CrossTalk would like to thank DHS for sponsoring this issue.

When organizations purchase software or software-reliant capabilities and services with inadequate consideration for built-in cybersecurity and software assurance, the residual risks of exploitability persist throughout the life of the purchased capability. The lasting effect of inadequate software assurance in procured items is part of what makes acquisition reform so important to achieving mission resiliency, and could provide a more enabling role for achieving more comprehensive cybersecurity. Meanwhile, due to the growing sophistication and complexity of software that controls and enables Information and Communications Technology (ICT), military and federal agency information systems are increasingly at risk of compromise, and organizations need guidance to help manage software supply chain risks. Requirements specification, acquisition and procurement activities must incorporate software assurance criteria as part what constitutes "technically acceptable" and "fit-for-use" in higher assurance mission environments.

The Federal Acquisition Regulation (FAR) continues to change; focusing on the fact that supply chain introduces risks to essential information and services. What progress have we made, and what do we still need to do to better safeguard society and missions from supply chain risks? What should acquisition managers include, as part of their due-diligence, in considering potential suppliers of ICT/software products and services? In the 2014 report "Improving Cybersecurity and Resilience through Acquisition " <http://gsa.gov/portal/content/176547>, in response to Section 8(e) of the President's Executive Order 13636, GSA and DoD, in coordination with DHS, made recommendations regarding the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration; specifically recommending acquisition reforms. More explicit measures are now being advocated because our ICT/software 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 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/software risks that arise through malice or negligence. Suppliers and acquirers need standardized means for conveying information about common issues, especially regarding non-conforming products that might contain counterfeit, tainted, or defective components that can enable exploitation or cause subsequent harm.

Unfortunately, partially because of the lack of adequate due-diligence in acquisition, vulnerabilities are proliferating rapidly thus stretching our mission 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 the Common Weakness Enumeration (CWE), which provides standardized means for identifying and mitigating architectural, design, and coding flaws introduced during development and prior to use, and the Common Attack Pattern Enumeration and Classification (CAPEC), which enables developers and defenders to discern attacks, build software resistant to them, and determine the sufficiency of test regimes. 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 tainted ICT/software 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.

DHS, DoD, NIST, and GSA co-sponsor the Software & Supply Chain Assurance (SSCA) Forum in which Federal, academic, and industry stakeholders discuss risks and mitigation methods. SSCA Forums are free and open to the public -- see details at <http://gsa.gov/portal/content/194963>, and resources are available on the SSCA Community Resources and Information Clearinghouse (CRIC) at <https://buildsecurityin.us-cert.gov/swa>.

Venues such as the SSCA Forum are critical to our understanding of how suppliers incorporate security-aware practices into the production of software. An appreciation of how acquisition and procurement can exercise proper due-diligence 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 software assurance as part of acquisition of software-reliant capabilities that can provide valuable insights into techniques, practices, methods, and models that target and mitigate vulnerabilities in the supply chain.

Justin Hill
CrossTalk Publisher