USASMDC/ARSTRAT

Technology Center

SCRM

Supply Chain Risk Management

Summary

- Conduct logical assessment of products, software, assemblies, and components to include: testing article attributes, code inspection and reverse-engineering.
- Perform inspection of test articles, to include, visual inspection, destructive testing, functionality testing against design and manufacturer's specs.
- Provide standards for assessing or investigating evidence of remarking, re-use, prototyping and spares and reject disposal, stockpiling, supplier/ broker/vendor screening, and other counterfeiting or deception mitigations.
- Develop SCRM T&E related best practices, policies and procedures, and training.

Supply Chain Risk Management (SCRM) is the systematic process of identifying vulnerabilities and threats throughout our "supply chain" and developing mitigation strategies to combat those threats.

The U.S. Army Space and Missile Defense Command/Army Forces Strategic Command was selected by the Assistant Secretary of the Army, Acquisition, Logistics, Technology, (ASA (ALT)) Defense Industrial Base Cyber Security Office as the Army's SCRM Test and Evaluation (T&E) cell. The SCRM pilot program provides an opportunity for the Department of Defense to learn what practices work effectively; what gaps exist in policy; how the current or proposed practices for discovering, and managing risk perform; and anticipated cost, schedule and performance impacts. An integral component of SCRM risk mitigation is T&E which includes screening, verification & validation (V&V), and traditional test and evaluation practices.

SCRM

Supply Chain Risk Management

Technology Center

The DoD Comprehensive National Cybersecurity Initiative Supply Chain Risk Management (SCRM) piloting approach is to execute information and communications technology supplier risk management on multiple pilot projects. The goal is to develop knowledge and experience from an acquisition perspective to understand, identify, mitigate, and govern risks presented by suppliers of information and communication technology.

This improved situational awareness of the supply chain will enable acquisition managers to implement key practices as well as other appropriate mitigations. In executing the SCRM Threat Assessment Process, the pilot will: develop supplier lists for evaluation; review threat assessment reports received from the Threat Assessment Center (TAC) for timeliness, understandability and usefulness; develop and evaluate proposed mitigations and their impacts; and implement appropriate mitigations on the project (or provide feedback as to why it cannot be performed).

The pilot project will also provide lessons learned and other feedback to the assistant secretary of defense for Network and Information Integration SCRM Program Management Office, via the SCRM subject matter experts assigned to work with the pilot project.

Participation in this effort will provide USASMDC/ARSTRAT the opportunity to support in and influence a critical national security initiative. Equally important, it will assist the command in identifying and understanding potential SCRM risks to its own acquisitions and those it supports, positioning it to mitigate the risks early in the development process. USASMDC/ARSTRAT will also be able to capitalize on SCRM synergy and commonality enabling the command to conduct SCRM piloting activities using an amount of effort and resources that would be prohibitive if the command were to take on the effort by itself.

The initial DoD SCRM pilot activity validated a requirement for a test and evaluation capability to verify hardware and software in support of the overall SCRM effort. USASMDC/ARSTRAT, as the Army's SCRM T&E cell, will be responsible for managing SCRM-related technology capabilities research, testing, and evaluation activities.

An overall T&E repeatable approach will be used during the pilot program. The selected Army pilot programs are in different phases of S&T or acquisition, and not all T&E tools and processes may apply. Applying the same overall approach will be beneficial for comparison purposes. The planned pilots will examine a system that is presently deployed and used in combat today; a system that is in procurement in the Army; and current defense industry supply chain management best practices.

The SCRM challenge is clearly beyond the ability of any one organization to fully address alone. No single entity is capable of identifying and mitigating all possible SCRM-related threats and vulnerabilities. For this reason, the development of partnerships with the greater DoD SCRM community, DoD/Army test facilities and laboratories, system integrators and consultants, industry, and academia will be critical to enabling the successful implementation of the Army SCRM Center of Excellence T&E cell.

The combination of piloting with component/organization CoEs and pilot projects will provide the experience that will, at the conclusion of the pilot period, form the recommendations to the interagency policy process for institutionalizing a robust SCRM capability.

For more information, please contact:
USASMDC/ARSTRAT Public Affairs Office
P.O. Box 1500
Huntsville, AL 35807
Phone: 256-955-3887
Fax: 256-955-1214
Email: webmaster@smdc.army.mil
www.facebook.com/armysmdc
www.twitter.com/armysmdc
www.flickr.com/armysmdc
www.youtube.com/armysmdc

Distribution A 0810/0173