CrossTalk would like to thank DHS for sponsoring this issue.

Each person and organization in the supply chain path "touches," or has influence on, the security and resilience of software used to control products, systems, and services.

Just as with food and pharmaceuticals, software can be corrupted in ways that put users, organizations, and missions at risk. Software can become tainted by malware, exploitable weaknesses, and vulnerabilities. But no matter the method of compromise, those at the end of the supply chain are unwittingly exposed to the residual risk.

Information and communications technology supply chains are interdependent global ecosystems that consist of organizations, people, activities, information, and resources. And these complex ecosystems are vulnerable to a host of threats and hazards such as natural disasters, accidents, and malicious attack. Globalization of the commercial information and communications technology marketplace provides increased opportunity for anyone intent on harming the United States to gain unauthorized access to systems, data, and communications. Securing the global supply chain is integral to securing both our national security and the world economy.

The government and private sector own separate parts of the supply chain risk equation. This means that no single organization independently controls all the processes or possesses all the information required to manage the full risk. Public/private collaboration is crucial to supply chain risk management.

Our Supply Chain Risk Management (SCRM) program promotes the improvement of formal threat sharing processes, planning and investment documentation, supply chain incident reporting, national security systems standards, and the Federal cybersecurity workforce.

In concert with the DoD and NIST, the DHS Software Assurance program co-sponsors a forum during which our Federal, academic, and private sector partners discuss Software Assurance (SwA) risks and mitigation methods. This Software Assurance Forum has contributed several excellent resources to the software supply chain risk management community. These resources are available on the SwA Community Resources and Information Clearinghouse at <https://buildsecurityin.us-cert.gov/swa>.

Venues such as the SwA Forum are critical to our understanding of how suppliers incorporate security-aware practices into the production of software. Baseline understanding can inform risk-based decisions when purchasing software or contracting for software-reliant systems or services.

This issue of **CrossTalk** includes articles focused on advancing SCRM that we hope will provide valuable insights into SCRM techniques, research methods, and models that target vulnerabilities in the supply chain. Thank you for taking advantage of this excellent resource.

Roberta Stempfley
Acting Assistant Secretary
Office of Cybersecurity and Communications
Department of Homeland Security