VENABLE® LLP

Government Contracts Update

February 2014

Cybersecurity: Coming Soon to a Government Contract Near You

AUTHORS

Rebecca E. Pearson
William L. Walsh, Jr.
Keir X. Bancroft

RELATED PRACTICES

Government Contracts

RELATED INDUSTRIES

Government Contractors
Cybersecurity

ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007

Do you want to be eligible for government contracts in the future? Per President Obama's **Cybersecurity Executive Order**, a DoD and GSA joint working group recently recommended how cybersecurity can be implemented in federal acquisitions. The White House has recommended that the joint working group move quickly to develop an implementation plan for these recommendations, and outreach efforts are currently underway. For starters, all contractors must implement basic cybersecurity hygiene, take a close look at their supply chains, and ensure their workforce receives adequate cybersecurity training.

Specific key recommendations include:

Establish Baseline Cybersecurity as a Condition of Award

For acquisitions presenting cyber risk, the government should ***only do business with*** organizations meeting baseline cybersecurity hygiene requirements. Baseline cybersecurity will apply to the contractor itself, and its products and services. The baseline recommendations include:

- Update virus protections;
- Apply multiple factor logical access;
- Ensure data confidentiality; and
- Maintain current security software patches.

Baseline cybersecurity requirements will be included in technical requirements for acquisitions, and include performance measures to ensure baseline cybersecurity is maintained, and ensure risks are identified throughout the lifespan of the product or service acquired.

Require Purchases from OEMs, Their Authorized Resellers, or Other "Trusted" Sources

If there is sufficient cyber risk, an agency may procure items only from original equipment manufacturers (OEMs), authorized resellers, or other trusted sources.

- Trusted sources – may be identified through use of qualified bidders, or manufacturers lists (QBLs). The standards for establishing the QBLs will be based on the level of cyber risk to be mitigated.
- Non-OEMs or trusted sources must guarantee the security and integrity of an item being purchased.
- For high cyber-risk procurements, government audit may be necessary to evaluate qualifications to provide items.

These requirements reflect the joint working group's focus on addressing supply chain risk and addressing anti-counterfeiting. An example of an OEM requirement is found in the recent draft RFP for the NASA SEWP V (Solutions for Enterprise-Wide Procurement) contract, which expressly limits certain equipment requirements to items coming from OEMs or their authorized resellers.

Condition Contract Eligibility on Workforce Cybersecurity Training

The joint working group has recommended comprehensive training for the acquisition workforce, including federal and contractor employees.

- For some acquisitions, contractors may be required to give their workforce compulsory cybersecurity training to be eligible to compete.
- A suggested model is GSA's "Pathway to Success," a mandatory training program for would-be offerors for GSA Schedule contracts.

The joint working group made other recommendations as well, including:

- Developing common cybersecurity definitions throughout federal acquisitions, based on international standards;

- Applying cybersecurity requirements, or “overlays” depending on the cyber risk of an acquisition; and
- Holding agency personnel accountable for implementing cybersecurity protections throughout federal acquisitions, a requirement that will no doubt increase pressure on contractors to comply with agency cyber requirements.

To ensure your organization remains eligible to compete in upcoming federal acquisitions and is aware of opportunities for public comment on proposed implementation, please reach out to Keir Bancroft at , Bill Walsh at , Rebecca Pearson at , or other members of Venable’s **Government Contracts Practice Group** about the latest cybersecurity developments in federal acquisition.