

## **Defense Systems November – December 2006**

### **WEB EXTRA of the Thomas Reardon Q&A**

Following are additional questions and answers from an interview with Thomas Reardon, chief of the Intelligence Division for the Army Network Enterprise Technology Command/9th Army Signal Command, that appeared in the November/December issue of DEFENSE SYSTEMS. Editor Dawn S. Onley talked with Reardon about how the command's efforts to improve end-to-end information assurance.

**DEFENSE SYSTEMS:** What are foreign hackers after and where are they coming from?

**REARDON:** Foreign entities are after information about our Army and how we intend to fight. It's hard to tell exactly where these actors are basing their activities to access this information. The attacks can launch from a variety of relay points. I can't get into the details for reasons relating to classification.

**DEFENSE SYSTEMS:** How is NETCOM specifically countering the threat?

**REARDON:** I cannot get into specific techniques; however, I can tell you that NETCOM's network operations centers are closely aligned with the various computer emergency response centers, the regional chief information officers around the globe, and Joint Task Force-Global Network Operations (JTF-GNO) to coordinate defense and mitigation activities.

**DEFENSE SYSTEMS:** What does FOCI stand for?

**REARDON:** Foreign Ownership, Control and Influence. This term comes from the National Industrial Security Program Operating Manual (NISPOM), and it is used to identify risks associated with the use of foreign vendors to support U.S. classified contracts. Before a classified contract can be let to a vendor that may be operating under some level of FOCI, the risk must be assessed.

We are working with Army CIO to recommend a change to the Federal Acquisition Regulation to extend this assessment to vendors seeking to support the Defense Department Global Information Grid at any classification level.

However, I must point out that DOD policy does not preclude the use of foreign commercial vendors, and our industry partners are becoming increasingly multinational and rely on foreign components and labor for IT products and services. Nonetheless, we must be careful to ensure that a vendor cannot be influenced by foreign entities or agents to do the wrong things, and we must be able to provide our decision-makers with sufficient information to mitigate risk through knowledge.

**DEFENSE SYSTEMS:** What prompted Army NETCOM to build a new battle command lexicon?

**REARDON:** Gen. Pollett is emphasizing that defense of the LandWarNet becomes leader business and commander business. Too many times in the past we have seen examples where commanders have viewed intrusions of their systems as the concern of the director of information management (DOIM) or signal officer (SIGO).

Commanders and leaders must be as familiar with terminology like Category 1 and Category 2 incidents (specific levels of intrusion as defined in CJCSM 6510.01, *Defense in Depth: Information Assurance and Computer Network Defense*) as they are with terms such as “passage of lines” and “hasty defense.”

Given the fact we are an Army and nation at war, these incidents must be considered the equivalent of incoming rounds. Category 5 events are also important to commanders and leaders as these events are caused by non-compliance of a directive to install a security patch or the improper configuration of a system. It is highly likely that a Category 5 event can be a precursor to a more serious Category 1 or 2 incident and must be considered as a serious issue by commanders and leaders.

Gen. Pollett is now making sure that the senior mission commanders of installations that are the recipients of a Category 1 or a Category 2 incidents are informed immediately. This is as important to a commander as any other issue involving readiness.

**DEFENSE SYSTEMS:** What is involved in tracking the source of a cyberintrusion?

**REARDON:** While I cannot comment on specifics, I *can* assure you that this source tracking involves a tremendous amount of coordination between network operators and defenders with law enforcement and counterintelligence, and JTF-GNO. This community of interest is constantly expanding and improving.

*Copyright 2006, PostNewsweek Media*