Cybersecurity – From Frameworks and Farewells to Foreign Affairs

Posted At : September 24, 2013 4:13 PM | Posted By : John Slye

Related Categories: Critical Infrastructure Protection, Department of Defense, Department of Homeland Security, Technology Trends, Intelligence Community, Information Security, Cybersecurity, Policy & Legislation

It's been a busy time lately on the cybersecurity news front. In the last few weeks, there have been reports ranging from the release of evolving cybersecurity policies to outright attacks, and rumors of past and future attacks, on traditional networks and websites as well as industrial and weapons systems. It seems that cybersecurity issues are all-pervasive.

On the policy side, the National Institute of Standards and Technology (NIST) released a preliminary cybersecurity **draft framework** outlining various standards, best practices and guidance to provide guidance to organizations on managing cybersecurity risks. According to **comments** surrounding the release, the goal is to complement, rather than replace, an organization's existing cybersecurity processes. The primary focus of the framework is improving cybersecurity among private **critical infrastructure** owners like utilities and other industrial entities, although there may be some applications for government agencies as well. The current draft is the next round in an eventual final framework that is expected to be codified in October.

The NIST critical infrastructure cyber- framework draft release comes on the heels of some very earnest comments from the outgoing Homeland Security Secretary, Janet Napolitano. In her **farewell address**, the Napolitano urged her eventual successor to have a strong sense of urgency in preparing for major cyber-attack on US infrastructure. "While we have built systems, protections and a framework to identify attacks and intrusions, share information with the private sector and across government, and develop plans and capabilities to mitigate the damage, more must be done, and quickly," Napolitano said.

While it is widely acknowledged that adversarial nations employ offensive cyber capabilities against the US government and industry, etc. the threat also includes non-state and other loosely-defined actors. For example, al-Qaeda has been **exploring** ways to conduct cyber-attacks on US drones, enlisting engineers to identify ways to exploit any technical vulnerability in the aircraft to jam or remotely hijack them or otherwise compromise them to reduce their effectiveness. And with the brewing potential for US strikes in Syria there were **reports** of tampering with a Marine Corps recruitment website by apparent pro-Syrian government hackers. It is unclear whether these or other actors could or would be able to effectively strike at other, less mundane, targets if things escalate.

Speaking of cyber-attacks . . . There's growing confirmation that the US is taking its offensive cyber capabilities as seriously as its defensive know-how. The **news** that US intelligence entities have carried out hundreds of offensive cyber-operations against adversaries over the last few years, likely to include the Stuxnet attack on Iranian nuclear control systems, hints at the scope, abilities, and magnitude of their efforts. A related **report** reinforced the fact that federal cybersecurity spending – both defensive and offensive – is decentralized and peppered throughout numerous programs and areas.

There is a theme that connects all of these areas: As information technology continues to advance and permeate how we operate our critical infrastructures, government and military, the demand to protect and exploit this technology will continue to grow. And federal spending will likely grow with it.

---

*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWin FIA**. Follow me on Twitter **@GovWinSlye**.*