# Defense CIO Wants Risk-Based Information Security Solutions

Posted At : September 16, 2014 9:40 AM | Posted By : Kyra Fussell
Related Categories: Critical Infrastructure Protection, Department of Defense, Innovation, Information Security, Cloud Computing, Cybersecurity

At an industry event in early September 2014, Department of Defense CIO Richard Hale described the setbacks associated with the current "one-size-fits-all" model for security system standards.

The goal of implementing risk-based security solutions is not a new concept, but there are differing opinions on how best to approach a risk-based model. Historically, there's also been an absence of best practices. In fact, the lack of consensus on best practices received a fair amount of attention over the past year during planning session targeting improvement for critical infrastructure protection.

Some of the barriers that the Defense Department faces are not unique. In many cases, however, defense information systems do require higher or additional levels of security. The administration has even called out improving information security as a Cross-Agency Priority (CAP) Goal, focusing on making network security advances and developing metrics for success as well as best practice sharing.

One of the hurdles agencies have faced in implementing risk-based security is getting a handle on their data. With the swelling volume and variety of information on government systems, organizations have been playing catch up to understand the information they currently store and manage. This effort is further complicated by varying levels of data sensitivity and classification.

Determining an agency's risk tolerance has also been a challenge. Fiscal constraints, however, are making it clear that treating all systems and data equally is unsustainable and impractical. As Hale noted, "I shouldn't spend as much money on morel and welfare websites as I do on nuclear command control. It doesn't make sense."

Cost efficiency wouldn't be the only benefit of adopting a risk-based information security posture. Innovation is another area that stands to gain as the Defense Department could more readily adopt commercial technologies. As the Defense Department looks to leverage cloud and mobile computing technologies, the issue of risk tolerance takes on an additional layer as the role of service providers increases. As the Defense Department pursues shared cyber defense capabilities, they need to establish common security controls requirements and identify trusted providers.

Hale's comments mentioned "zoning by mission risk," which could assess general levels of computing and network infrastructure risk-tolerance for different missions. This would help address the problem that Hale called out around security spending for websites and nuclear missions. It also allows missions with similar levels of risk-tolerance to benefit from efforts around common issues like sharing information and defining security requirements. Before such an approach could transition into general practice on an enterprise-level, an agency needs to have a handle on its data.

---

*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@FIAGovWin** .*