wiley

NEWSLETTER

Six Cybersecurity Questions for In-House Counsel

Winter 2012

Cybersecurity is a hot topic these days. While overall federal IT spending for 2013 is projected to decrease between 1%-4% for DoD and civilian agencies, federal investment in cybersecurity is expected to rise; Congress is actively debating enhanced cybersecurity legislation packages (*see* accompanying article); and Government IT specialists are furiously warding off the daily slog of hacks, worms, viruses and intrusions. Government contractors are full partners in the Government's cybersecurity efforts-contractors develop and maintain government systems and networks, and frequently manage sensitive government data on their own networks. Against this backdrop, and underscored by a host of cyber intrusions targeting government contractors in the last 18 months, here are six topical questions for in-house counsel to ponder.

- **What does the contract say?** There are surprisingly few uniform standards of care or cybersecurity requirements that apply to all government contracts. The FAR briefly addresses cyber issues in Part 39, and DoD recently acknowledged that the DFARS does not address safeguarding information on unclassified systems. *See* Safeguarding Unclassified DoD Information, DFARS Case 2011-D039, 76 Fed. Reg. 28089 (June 29, 2011). Cyber requirements vary by agency and contract, and security requirements are frequently incorporated into a statement of work via line item references to various NIST standards or agency instructions or directions; it is not uncommon for a contract to incorporate dozens of standards in this fashion. Contractors face risks if the operational team performing a contract is not familiar with those standards or if there are gaps between the standards of care that the contract

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

requires and what the contractor delivers. If a contractor's failure to adhere to required standards of care creates or increases a system or network vulnerability that is exploited in a cyber event, it is likely to lead to a contractual headache (in addition to the practical problems that an intrusion brings).

- **Do your company's systems meet proposed new minimum requirements?** The DoD's Proposed Rule on safeguarding unclassified DoD information, 76 Fed. Reg. 28089, calls for "basic" and "enhanced" safeguarding techniques, many of which require a contractor's IT systems to meet minimum security requirements. Although not final, the Proposed Rule telegraphs the direction that DoD, intelligence and eventually civilian agencies will likely move. The Proposed Rule would also require contractor personnel to follow basic IT security protocols (*i.e.*, do not use public kiosks to access DoD information; transmit electronic data using only "the best level of security and privacy available"). Meeting these new standards may require contractors to revisit their network security protocols and to implement employee IT training and compliance programs.
- **Do your company's systems adequately segregate government information?** For contractors who conduct federal and commercial business over a single IT network, or rely on federal "enclaves" for government contracts, contractors need to be certain that those systems adequately segregate and protect government data. For example, contractors who generate or store ITAR-controlled data on their government systems need to be certain that non-U.S. persons who may operate on the "commercial" side of the business do not have access to controlled data, so that there can be no improper "deemed export." Likewise, if a contractor stores information that is unclassified standing alone, but if aggregated could be upgraded in classification, the system may need to have protocols in place to prevent improper aggregation. Each company's system architecture needs to be designed or revisited with concerns like these in mind.
- **Do employees have access to personally identifiable information?** A recent proposed FAR rule, Privacy Training for Contractors, 76 Fed. Reg. 63896 (Oct. 14, 2011), would impose new training requirements for contractor employees who handle personally identifiable information (PII) for the Government, or design, develop, maintain, operate or have access to a government system of PII records. The Proposed Rule would extend Privacy Act obligations to the contractor workforce, and require contracting officers to insert one of three new clauses requiring training into covered contracts. In anticipation of a final rule, contractors should identify employees who have access to PII, and be prepared to develop new training and compliance programs consistent with the Proposed Rule's guidance.
- **Do employees have access to shared government systems that hold source selection sensitive or third-party proprietary data?** The temporary suspension of a contractor business unit in June 2010 as a result of alleged misuse of data on a Goverment system was a wake-up call to many in the industry regarding contractors' shared access to Government systems and networks that hold competitively sensitive information. It is not uncommon for Government employees (and contractors) to use these shared sites to store source selection sensitive or third-party proprietary data, sometimes (usually inadvertently) without adequate security controls to limit access or distribution. Contractor personnel must be trained to resist the temptation to "troll" these networks for improper competitive purposes.

Moreover, contractors need to be sensitive to potential "unequal access to information" organizational conflicts of interest that might arise from access to Government systems and networks, if that access could be construed to create an unfair competitive advantage in a later competition.

- **Should cybersecurity be added to your due diligence checklist?** Cybersecurity risks can manifest as contractual, past performance and even suspension and debarment problems. DoD already has the authority under Section 806 of the 2011 NDAA to exclude sources (including subcontractors) from competitions in connection with national security systems if the source poses a supply chain risk. Furthermore, a likely new trend in cybersecurity legislation currently pending in Congress will increase certification liability for contractors overseeing "critical infrastructure," raising further the risk of related False Claims Act exposure. In light of these emerging business risks, companies may need to separately evaluate cybersecurity issues in connection with M&A due diligence.

By no means comprehensive, these questions should at least provoke some thought within contractor organizations. One thing is clear, cybersecurity is one of The Next Big Things in the federal space, and contractors need to be prepared to react and adjust as threats and requirements evolve. Clients regularly consult Wiley Rein on a range of cybersecurity issues, particularly the unique risks that government contractors face in this area.