CrossTalk would like to thank **DHS** for sponsoring this issue.

Cybersecurity is a risk management issue, not just a technology issue. Regrettably, for many years, cybersecurity risk decisions were delegated to low levels, ignored, or not even imagined by senior leaders as well as those who conceive, engineer, and sustain software-intensive systems. Delivering products often focused on the availability and functionality of a product rather than balancing those attributes with data integrity and confidentiality. Some producers accepted risk for those who used their products without incorporating cybersecurity best practices into product design. As a consequence, those with malicious intent (commonly referred to as "bad actors") increasingly leverage product weaknesses to gain unauthorized access to information, presenting threats to privacy, public safety, protection of intellectual property, and national security. The threats now are many and present real and difficult challenges for those charged to protect vital information.

Security and resiliency must be tightly integrated throughout the conception, design, implementation, deployment, maintenance, and operation of our cyber assets. Ultimately, it falls on the ability and attention of cyber workers across a broad range of specialties to better manage risk by identifying and mitigating vulnerabilities at every stage of a product's life. Unfortunately, the average cyber worker is increasingly over-matched when confronted by an ever-increasing demand to master more and more skills, languages, configurations, etc. You, our readers, can help those cyber workers better manage cyber risk by "baking-in" security at every stage of a system's lifecycle. By doing so, you can deny attackers opportunities to disrupt or corrupt vital services. The Department of Homeland Security sponsors this issue of CrossTalk to feature new ideas that promise to better empower the cyber workforce.

As you read through this issue, please ask yourself a couple of questions. For instance, are we fully utilizing the talent of our cyber analysts, or can we offload some of this work to automated cyber tools? Are we developing and delivering easy-to-use tools where security is a default setting rather than an option? Is process-driven software development maximizing the value of the people in the process, or can it be improved? How can training programs better recognize and address common gaps in the developer knowledge base? Are attempts to increase the size of the workforce sustainable? Analysis by experts in the field in the following articles shed light on some of these topics.

In today's environment marked by a vexing scarcity of cyber talent, it is clear that we cannot afford to waste the potential of our cyber human capital. In fact, to keep pace with emerging challenges, we must do our utmost to expand its potential. No single, easy solution has emerged to remedy our cyber challenges, and finding today's solutions will require plenty of smart, innovative people, new ideas and approaches to solving problems and, ultimately, a lot of hard work. It is important to strive to ensure that within our cyber workforce, nothing is wasted.

Greg Touhill
Brigadier General, USAF (ret)
Deputy Assistant Secretary
Office of Cybersecurity and Communications
U.S. Department of Homeland Security