

Cybersecurity Alert

April 2012

DoD Fast-Track Acquisition Process Promises New Opportunities for Contractors

AUTHORS

Robert A. Burton
Dismas Locaria
Andrew E. Bigart

RELATED PRACTICES

Government Contracts

RELATED INDUSTRIES

Government Contractors

ARCHIVES

2012 2008 2004
2011 2007 2003
2010 2006 2002
2009 2005

The U.S. Department of Defense (“DoD”) is establishing a fast-track acquisition process for cybersecurity products and services. The new process, which DoD plans to roll out within the next six months, promises to provide new opportunities for government contractors in the cybersecurity industry. This Client Alert provides an overview of DoD’s proposal (which has not been detailed in public) and guidance for companies looking to position themselves for these acquisitions.

Under the proposal, DoD would set up a separate track for the acquisition of urgent, mission-critical cyber warfare products and services. All other acquisitions would follow a more deliberate, standard acquisition track. U.S. Cyber Command (“USCYBERCOM”) would review each acquisition and determine the appropriate path to follow based on factors such as need, timing, complexity, and cost of developing a particular cyber warfare capability. USCYBERCOM would, presumably, have flexibility to postpone or eliminate standard acquisition requirements under certain urgent time frames.

To manage the process, DoD plans to set up a Cyber Investment Management Board (“Board”), chaired by Frank Kendall, Acting Undersecretary of Defense for Acquisition, Technology and Logistics; James Miller, Acting Undersecretary of Defense for Policy; and Admiral James Winnefeld, Vice Chairman of the Joint Chiefs of Staff. It is not clear at this time what relationship the Board would have with USCYBERCOM.

Cybersecurity companies should consider the following in order to best position themselves for taking advantage of this “fast-track” process:

- Establish a federal business monitoring and marketing presence to identify cybersecurity opportunities at their infant stages so that you are able to quickly respond when the agency moves a procurement forward.
- Anticipate and prepare to address certain basic government contracting prerequisites before the DoD goes to market for providers. These may include:
 - Registration with the Central Contractor Registration (“CCR”) and the Online Representations and Certifications Application (“ORCA”); and
 - Possessing a Commercial and Government Entity (“CAGE”) code.
- Implement general compliance requirements, such as:
 - Having a written code of business ethics and conduct, and if the company is other than “small,” having in place a suitable compliance program;
 - Meeting various socio-economic requirements (e.g., having an affirmative action plan); and
 - Ensuring products are manufactured in compliance with DoD domestic preference requirements.
- Obtain facility and staff clearances so that your company is able to bid and work on projects that involve classified information.

Addressing these issues in advance will allow companies to respond quickly and effectively to fast-track cyber product and service procurements.