Modernizing Air Force Cybersecurity Test and Evaluation

Walter Rhoads

The Challenge: The current U.S. Air Force workforce cannot support its current cybersecurity test and evaluation requirements. Yet those requirements are expected to increase as the demand for cybersecurity test and evaluation continues to grow.

The USAF should first seek to augment its workforce capability to support cybersecurity evaluations of systems either in or entering production.

The United States Air Force (USAF) 46th Test Squadron (46 TS) asked IDA to structure a roadmap for workforce, infrastructure, and process cybersecurity test and evaluation (CSTE) modernization efforts. The effort provided a time-phased, cybersecurity test investment roadmap based on priority, cost, and technology maturity levels to support future airborne platform; weapons; and command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR) cyber acquisition programs.

To assess the workforce requirements for CSTE modernization, IDA applied three methods using available data, empirical rules of thumb, and simple projections based on historical and planning data. The first method, which was the most rigorous, used a standard workforce planning model that assumed the data for each parameter in the formula was available, directly measured, and collected at the same time. The second method quantified expected demand and likely supply needs based on acquisition parameters and estimated life-cycle costs; this method relied on subject matter experts and planners who employed rules of thumb when developing concepts and rough order of magnitude cost estimates. The third method examined existing staffing levels, how the workforce was deployed and employed, and the 46th/DET's known portfolio of acquisitions and programs.

Each method was used to produce a demand forecast and supply forecast from which an assessment of workforce gaps was made. The detailed labor data for select individual events provided insight into the substantial number hours spent on travel, planning, and dry-run activities. For example, penetration activities for the Air Force Distributed Common Ground System (AF DCGS) comprised less than 20% of the 2,000 hours spent on this program; dry runs and reconnaissance accounted for 36%, and planning and travel accounted for 40%.

We found that the current USAF workforce has insufficient size and depth to support current or potential future CSTE requirements. The USAF CSTE workforce is currently structured to support Risk Management Framework (RMF) control

compliance evaluation for fielded systems and acquisition programs. These shortfalls are particularly acute for CSTE intended to support production and fielding decisions.

IDA recommends that the USAF pursue a spiral improvement program to augment, broaden, and deepen its CSTE workforce. These improvements should be phased to accomplish near-, mid-, and far-term objectives.

The USAF should first seek to augment its workforce capability to support cybersecurity evaluations of systems either in or entering production. This first step would involve (1) ensuring that the USAF CSTE workforce has professional certifications in all relevant disciplines and has all necessary clearances; (2) expanding the existing National Security Agency (NSA)-certified threat portrayal team capabilities; and (3) integrating system subject matter experts in Aircraft and Weapons (A&W) and C4ISR systems, including industrial control systems.

To develop an augmented, robust threat portrayal capability in a low-cost, expedited manner, IDA recommends that the USAF develop teaming arrangements among the Threat System Management Office (TSMO), the 57 Information Aggressor Squadron (IAS), the 177 IAS, and the 46 TS. A teaming arrangement will substantially reduce the USAF costs because TSMO reports that establishing an NSA-certified threat portrayal team can take 4 to 5 years, cost $3 million, and involve annual maintenance costs of $2 million. Furthermore, they report that developing appropriately trained government leads may require at least 18 months.

To meet mid- and long-term objectives, IDA recommends that the USAF expand its civilian workforce with dedicated subject matter expertise in threats, weapon systems, and operational environments. Consistent with this recommendation, the USAF should establish a comprehensive workforce solution that is designed to build domain expertise through training, outreach, and direct experience.

We further recommend that the USAF develop a joint community of interest among the following organizations: 92 Information Operations Squadron (IOS), 57 IAS, 177 IAS, the Army Research Laboratory's Survivability and Lethality Analysis Directorate, and the Naval Systems Command Cyber Warfare Directorate.

Implicit in the foregoing recommendation is a need to retain a skilled workforce through development, training, and financial compensation incentives.

The 46 TS is now implementing IDA's recommendations.

Mr. Walter Rhoads in an Adjunct Research Staff member in IDA's Information Technology and Systems Division. He holds a Master of Science in systems analysis and management from the University of Southern California.