Security Debrief | September 8, 2014

Cyber Policies and Executive Order Need Harmonization With Acquisition Rules and Practices

By David Z. Bodenheimer, *Guest Contributor*

(http://securitydebrief.com/wp-content/uploads/2014/09/bodenheimer-david_color300dpi-c.jpg) As one of the world's largest buyers, the U.S. federal government's acquisition rules and buying practices have a direct impact upon major segments of the U.S. and global marketplaces. This key federal role extends to information technology (IT) and cybersecurity where the federal government will spend $82 billion on IT products and services in Fiscal Year 2014 alone, use and oversee huge networks and data repositories, and guard vital information ranging from healthcare data and taxpayer returns to military technology and commercial trade secrets.

Cybersecurity Executive Order 13636 (http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity) and Presidential Policy Directive 21 (http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact Sheet 12March13.pdf), both issued in February 2013, recognize that the federal acquisition process must be addressed as part of the overall federal strategy for enhancing cybersecurity. The Department of Homeland Security is the Federal government's lead agency for coordinating the protection, prevention, mitigation, and recovery from cyber incidents. DHS also works regularly with business owners and operators to strengthen their facilities and communities by sharing cyber and other threat information. To further these important efforts, the

Cybersecurity EO directed the expansion of the DHS Enhanced Cybersecurity Services (ECS) program. Through ECS, DHS will assist critical infrastructure entities in reducing their cyber risk and more effectively keep sensitive data and critical systems secure.

The Executive Order recognizes that a "whole of government" approach will be needed to make it work, but there is a huge gap that needs to be filled. Currently, federal agencies and contractors do not have a unified government-wide acquisition regulation specifying what particular cybersecurity requirements apply to which federal procurements. Individual agencies have filled this void with their own unique choices of acquisition regulations and policies governing cybersecurity, resulting in a multiplicity of cyber regulatory regimes. This is creating a serious problem as private sector contractors attempt to comply with conflicting and confusing requirements.

It need not be this way. To address the regulatory process for federal acquisitions, the Cybersecurity Executive Order required that the acquisition regulators review the current landscape and "address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity." A DoD/GSA working group was formed and after considerable work, it issued its final report (http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf) in November 2013. Unfortunately, it created additional areas of confusion as it attempted to address the need for harmonization.

Fundamental federal acquisition and cybersecurity principles reinforce the Executive Order's call for harmony in cyber acquisition regulations:

> *Regulatory Uniformity* – As its core purpose, the Federal Acquisition Regulation (FAR) seeks "uniform policies and procedures for acquisition by all executive agencies." It also limits agency-level regulations (FAR§1.302) to those necessary to implement FAR policies and satisfy "specific needs of the agency."
>
> *Cost-Effective Cybersecurity* – As a key principle, federal law requires that agencies' cybersecurity programs and risk analyses consider cost-effectiveness – a factor likely to be enhanced by uniform acquisition regulations governing cybersecurity.
>
> *Greater Competition* – Like the FedRAMP objective for federal cloud cybersecurity ("approve once, use often"), uniform acquisition regulations for cybersecurity would reduce the burden for contractors – particularly small businesses – to compete more efficiently against a common government-wide cybersecurity baseline.

Better Cybersecurity – In response to the Cybersecurity Executive Order, both the Department of Defense (DoD) and the General Services Administration (GSA) acknowledged that harmonized acquisition regulations would enhance cybersecurity.

Current federal acquisition rules governing cybersecurity lack harmony and transparency. Neither federal agencies nor contractors can turn to a single government-wide acquisition regulation to identify the applicable cyber acquisition requirements. Instead, both agency officials and federal contractors must search each agency's individual acquisition regulations and internal policies to identify such requirements. A review of these agency-level cyber regulations reveals a number of challenges:

Regulatory Disharmony – Not surprisingly, different agencies have adopted different cyber rules and policies. Even within some agencies, inconsistencies exist for certain requirements, such as data breach notification.

Internal Agency Policies – Nearly all agencies have acquisition requirements imposing internal agency policies and instructions upon contractors, even though these internal guidelines do not appear to be published for public comment as required by law.

Non-Standard Cyber Requirements – Some agency acquisition regulations impose cyber requirements with minimal reference to government-wide standards for risk assessments, security controls, and other cybersecurity best practices.

In summary, the Executive Order 13636 and PPD-21 triggered a much-needed opportunity to address the agency-by-agency patchwork of acquisition regulations and policies governing cybersecurity. Yet, as the report of the DOD/GSA working group made clear, much work remains to be done to eliminate conflicts and confusion.

Harmonizing the cyber acquisition regulations would offer multiple benefits: (1) reducing agency-by-agency conflicts; (2) promoting greater competition based upon increased commonality in cyber rules; and (3) enhancing cybersecurity by leveraging best practices more cost-effectively across the federal government.

David Z. Bodenheimer, a Government Contracts partner and litigator in Crowell & Moring LLP's Washington, DC office, brings more than 30 years of experience in doing business with the federal government, handles a broad range of public-sector acquisition and cybersecurity issues, and serves as the Public Contract Law Section's (PCL) representative to the ABA President's Cybersecurity Legal Task Force.

Read More