Reinforcing Systems Assurance In Cyber Risk Management

Systems assurance is a matter of strategic concern to our nation's security; one the DHS takes very seriously. Fundamentally, it is the concerted effort to ensure that users have the highest level of confidence possible in their critical systems and data.

In other words, systems assurance is the integrated effort to enhance user confidence in the safety, security, reliability, availability, and maintainability of processes and products. A number of factors impact the user community's confidence, including standards setting, procedures development, regulations, and specific verification and certification criterion.

Industry and the government have been working hard and have made important progress in providing systems assurance for their customers. Collaborative efforts are advancing standards and practices for systems and software assurance.

However, building and sustaining customer confidence is difficult and in an ever-changing technological environment where such confidence is easily diminished. In fact, malicious actors have shown great adaptability in their efforts to undermine assurance efforts. This is why we must be constantly vigilant and strive to implement innovative systems assurance technologies.

It also must not be forgotten that enhanced systems assurance supports intellectual property rights protection, improved consumer trust, and more confident business operations and services. A broad spectrum of critical applications and infrastructure, from process control systems to commercial applications, depend on secure, resilient systems. That is why we must manage risks to these systems effectively and improve our capabilities and capacity to mitigate those risks.

Let me close with the observation that the most effective systems assurance efforts are "baked" into the risk management process from the very beginning of the system development life cycle. Security and resiliency must be integrated throughout the life cycle. If they are not, customers may unknowingly accept risks that could have profound financial, legal, and national security implications.

By working together—building on efforts already underway, and striving to take steps that will enhance and improve confidence in critical systems and data—we can make an impact that will better secure the nation.

I sincerely hope you enjoy this issue of CrossTalk and learn from the keen insights and recommendations contained herein.

Gregory Schaeffer
Assistant Secretary for Cybersecurity and Communications
U.S. Department of Homeland Security