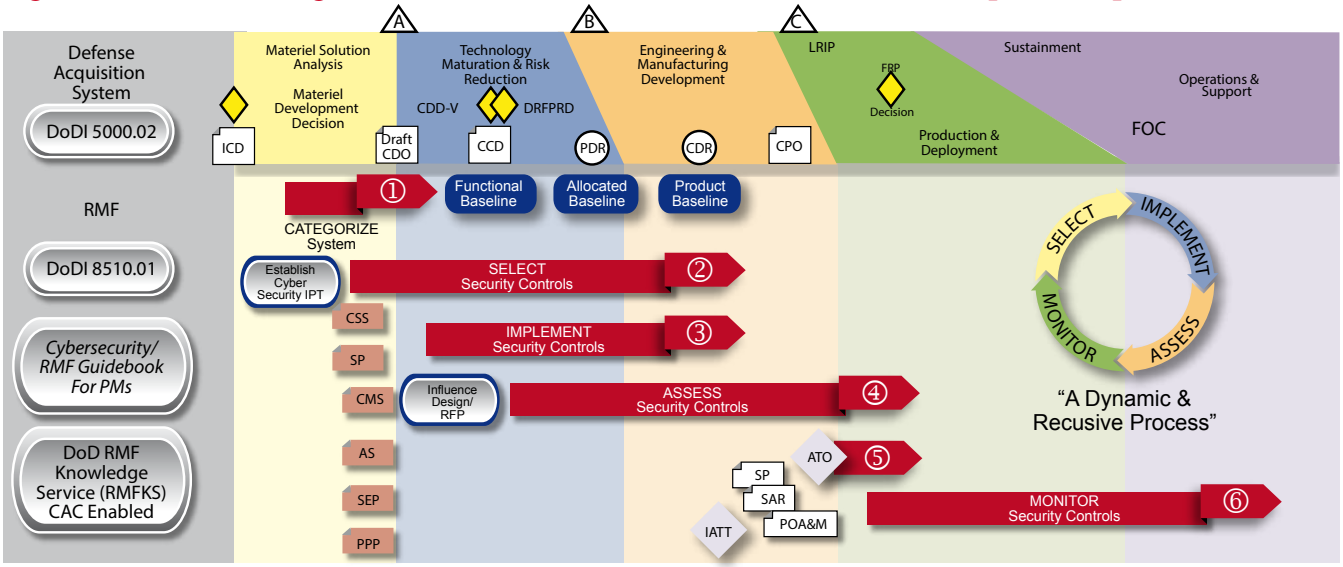
CALIT was developed on the premise that effective integration of cybersecurity into the DoD acquisition life cycle encompasses several different processes, including:

- DoD Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System

Key to Abbreviations in Figures 1-4

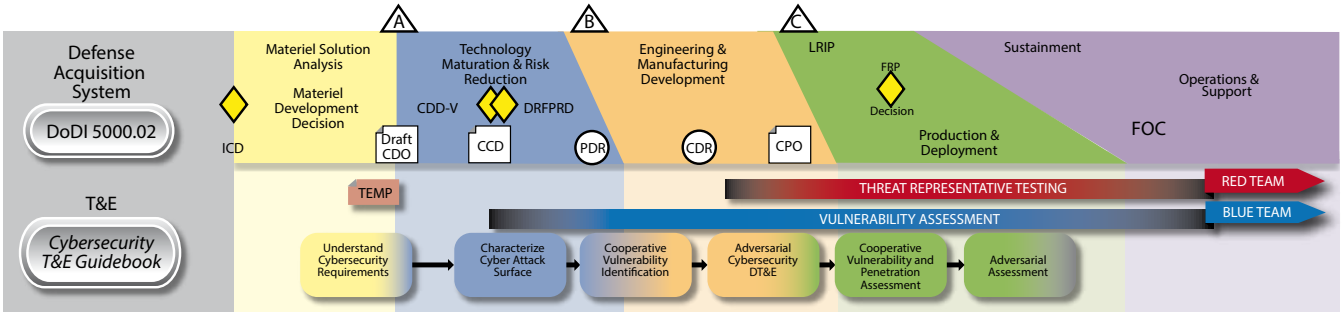
AS=access security; ATO=authority to operate; CAC=common access card; CDD=Capability Development Document; CDD-V=validation of CDD; CDR=critical design review; CMS=configuration management system; CPD=Capability Production Document; CPI=critical program information; CSS=contractor support services; DRFPRD=development request for proposal release decision; DT&L=developmental test and evaluation; EMD=engineering and manufacturing development; FOC=full operational capability; FRP=full-rate production; IATT=interim authority to test; ICD=Initial Capabilities Document; IPT=integrated product team; ITEA=Initial Threat Environment Assessment; LRIP=low-rate initial production; P&D=production and deployment; POA&M=plan of action and milestones: PDR=preliminary design review; PPP=program protection plan; sar=safety assessment report; SE=systems engineering; SEP=Systems Engineering Plan; SP=start point; SSE=system security engineering; STAR=System Threat Assessment Report; T&E=test and evaluation; TMRR=technology maturation and risk reduction; TSN=trusted systems and network; VOLT=validated online life-cycle threat.

Figure 1. Risk Management Framework Swim Lanes and Six-Step Life-Cycle Process



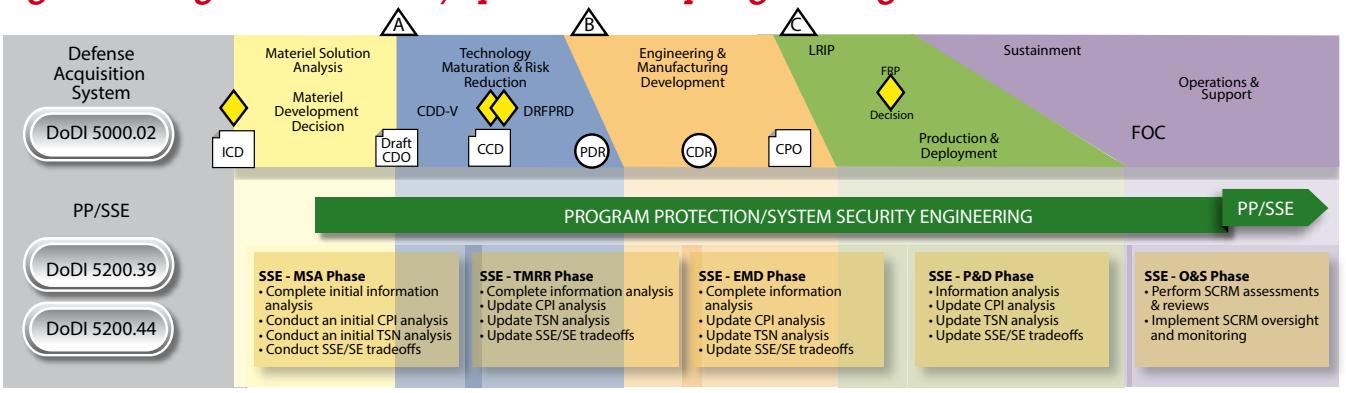
Source: CALIT Version 2.03, DAU (https://www.dau.mil/tools/t/Cybersecurity-and-Acquisition-Lifecycle-Integration-Tool-(CALIT)

Figure 2. Cybersecurity Test and Evaluation Swim Lane



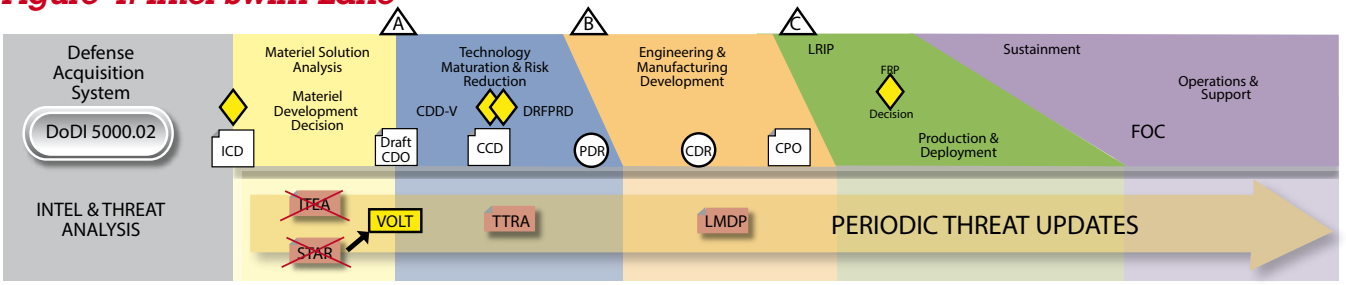
Source: CALIT Version 2.03 (https://www.dau.mil/tools/t/Cybersecurity-and-Acquisition-Lifecycle-Integration-Tool-(CALIT)

Figure 3. Program Protection/System Security Engineering Swim Lane



Source: CALIT Ver 2.03 (https://www.dau.mil/tools/t/Cybersecurity-and-Acquisition-Lifecycle-Integration-Tool-(CALIT)

Figure 4. Intel Swim Lane



Source: CALIT Ver 2.03 (https://www.dau.mil/tools/t/oDisecurity-and-Acquisition-Lifecycle-Integration-Tool-(CALIT)

- DoDI 8510.01—RMF for DoD Information Technology (IT)
- Cybersecurity Test and Evaluation
- Program Protection/SSE
- Cyber Threat Analysis
- DoDI 5200.39, Critical Program Information Identification and Protection Within Research, Development, Test and Evaluation
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

The CALIT provides the user insight into these supporting processes and the ability to visualize how these processes work together to promote cyber-resilient weapon systems. Figure 1 depicts the four individual "Swim Lanes" oriented under the Hardware Intensive acquisition model.

The RMF swim lane in Figure 1 show the RMF six-step process across the life cycle.

A central role of the DoD RMF for DoD IT is to provide a structured but dynamic and recursive process for near real-time cybersecurity risk management. For example, the assessment of risks drives risk response and will influence security control selection and implementation activities, while highlighting a need to reconsider information and communication needs or the entity's continuous monitoring activities. RMF is not a strictly linear process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and will influence another.

The Cybersecurity Test and Evaluation (T&E) swim lane (Figure 2) depicts this unique six-phase process across the acquisition life cycle.

Compliance with traditional cybersecurity policy has proven insufficient to ensure that systemic vulnerabilities are addressed in fielded systems used on the battlefield. A broader cybersecurity T&E approach that focuses on military mission objectives and their critical supporting systems is needed to fully address the cyber threat. Cybersecurity is an integral part of developmental and operational T&E. Cybersecurity T&E planning, analysis and implementation constitute an iterative process that starts at the beginning of the acquisition life cycle and continues through maintenance of the system. Cybersecurity T&E is performed in conjunction with the RMF as defined in DoDI 8510.01, RMF for DoD IT. The use of both Blue Teams and Red Teams as part of a robust cybersecurity T&E effort is a key component of an effective cybersecurity effort.

The Program Protection (PP) and SSE swim lane in Figure 3 depicts the key engineering related processes across the acquisition life cycle.

Program protection is the integrating process for managing security risks to DoD warfighting capability from:

- Foreign intelligence collection
- Hardware exploitation
- Software vulnerabilities
- Cybersecurity vulnerability (Yes, cybersecurity is a subset of Program Protection!)
- Supply chain exploitation
- Battlefield loss throughout the system life cycle

Figure 4 addresses the intelligence threat swim lane.

SSE is the discipline that implements program protection. SSE is a specialty discipline of systems engineering with several components:

- Cybersecurity (That's right, cybersecurity is a form of Systems Engineering too!)
- Hardware Assurance
- Software Assurance
- Anti-tamper
- Supply Chain Risk Management
- Defense Exportability
- Security Specialties (Personnel Security, Physical Security, Information Security, etc.)

A cursory review of the PP/SSE swim lane reveals the two primary PP/SSE-related activities occurring across the acquisition life cycle. The activities are the Criticality Analysis and the Trusted System and Networks Analysis. Both of these analyses are key components of the overall cybersecurity effort.

A discussion about cybersecurity on DoD acquisition programs would not be complete without addressing the impact(s) of the cyber threat on the system.

The primary document that provides the program specific threat assessment is the System Threat Assessment Report (STAR), which provides a holistic assessment of enemy capabilities to neutralize or degrade a specific U.S. system by addressing both threat-to-platform and threat-to-mission.

The STAR is intended to serve as the authoritative threat document supporting the acquisition decision process and the system development process. The STAR can also be used to guide test planning. Due to the static nature of the STAR, a more "real time" threat assessment is needed. To address this shortcoming, the Validated Online Lifecycle Threat (VOLT) tool will supersede the STAR. Transition to the VOLT Tool is mandated in Better Buying Power 3.0 Implementation Guidance. As of the time of this article, the VOLT tool has not been fully implemented.

Conclusion

The Defense Acquisition Workforce requires real time visualization tools that help them understand and apply key DoD related policies and processes more easily. CALIT is a new, interactive capability that focuses on the cybersecurity component for DoD acquisition programs. The CALIT can be found at https://www.dau.mil/tools/t/Cybersecurity-and-Acquisition-Lifecycle-Integration-Tool-(CALIT). Another key tool just released is the Interactive Defense Acquisition Life Cycle Chart which can be found at https://www.dau.mil/tools/t/ILC. Better understanding of the key cybersecurity processes and how they integrate across the acquisition life cycle is critical to engineering cyber resilient systems that must operate effectively in a cyber-contested environment.

DAU will continue to deliver quality interactive tools to help the Defense Acquisition Workforce achieve better acquisition outcomes.

The authors can be contacted at **steve.mills@dau.mil** *and* **tim.denman@dau.mil**.

MDAP/MAIS Program Manager Changes

With the assistance of the Office of the Secretary of Defense, *Defense AT&L* magazine publishes the names of incoming and outgoing program managers for major defense acquisition programs (MDAPs) and major automated information system (MAIS) programs. This announcement lists all such changes of leadership, for both civilian and military program managers for May-June 2017.

Army

Col. Roger D. Kuykendall assumed responsibilities of program manager for Improved Turbine Engine and Future Vertical Lift Programs on May 30.

Col. Gregory S. Fortier relieved **COL William D. Jackson** as project manager for Cargo Helicopter on June 29.

Col. Robert J. Mikesh relieved **COL Harry R. Culclasure** as project manager for Army Enterprise Systems Integration Program on June 29.

Navy/Marine Corps

CAPT Matthew Commerford relieved **CAPT Albert Mousseau** as program manager for the Direct and Time Sensitive Strike Program (PMA-242) on June 29.

CAPT John Keegan relieved **CAPT Michael Ladner** as program manager for the Surface Ships Weapons Program (IWS 3.0) on June 2.

Air Force

Col Daniel N. Marticello relieved **Col Amy J. McCain** as program manager for the Presidential Aircraft Recapitalization Program on May 22.