ARNOLD & PORTER LLP

ADVISORY April 2010

DOD SEEKS TO PROTECT DOD INFORMATION ON UNCLASSIFIED CONTRACTOR COMPUTER SYSTEMS

The US Department of Defense (DOD) has proposed new rules to establish baseline requirements for safeguarding unclassified DOD information currently housed or transmitted on its contractors' and subcontractors' computer systems. On March 3, 2010, DOD issued an advance notice of proposed rulemaking (ANPR) and notice of public meeting.[1] The ANPR discussed possible changes to the Defense Federal Acquisition Regulation Supplement (DFARS) that would add new requirements for the safeguarding and proper handling of unclassified DOD information. The proposed rules would apply to all DOD prime contractors and all subcontractors at any tier, regardless of the amount of the prime contract or subcontract. The rules would supplement and expand existing DOD regulations, directives, and contract requirements which obligate contractors to safeguard DOD information and Personally Identifiable Information (PII). Under the proposed rules, contractors and subcontractors would be required to provide adequate security to protect unclassified DOD information on their information systems. In addition, contractors and subcontractors would have to report cybersecurity breaches for certain kinds of information to DOD. Once the rule is finalized, these regulatory requirements will appear as DFARS provisions to be included in DOD solicitations and contracts. DOD may also revise existing contracts to incorporate these new requirements.

DOD is seeking comments from government and industry on these potential changes. In particular, DOD would like to hear about relevant best practices, specific experience with any of the suggested requirements, and suggestions and concerns about the potential compliance burden. Comments about the ANPR must be submitted to DOD on or before May 3, 2010.

I. BASIC SAFEGUARDING REQUIREMENTS

In addition to existing federal regulations that impose a variety of information assurance obligations on contractors, under the ANPR, all contractors and subcontractors having any DOD data on their information systems would have to follow new basic safeguarding requirements. If a DOD contractor or subcontractor

1 Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Information (DFARS Case 2008–D028), 75 Fed. Reg. 9563 (Mar. 3, 2010); Defense Procurement and Acquisition Policy Defense FAR Supplement (DFARS) Publication Notice 20100303, *available at* http://www.acq.osd.mil/dpap/dars/change_notices.html (containing a brief summary and a link to the DFARS revisions in Word format).

Brussels
+32 (0)2 290 7800

Denver
+1 303.863.1000

London
+44 (0)20 7786 6100

Los Angeles
+1 213.243.4000

New York
+1 212.715.1000

Northern Virginia
+1 703.720.7000

San Francisco
+1 415.356.3000

Washington, DC
+1 202.942.5000

is unsure whether the data are DOD data, it must treat this as DOD data until DOD confirms otherwise.

Restrict Access

There are several proposals that would restrict public access to systems that contain DOD data. Two of the proposals restrict how contractors and subcontractors can access DOD data. One would prevent contractors and subcontractors from using computers that do not have access controls, such as username and password requirements, to access DOD information. Similarly, another would not allow contractors and subcontractors to use public computers, such as those in hotel business centers or internet cafes, to access DOD data.

There are also proposals that would restrict how contractors and subcontractors could share DOD data. For example, the requirements would prohibit contractors and subcontractors from posting DOD information on publically available web sites, except those web sites requiring user authentication, such as usernames and passwords, to gain access. The requirements would also prohibit contractors from transferring DOD information to subcontractors unless a subcontractor has in place at least an equivalent level of cybersecurity. Finally, whatever information is shared among contractors and subcontractors would be shared only on a need-to-know basis.

SECURE SYSTEMS

Contractors and subcontractors would also have to secure the parts of their information systems that house and transport DOD data. They would be required to store DOD information in a secure area, such as a locked room or cabinet, or behind at least one layer of user authentication, such as usernames and passwords. Contractors and subcontractors would be required to install and maintain antivirus and anti-spyware applications on the systems that store DOD data. They would also be required to apply all security-related software updates on a regular basis. They would also need to secure all of their electronic transmissions, such as email. However, the degree of security provided to electronic transmissions, while using the best available technology and processes, could be less for some contractors and subcontractors, based on the limitations of their facilities, conditions, and environment. Although these changes are significant, many contractors and subcontractors already meet these revised requirements as part of their current information technology practices.

Contracting Requirements

Finally, the ANPR proposes changes in contracting requirements. The proposals would require contractors to ensure, by contract, that subcontractors that will handle DOD information meet these federal requirements. DOD would no longer use the disclosure of information clause in contracts or solicitations unless the contractor will have access to or create DOD information.

II. ENHANCED SAFEGUARDING REQUIREMENTS

The ANPR proposes an enhanced level of safeguards that would be required for certain kinds of data beyond the proposed basic safeguarding requirements and existing federal regulations that impose a variety of information assurance obligations on contractors. The enhanced safeguarding requirements would apply to any DOD information that is designated as Critical Program Information or for withholding under the DOD Freedom of Information Act Program Directive or DOD Freedom of Information Program Regulation or has similarly restricted access. It would also apply to information that is or has been designated for controlled access and dissemination—such as “For Official Use Only,” “Sensitive But Unclassified,” etc.—information that is subject to export control under either the International Traffic in Arms Regulations or Export Administration Regulations, and information covered by the DOD Distribution Statements on Technical Documents Directive and the DOD Withholding of Unclassified Technical Data from Public Disclosure Directive. Finally, it would apply to PII protected by the Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA).

System Security

Contractors would be required to provide a more secure system to house and transport DOD data under the enhanced safeguarding requirements. Contractors and

subcontractors would also be required to comply with the NIST security controls.[2] They would also have to install and maintain antivirus and anti-spyware software on all of their network systems, not just those housing and transporting DOD data. Similarly, contractors and subcontractors would have to apply security-relevant software patches, service-packs, and hot fixes promptly, as opposed to regularly under the basic safeguarding requirements. They would have to control external access to their networks using firewalls, router policies, and host-based security services. They would also have to monitor all access to company networks for unauthorized access and/or transmissions. Contractors and subcontractors would also need to encrypt wireless communication according to NIST standards. In addition to these new DOD requirements, contractors and subcontractors would still have to comply with all other federal requirements for safeguarding information as applicable.

Contractors and subcontractors would be required to encrypt all files containing DOD data that are subject to the enhanced safeguarding requirements whenever they are stored on any mobile computing device, such as laptops, or removable storage media, such as USB thumb drives. When traveling or using mobile computing devices, contractors and subcontractors would have to use encrypted wireless connections. If encrypted, wireless connections were not available, they would be required to encrypt all data files.

BREACH NOTIFICATION

The proposed rules would require contractors and subcontractors to notify DOD of relevant breaches of cybersecurity, as described below, within 72 hours of the discovery of a breach. This requirement would supplement any contractor system reporting requirements included within a contract.

Relevant Types of Breaches

Under the proposed rules, contractors and subcontractors would be required to report breaches by persistent and proficient hackers, breaches that resulted in the actual theft or manipulation of DOD data, and any breaches where the intruder gained access to systems used to store or transmit DOD data.

Report Contents

Contractors and subcontractors would be required to report the date of the breach and the date it was discovered. The report would detail how the breach occurred, specifically what Internet Protocol (IP) addresses, domain names, and software tools were involved. The report would also discuss what the hacker did once he or she got inside the system, including what systems he or she accessed and the roles and functions of those systems. Finally, the report would include what DOD programs were, or could be, affected by the breach.

A follow-up report may also be required. If so, it would again contain a list of DOD programs affected by the breach and a description of what type of DOD information was compromised, with a brief description of the compromised information. It would also include a description of the amount of DOD data that was compromised and an index of the affected systems and of any DOD data stored on or transmitted through the affected systems. Finally, it would include a description of how the system was breached.

Emergency Response

In response to the cybersecurity breach, the contractor or subcontractor would be required to immediately review the accessed systems to identify what DOD data might have been affected. They would also be required to preserve and protect images of the known affected systems for future investigation and to cooperate with DOD in the investigation.

Confidentiality

The government would not make the information about the cybersecurity breach public. However, the government would share the information as needed to support the investigation, to enhance cybersecurity in other programs, and for legal and counterintelligence investigations.

III. NEW DFARS CLAUSES

As noted above, the new safeguarding requirements would be implemented through two new DFARS clauses.

2 NIST Special Publication 800–53 (Current Version), Recommended Security Controls for Federal Information Systems and Organizations, *available at* http://csrc.nist.gov/publications/PubsSPs.html.

The ANPR would add a new subpart to the DFARS called "Safeguarding and Cyber Intrusion Reporting of Unclassified DOD Information Within Industry." Proposed DFARS Subpart 204.74. Proposed DFARS 204.7403(b)(1) would provide that the Basic Safeguarding clause should be included "in solicitations and contracts" when the government "has identified that the [prime] contractor or a subcontractor **at any tier** will potentially have DOD information resident on or transiting its unclassified information systems. Similarly, proposed DFARS 204.7403(b)(2) states that the Enhanced Safeguarding and Cyber Intrusion Reporting clause should be included in solicitations and contracts when the prime or subcontractor at any tier will potentially have DOD information that meets the requirements for enhanced protection resident on or transiting its unclassified information systems.

As noted above, there is no dollar threshold for including these clauses in prime or subcontracts. Nor is there any exception for small businesses.

IV. PUBLIC MEETING

DOD will hold a public meeting on April 22, 2010, from 8:00 a.m. to 4:00 p.m. EST in the National Aeronautics and Space Administration's (NASA) James E. Webb Memorial auditorium, NASA HQ, 300 E Street SW, Washington, DC 20546. Attendees are welcome to make presentations and may choose to submit the presentations as comments as well. Presenters must submit their presentations by April 8, 2010.

We hope that you have found this advisory useful. If you have additional questions, please contact your Arnold & Porter attorney or:

Ronald D. Lee
+1 202.942.5380
Ronald.Lee@aporter.com

Ronald A. Schechter
+1 202.942.5160
Ronald.Schechter@aporter.com

Steven S. Diamond
+1 202.942.5223
Steven.Diamond@aporter.com

Nancy L. Perkins
+1 202.942.5065
Nancy.Perkins@aporter.com

Caitlin K. Cloonan
+1 703.720.7021
Caitlin.Cloonan@aporter.com

Peter V. Roman
+1 202.942.5290
Peter.Roman@aporter.com