CrossTalk would like to thank DHS for sponsoring this issue.

Our information and communications technology (ICT) assets are under constant attack. Thwarting the active attacker is not something most designers, engineers, developers, or project managers normally consider or have been trained to address. Yet encouraging resilience as a criteria in every stage of development and supply of ICT must continue to be the forward-leaning focus of the Software and Supply Chain Assurance efforts within government and industry. Attacks against our supply chains unite acquirers and suppliers in the search of scalable means for sharing information about ICT risks that arise through malice or negligence. Suppliers and acquirers need standardized means for conveying information about common issues related to both the hardware and software aspects of ICT, especially regarding non-conforming products that contain counterfeit, tainted, or defective components that can cause subsequent harm.

How can we collaboratively orchestrate industry and government response to these attacks? One way is through the Common Vulnerabilities and Exposures (CVE) List, which is an extensive listing of publicly known vulnerabilities found after ICT components have been deployed. Sponsored by the Department of Homeland Security (DHS), the ubiquitous adoption of CVE has enabled the public and private sectors to communicate domestically and internationally in a consistent manner the vulnerabilities in commercial and open source software. CVE has enabled our operations groups to prioritize, patch, and remediate nearly 60,000 openly reported vulnerabilities.

Unfortunately, vulnerabilities are proliferating rapidly thus stretching our capabilities and resources. As we seek to discover and mitigate the root causes of these vulnerabilities, sharing the knowledge we have of them helps to mitigate their impact. In order to keep pace with the threat, we must facilitate the automated exchange of information. To achieve that, DHS sponsors “free for use” standards, such as:

- **Common Weakness Enumeration (CWE),** which provides for the discussion and mitigation of architectural, design, and coding flaws introduced during development and prior to use;
- **Common Attack Pattern Enumeration and Classification (CAPEC),** which enables developers and defenders to discern the attacks and build software resistant to them;
- **Malware Attribute Enumeration and Characterization (MAEC),** which encodes and communicates high-fidelity information about malware based upon behaviors, artifacts, and attack patterns;
- **Structured Threat Information eXpression (STIX),** which conveys the full range of potential cyber threat information using the Trusted Automated eXchange of Indicator Information (TAXII) to define the technical mechanisms for exchanging actionable cyber threat indicators.

These open specifications for interoperable security automation enable secure, machine-to-machine communication of actionable indicators between organizations that want to share this information. The components have been developed collaboratively between Federal Government and industry partners working toward information sharing mechanisms and solutions to reduce the risk of counterfeit and tainted ICT components. These standardized means for sharing information are already being used, and they contribute to our efforts to enable all stakeholders to secure their part of cyberspace.

Though not an exhaustive list, the articles in this issue of CrossTalk demonstrate the breadth of anti-counterfeiting and supply chain risk management efforts taking place as well as the depth of the need to share data and lessons learned. We hope you find this issue to be a useful resource to address the very real challenges we face in software assurance, supply chain risk management, and operations.

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