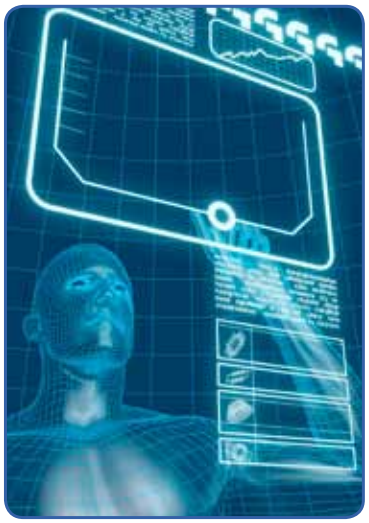
Addressing Cyber Security from the Sidelines

Many have heard of the various very scary stories "out there" regarding cyber incidents such as counterfeit electronics being embedded in DoD systems, hacks into both DoD and commercial systems, viruses, malware, etc. The list goes on, and there are unfortunately too many others to mention in this short article. But you may not have heard that Huntsville, Ala., is a major target for foreign intelligence efforts.

To help address this and the nation's cyber threat, a couple of efforts are ongoing in Huntsville. First, there is an effort orchestrated by the mayor of Huntsville called "Cyber Huntsville." This is a team effort involving industry, government and academia leveraging the highly technical, talented workforce and capabilities in Huntsville, making it a "Cyber Center of Excellence" for the nation.



The second effort involves the U.S. Space and Missile Defense Command (SMDC), which has been designated as a pilot program under the ASA/ALT to help determine what needs to be written into DoD acquisition policy and guidance to address the issue with cyber security and the global supply chain. This effort is called Supply Chain Risk Management.

Many people automatically think logistics when discussing supply chain concerns, but in reality cyber-related vulnerabilities are built into products we use in the development of DoD systems through the supply chain. For instance, you may know who the prime contractor is on a DoD contract, but you may not know the third- or fourth-tier vender, who actually provides the software or hardware for the system under development. SMDC is working with local Redstone organizations like the Threat Systems Management Office to help understand what some of the threats are in the supply chain and what can be done about them.

What about DoD policy? Such a policy is forthcoming on how to deal with the ever-evolving cyber threat. The Army is also trying to determine how best to address cyber security in test and acquisition policy. Until a new policy is developed, DAU can assist organizations through curriculum based on current policy and guidance geared toward developing secure systems. For example, information assurance and software assurance are both tools that can be used to help build secure systems. Both, based in current policy, are offered by DAU in the classroom as well as online continuous learning modules.

Program offices balancing cost, schedule, technical performance, and risk during system development may make trades to get their system approved by the Designated Approval Authority for operation. To help get a system fielded on time, these trades may circumvent some of the current policy and guidance, and program managers and program office personnel must be more aware of the vulnerabilities they may introduce into a developing system by doing so.

Addressing the cyber threat really involves thinking critically about a problem and how to implement a solution to that problem. For a well-thought-out problem, some risks may be mitigated in DoD acquisition by having a constantly updated threat assessment throughout the program. These threats can be addressed by using and properly applying existing tools from program management and systems engineering to contracting processes. As Col. Tom Freeman of the National Security Agency said, "Cyber is a team sport." It cannot be done by a single subject matter expert or a single agency and requires team work by all stakeholders in a well-coordinated, mission-focused effort.

SSCF at Aberdeen Proving Ground Holds Commencement Ceremony for Second Graduating Class

Seven graduating fellows crossed the stage at the Mission Training Facility, C4ISR Campus, APG, on May 18 to receive their Senior Service College Fellowship Program diplomas, marking completion of 10 months of intense and demanding leadership and acquisition study. This commencement ceremony celebrated the graduation of the second class of fellows from the CNE region. The ceremony was attended by more than 70 people, with numerous distinguished guests, including nine members of the Senior Executive Service, friends, and family members. Participating were guest speaker Rear Adm. Lenn Vincent, U.S. Navy, retired, DAU Industry chair; Bob Daugherty, Dean, Capital and Northeast Region, DAU; and Barbara Downs, Webster coordinator for DAU programs. During his keynote address, Adm. Vincent explained to the fellows his "baker's dozen of leadership thoughts." He reminded the fellows that "doing your job is not enough. It's not just working hard, but finding how you can work better." Graduates included Steve Cooper, Raymond Fontaine, Stephanie Halcisak, Raj Malhotra, Daniel Shearer, Dennis Teefy, and Randy Young. Notably, three of the seven fellows—Mr. Cooper, Mr. Teefy, and Mr. Young—also completed an additional five courses necessary to earn a master of arts degree in management and leadership from Webster University. After completing the SSCF Program, the fellows are returning to more challenging positions in their sponsoring organizations or have accepted positions of greater responsibility in new units.