Acquisition Update: New Coast Guard Cybersecurity Initiative Strengthens C4ISR Program

Feb. 26, 2015

The Coast Guard is implementing a new information assurance process that will strengthen cybersecurity for the command, control, communications, computers, intelligence, surveillance and reconnaissance equipment on the service's newest cutters.

The Coast Guard's C4ISR program is developing secure and reliable computer systems for the national security cutter and the offshore patrol cutter in a project with the C4&IT Directorate (CG-6).

The Coast Guard is using the Risk Management Framework, the Department of Defense's updated approach to protecting computer networks. "The threats to systems and data come from malware infecting a system; theft or loss of computers and storage disks; unauthorized access by internal users and outside cyber attacks," said Cmdr. Warren Judge, C4ISR technical director and core technologies manager.

The C4ISR program is working with the Command, Control, Communications, Computers and Information Technology Directorate (CG-6) to develop secure and reliable computer systems for the national security cutter and the offshore patrol cutter using RMF.

Judge believes that RMF will help the C4ISR program team address the expanding and evolving threats to Coast Guard systems. "The increased cyber and insider threat requires the ability to monitor, track, search for and respond to attacks by adversaries within the environment," Judge said. RMF is a comprehensive development process that is also very flexible and can protect against a variety of risks. It is effective because it addresses cybersecurity as an integral part of the acquisition process, rather than as an additional component that is addressed after a cutter is built. Designing cutter systems with integrated risk management produces more effective system control and reduces costs.

RMF also includes an "enterprise" approach to security that recognizes the interrelationships between different systems. Rather than viewing a cutter as an isolated platform, the Coast Guard recognizes that the cutter is in communication with satellites, intelligence networks and other systems. Any security vulnerability on the cutter can be a vulnerability for other systems the cutter interacts with, and vice versa. The RMF approach asks acquisition teams to place the cutter within the larger Coast Guard and government enterprise and to enact cybersecurity controls to protect information flowing between the cutter and other systems.

In 2014, the DOD began requiring its programs and contractors to meet RMF standards. The new protocol provides common IT language and certification processes and will lead to more compatible system designs across multiple agencies. When combined with an enterprise design approach, more compatible systems will improve the Coast Guard's ability to operate with its government partners.