Set-Aside Alert™
www.setasidealert.com
Vol. 22, No. 3 Your source for Federal set-aside and small business contracting news since 1992 Feb. 7, 2014

# Are you ready for the cybersecurity boom?

**by Jon Williams, partner, PilieroMazza PLLC**

The government buys a significant amount of information technology (IT) services from the private sector, and this probably will always be true. However, in recent years the government's overall IT spending has stagnated. IT is still the place to be for many contractors, but understanding the direction of federal IT spending is critical to ensuring you are positioned where the government and technology are headed.

**Cybersecurity a hot area**

In fiscal year 2014, IT spending is expected to grow for the first time in several years, driven in part by a surge in spending on cybersecurity.

Cybersecurity is an increasingly hot area and it seems to have staying power: overall spending on cybersecurity is estimated to be as much as $13 billion in 2014, and is expected to steadily increase to $17 billion by 2017. Therefore, if you work in the IT field, you should be asking yourself whether your company is positioned to benefit from the boom in cybersecurity spending.

The current federal budget for cybersecurity is geared towards investments in innovative solutions to protect against emerging threats to federal networks and critical infrastructure.

In addition, the government is focusing on research and development, continuous monitoring and better prevention of intrusions, improving incident response, and facilitating information sharing among agencies regarding threats.

Certain agencies, like DHS and the VA, are seeing a significant increase in IT spending. DHS in particular has and will continue to play an important role in the government's cybersecurity measures.

**Legislative initiatives**

There have been several recent attempts at legislation to address cybersecurity. The lawmakers have had difficulty advancing these measures because of privacy and other concerns raised by the Edward Snowden situation and the increased scrutiny of the National Security Agency's practices.

One bill that may have decent prospects was introduced by House Homeland Security Committee Chairman Michael McCaul, R-TX, in December. The bill, referred to as the Cybersecurity and Critical Infrastructure Protection Act of 2013, is aimed at preventing cyber attacks on the banking system, energy pipelines, telecommunications networks, and other critical infrastructure. The bill does not include controversial liability protections found in an earlier House-passed measure that would have given companies broad liability protections in exchange for sharing cyber threat data with the government. The bill has been lauded because it codifies DHS' National Cybersecurity and Communications Integration Center as the entity charged with facilitating real-time sharing among agencies of information about cyber threats to critical infrastructure.

**Cybersecurity in contracting**

As the government continues to focus on increasing cybersecurity, contractors should expect to see more cybersecurity requirements flowed down to them in prime contracts and subcontracts. For example, last November, two new DFARS rules were implemented to place responsibilities on contractors for cybersecurity. Both of the new rules were effective November 18, 2013.

The first of the two new rules requires contractors to implement adequate measures to safeguard unclassified DOD information within the contractor's information systems. This rule also requires reporting of certain intrusions into the contractor's information systems. Cloud service providers and ISPs are considered to be a subcontractor under the rule, and the prime contractor is responsible for ensuring compliance by its subcontractors.

The second rule is designed to allow the DOD to assess the risk of cyber threats in contractor supply chains on procurements related to national security. Defense contractors throughout the DOD's supply chain have been targeted by cyber attacks designed to steal unclassified technical data.

To address supply chain vulnerabilities, the new rule establishes a pilot program to mitigate supply chain risk. The pilot program will run through September 2018. The new rule indicates procuring officials should consider whether to use an evaluation factor regarding supply chain risk when establishing solicitations. The rule also allows the government to limit disclosure of certain information in post-award debriefings and states that such limitations cannot be protested to the GAO. A supply chain risk contract clause will be added to contracts in appropriate cases.

**Cybersecurity a growing priority**

The growing priority for cybersecurity in federal contracts will expand beyond DOD contracts that deal with national security issues. Indeed, there are a variety of ways and many agencies through which determined cyber criminals can attempt to access critical information or affect critical infrastructures. Consequently, contractors should expect to see more cybersecurity measures in their contracts even if your company does not perform IT and/or defense work.

And with this trend comes opportunity. The budget forecasts demonstrate the government is placing a premium on innovation and solutions in the cybersecurity field. Therefore, if you follow the money and the technology, cybersecurity is an area you want to have on your radar in 2014 and the next several years.

*Jon Williams is a partner with PilieroMazza and a member of the Government Contracts Group. He also works with the Business & Corporate and Labor & Employment Groups. He may be reached at jwilliams@pilieromazza.com.*