Making Global Collaboration Secure
In a Changing Threat Environment

PERSPECTIVES:
Chandra McMahon

Vice President & Chief Information Security Officer
Enterprise Business Services
Lockheed Martin

Chandra McMahon is Lockheed Martin's Chief Information Security Officer and Vice President of Corporate Information Security. In this role she is responsible for Lockheed Martin's information security strategy, policy, security engineering, operations and cyber threat detection and response. She also currently serves as the executive sponsor of the Corporate Business Resiliency initiative and co-chairs the Lockheed Martin's Women's Leadership Forum.

Prior to her current role, Ms. McMahon served as the President of Lockheed Martin Properties, Inc. with responsibilities including corporate real estate, commercial leasing, economic development and facilities management. In this capacity, she led the construction and launch of Lockheed Martin's Center for Leadership Excellence, the Corporation's education and training center.

Ms. McMahon has more than 22 years of diverse management and technology experience leading critical initiatives for Lockheed Martin. While in various IT leadership positions in the heritage Integrated Systems & Solutions (IS&S) CIO organization, Ms. McMahon developed IT services strategies and delivered capabilities that met the changing needs of the business while still achieving operational cost reductions. Beyond Lockheed Martin and as a director at First Consulting Group, Ms. McMahon launched an industry-leading enterprise content management product suite for the pharmaceutical sector and led a multinational product development team with members in Asia, Europe and the United States.

Ms. McMahon holds a bachelor of science degree in industrial engineering and operations research and a master's degree in engineering science. She has also earned the designation of the Program Management Institute's Project Management Professional (PMP).

Coming up in March, the Transglobal Secure Collaboration Program (TSCP) will hold its Spring Symposium and Expo at Lockheed Martin's Global Vision Center in Arlington, Virginia. As secure collaboration is TSCP's focus, ***Trust Points*** was pleased to have the opportunity to interview Ms. McMahon, and hear her view on some of the challenges that face TSCP member companies as well as their customers and organizations that make up their supply chains. The following are our questions (TP) and responses from Ms. McMahon (CM).

TP: The global economic situation continues to stress IT investments. In the area of Secure Collaboration with Industry and Government, what key initiatives and services do you envision will be critical over the next five years?

CM: We are working with the Transglobal Secure Collaboration Program (TSCP) on specifications to access applications and data across organizational boundaries, commonly referred to as federated access. We are doing so using the identities on industry issued smart cards as well as on customers' Common Access Cards (CAC) and Personal Identity Verification (PIV) cards. I also believe, as we collaborate across corporate and national boundaries, consistent labeling and marking of information is critical to protecting proprietary information and complying with export control policies. We are engaged with TSCP members and technology providers to jointly develop common specifications that address information protection.

Finally, exchanging email securely with our customers, partners and suppliers by encrypting the content using TSCP specifications is a critical focus area. Avoiding one-off solutions and using industry standards enhances our return on investment by creating solutions that are re-usable by many programs, reducing overall operational and maintenance costs while protecting content during transmission and storage.

TP: What IT security and cyber challenges or issues are coming down the road for your company? What keeps you up at night?

CM: The growing use of mobile devices and cloud computing immediately come to mind. On the mobility front, the key here is the proliferation of devices that need to be secured. From iOS to Android – iPads to other tablets – this challenge is only going to grow over time. When it comes to cloud computing, the key is identifying the location and security of your data. By its very nature, the cloud runs contrary to that traditional concept of location-based data and control, but that's a key issue we've got to address.

We are also forced to continue adding new capabilities to address ever-changing tactics used by our adversaries. We continue our focus on intelligence-driven defense that leverages our Cyber Kill Chain methodology. That's why we've ensured our team has adequate resources to deploy new defensive solutions as well as advanced forensics capabilities.

Finally, we've recognized that our employees have become a first-line of defense. A big area of concern lies in the use of social engineering tactics to better target individuals. We've worked hard to train our employees on things they should and shouldn't do to minimize this risk.

TP: What do you see as impediments to Cloud Computing Adoption within the Aerospace and Defense Industry? What areas or programs do you envision going to the cloud?

CM: We sponsored a recent survey that asked government IT decision-makers about their potential adoption of and concerns with cloud computing solutions. We found that key decision makers are becoming more comfortable with moving to cloud solutions based largely on growing familiarity with the concept and increased experience with implementations. However, they also continue to express concerns, especially when it comes to storing highly sensitive information in the cloud.

The survey found that Software as a Service (SaaS) is probably one of the most highly accepted uses of cloud technology right now. Other uses such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS) or IT as a Service (ITaaS) are still being considered. I think you'll continue to see this landscape change over the coming couple years as government IT folks get more comfortable with the technology and our security professionals fully analyze, develop and deliver appropriate means of protection.

TP: What capabilities and solutions do you believe your company will need to be developed on behalf of your customers?

CM: As we've discussed, I think mobility and cloud computing are both areas where our Corporation can provide a lot of value. We are also focused on offering managed security services to help address the issue of the Advanced Persistent Threat (APT). Our Corporation has extensive expertise in big system integration type solutions and I think the area of cyber security will be no different. We'll need to help customers protect and manage their information in a way that is agile, effective and affordable.

TP: The Aerospace and Defense industry has evolved into a worldwide partnership of customers, partners, and suppliers. What common challenges do you envision will need to be addressed to meet the requirements of secure collaboration?

CM: There are a variety of challenges that need to be addressed. Much of this goes back to assured identity – making sure users are who they say they are. Without that level of trust, it is hard to establish effective means of collaboration. I also think it is important we continue to work to establish common standards and at times leverage common technologies. Speaking the same language and using similar, interoperable technologies will greatly aid our efforts in secure collaboration. Finally, I think we'll need to collectively address the growing importance of mobile devices and how they can be used for secure collaboration.