BNA, INC.

FEDERAL CONTRACTS

BNA Employee-Owned Since 1947

REPORT

DOD

Proposed Rule for Protecting DOD Information on Unclassified Contractor Computer Systems — The Devil is in the Details

By Ronald A. Schechter, Ronald D. Lee, and Caitlin K. Cloonan

I. Introduction

Over the past twenty years, the world has seen technology develop at lightning speed. Exponential increases in our collective ability to communicate, access and process information have been created using the seemingly endless and ethereal collection of data available within cyberspace. The ease with which we can harness and use data has transformed national and global economies almost overnight and connected people in ways never before imagined. For better or worse, these advances continue to transform our world each and every day.

Ronald A. Schechter is a partner in the Washington office of Arnold & Porter LLP, counseling clients on government contract and national security issues. He can be reached at (202) 942-5160 or Ronald.Schechter@aporter.com. Ronald D. Lee is a partner in the Washington office of Arnold & Porter LLP, practicing in national security, cybersecurity, and technology law and policy. He can be reached at (202) 942-5380 or Ronald.Lee@aporter.com. Caitlin K. Cloonan is an associate in the Northern Virginia office of Arnold & Porter LLP, with a practice encompassing all aspects of federal government contracts law, including litigation, compliance, bid protests, claims, suspension and debarment, and contract administration issues. She can be reached at (703)720-7021 or Caitlin.Cloonan@aporter.com.

Though in most instances technological advances have improved our lives and been used for good, technology also offers fertile ground for those seeking to harm individual American citizens or to threaten U.S. national security. The threat of cyber crime is nothing new—it's been portrayed in fictional movies like ''War Games'' and witnessed firsthand with the capture of real-world spies such as Richard Hanssen.

In the past, these threats, whether fiction or real, where often characterized as a rogue individual ''breaking into'' a government system to steal classified and secure ''military'' information. However, the reality of the post-September 11th world is that cyber terror threats target far more than just ''military'' systems alone—these terrorists and criminals target entire governments and private industry alike. As the Director of National Intelligence (DNI) stated in Congressional testimony: ''the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial

 ISSN 0014-9063

networks, and other critical infrastructures.''[1] Today, a number of nations, rogue or otherwise, may already have the technical capability to conduct large scale cyber attacks against individuals, companies, industries or governments. Unlike years ago when cyber crime was limited to those possessing advanced computer capabilities, today's ''weapon of choice'' can be anything from a laptop computer or cell phone, to a handheld device or some other everyday wireless technology. This opens cyberspace up to the potential for a low-cost, yet highly damaging attack.

In response to this ever-growing cyber threat, the Federal government created several task forces and related organizations to recommend guidelines and to put forward new processes, standards and regulations for protecting both classified and unclassified data that are shared between government and private industry. In addition, various departments within DOD have over time promulgated their own individual security procedures as well.

Given this hodge-podge of security requirements, this year the DOD made a concerted effort to try to consolidate its policies, combine its resources and unify its cyber defenses against the threat of cyber attacks. One of the most critical and daunting tasks in this process involved developing a standard set of DOD rules for safeguarding unclassified information. On March 3, 2010, DOD issued an advance notice of proposed rulemaking (ANPR) and notice of public meeting.[2] The ANPR discussed possible changes to the Defense Federal Acquisition Regulation Supplement that would add new requirements for the proper safeguarding and handling of unclassified DOD information. The proposed rules would apply to all DOD prime contractors and subcontractors at any tier, regardless of the dollar amount of either the prime contract, or subcontract. The rules would supplement and expand existing DOD regulations, directives, and contract requirements, which already obligate contractors to safeguard DOD information and Personally Identifiable Information (PII).

Under the proposed rule, DOD contractors and subcontractors would be required to provide adequate security to ensure protection of unclassified DOD information on their information systems. Contractors and subcontractors also would be required to report cyber security breaches for certain kinds of non-contract related information to DOD. Once finalized, these regulatory requirements will appear as DFARS provisions and be included in all DOD solicitations and contracts. There is also the distinct possibility that DOD may seek to revise existing contracts to incorporate these new requirements.

Given the broad nature of the proposed changes, DOD has requested both government and industry to provide comments on these changes and their potential impact. In particular, DOD is seeking information about relevant best practices, specific firsthand experience with any of the proposed requirements, along with suggestions and concerns about the compliance burden these provisions would impose upon anyone doing business with DOD. Based on the public comments submitted to date, it is clear that most people agree with DOD's overall goal of simplifying and consolidating its existing cyber threat requirements, but there is an equal amount of concern that the proposed rule as written may be too rigid and impractical for many existing DOD partners—particularly smaller and mid-size companies.

II. OVERVIEW OF THE PROPOSED RULE

A. Basic Safeguarding Requirements Existing federal regulations already impose on contractors a variety of informational assurance obligations for safekeeping information. The new proposed rule expands upon existing requirements, and requires all contractors and subcontractors with any DOD data on their information systems to follow both existing and new basic safeguarding requirements. If a contractor or subcontractor is unsure whether the data residing in its systems are considered to be DOD data, it must automatically assume it is, and treat it as such, until the DOD confirms otherwise.

1. New ANPR Contracting Requirements As proposed, contractors would be contractually bound to ensure that all of their subcontractors also meet and adhere to the new federal requirements. In addition, DOD would also cease to use the disclosure of information clause in its contracts or solicitations, unless the contractor has access to, or creates, DOD information.

2. Securing Systems In order to ensure system integrity, contractors and subcontractors would be required to secure any parts of their information technology systems that house or transport DOD data. Essentially, these IT components would need to be placed in a secure area, such as a locked room or cabinet, or behind at least one layer of user authentication—e.g., requiring usernames and passwords for access.

Contractors and subcontractors also must install and maintain antivirus and anti-spyware applications on systems that store DOD data. Security-related software updates would also be required on a regularly scheduled basis, and all electronic transmissions, including email, would have to be secured without exception. That said, the degree of security provided to electronic transmissions could be less for some contractors and subcontractors, based on the limitations of their facilities, conditions, and environment—provided there is proof they already use the best technology and processes available.

While many DOD contractors and subcontractors already meet these revised requirements as part of their current information technology practices, others may soon need to begin investing in additional IT support and technology.

3. Restricting Access Several of the proposed rules would significantly restrict public access to systems containing any DOD data, and would also restrict how contractors and subcontractors access DOD data. Contractors and subcontractors would be unable to access DOD information via any computer that does not have

[1] Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record*, March 10, 2009, at 39-40.

[2] 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).

  FCR ISSN 0014-9063

minimal access controls, such as username and password requirements. Similarly, contractors and subcontractors would no longer be allowed to use public computers, such as those in hotel business centers or internet cafes, to access DOD data—even that which is unclassified.

Contractors and subcontractors also would be prohibited from posting DOD information on most publically accessible web sites, with the exception being those web sites requiring user authentication, such as usernames and passwords, for access. Contractors would be prohibited from transferring DOD information to subcontractors unless the subcontractor has an equivalent level of cyber security in place as that of the contractor.

Finally, whatever information is shared among contractors and subcontractors could only be shared on a need-to-know basis.

B. Enhanced Safeguarding Requirements The proposed rule would impose enhance safeguarding requirements for certain types of data beyond existing provisions that already 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 (CPI); or is subject to withholding under the DOD Freedom of Information Act Program Directive or the DOD Freedom of Information Program Regulation; or has similarly restricted access.

These proposals would apply to information that is, or has been, designated for controlled access and dissemination such as ''For Official Use Only,'' ''Sensitive But Unclassified,'' etc., and information that is subject to export control under either the International Traffic in Arms Regulations or Export Administration Regulations. Information covered by the DOD Distribution Statements on Technical Documents Directive and the DOD Withholding of Unclassified Technical Data from Public Disclosure Directive would also be covered under the new directive, as well as to PII protected by the Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA).

1. System Security The enhanced safeguarding requirements would require Contractors to provide a more secure system to house and transport DOD data. Contractors and subcontractors would also be required to comply with National Institute of Standards and Technology (NIST) security controls.[3] They would have to install and maintain antivirus and anti-spyware software on all of their network systems, not just those housing and transporting DOD data.

Under the enhanced requirements, contractors and subcontractors would have to apply security software patches, service-packs, and hot fixes ''promptly,'' as opposed to ''regularly'' as defined under the basic safeguarding requirements. They would have to control external access to their networks using firewalls, router policies, and host-based security services. All access to company networks would have to be monitored for unauthorized access and/or transmissions—regardless of whether network is DOD related or not.

All wireless communication must be encrypted to meet 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 may be applicable.

Contractors and subcontractors would be required to encrypt all files containing DOD data that are subject to enhanced safeguarding requirements whenever the data are stored on any mobile computing device, such as a laptop, Blackberry or iPhone, as well as 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, all data files would have to be encrypted.

2. Breach Notification The proposed rules would require contractors and subcontractors to notify DOD of relevant breaches of cyber security, as described in greater detail below, within 72 hours of the discovery of a breach. This requirement would be in addition to any reporting requirements already included within a contract.

a. Relevant Types of Breaches 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 an intruder simply gained access to systems used to store or transmit DOD data, but did not actually access and DOD data itself.

b. Emergency Response In response to cyber security breaches, the contractor or subcontractor would be required to immediately preserve and protect images of the known affected systems for f use in any DOD investigation. Simultaneously, the contractor or subcontractor would undertake a full review of the accessed systems to determine whether additional DOD data ***may*** have been impacted by the breach.

c. Security Breach - Report Contents Contractors and subcontractors would be required to report the date of the breach and the date it was discovered—if they differed. The report would detail how the breach occurred, and specifically what Internet Protocol ''(IP'') addresses, domain names, and software tools were involved. The report would also discuss what the hacker did once system access was gained, including what systems were accessed and the roles and functions of those systems.

The report would also include not only the specifically affected DOD programs, but would also need to describe what additional programs could assume to have been affected by the breach. Depending on the circumstances, a follow-up report may 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. 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 full description of the cyber attack and exactly how the system was penetrated.

[3] 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.

d. Confidentiality Under the proposed rule, the government would not make the information about the cyber security breach public. However, the government would reserve the right to share the information as needed to support the investigation, enhance cyber security 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. The ANPR would add a new subpart to the DFARS called ''Safeguarding and Cyber Intrusion Reporting of Unclassified DOD Information Within Industry,'' in which the two new clauses would reside.

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, there are no dollar thresholds for including these clauses in prime or subcontracts, nor is there any exception for small businesses.

IV. POTENTIAL ISSUES The two levels of protection proposed in these DFARS rules present a host of issues, both to the defense contracting community and also to any commercial vendor selling to DOD. Following the publication of the ANPR, numerous firms submitted comments to the proposed language, detailing the various technical challenges presented by the proposed regulation and offering their own suggestions and revisions. The comments reveal the many challenges of a ''one-size fits all'' approach and suggest that perhaps DOD's goals might best be accomplished with a rule that is one size fits ''***most***.''

A. Scope Review of the proposed rule reveals that DOD seeks to protect unclassified information in every contract, and at every level. Thus, as currently written, the proposed rule is sweeping in scope and would apply to every DOD contract (including all subcontracts) where DOD information is ''resident on or transiting'' a contractor's unclassified (internal) information system. The proposed rule does not set any dollar threshold for prime or subcontracts, nor does it specifically exempt small businesses or commercial procurements.

This sweeping scope could create significant and unintended repercussions to the DOD procurement community—primarily a chilling effect that dissuades small to medium-sized firms from participating in DOD procurements, because they simply cannot afford the administrative and financial burdens of compliance with the rule. In addition, contractors will undoubtedly seek to pass along, ultimately to DOD, the costs of compliance with this proposed rule. Thus, DOD could soon face significant increases in contractors' proposed contract prices.

B. Standardization - Objective or Obstacle?

In recent years, cyber threats have increased exponentially, as have the quantity of rules and regulations imposed upon contractors accessing and storing unclassified DOD information. DOD contractors have struggled to comply with this litany of new requirements. At the same time, these multiple regulatory requirements have created tensions across agencies seeking to ensure and enforce their own individual polices.

In response to this challenge, the new proposal offers a uniform set of rules applied across DOD's many agencies, divisions and departments. However, while the objectives of this approach are to simplify and streamline the process and ease regulatory burdens, the new strategy brings other unique issues into play.

In an effort to standardize and streamline cyber security across industry, the proposed rule does not recognize that numerous firms have multiple contracts with DOD and other agencies and that many of these firms already protect unclassified government and company proprietary information on a comprehensive, systemwide basis, rather than on a contract-by-contract basis. To ensure full compliance with the new DOD rule, contractors may be forced to overhaul their existing IT security protocols in their entirety—even though they already accomplish what the DOD is attempting to do. This could potentially create an administrative burden, disrupt existing IT security framework or could force duplication of existing resources.

In addition, some firms have expressed concern with the rule's proposed scope, which appears overly-broad in some areas, and overly specific in others. One example of this overly-broad approach is the requirement that safeguarding/marking address ''all DOD information.'' which may make execution difficult. For instance, the rule states generally that a basic level of protection will be provided to ''any'' DOD information that has not been cleared for public release in accordance with DOD Directive 5230.09. The rule then broadly declares that all unidentified information is assumed to be DOD information unless the cognizant DOD activity determines otherwise. This indefinite language may make it difficult for DOD contractors to know exactly what information has been cleared unless DOD marks every piece of information with a legend indicating the status of each piece of information.

While the language of the rule is very broad in some areas, other areas are so detailed that they may limit flexibility or any room for interpretation. Specifically, the rule references certain malware protection services (anti-virus, anti-spyware), and software upgrades (patches, service packs, hot-fixes) to protect basic safeguarding of information. While many companies use these packages, not all do, and that may unnecessarily limit potential protective measures.

Examination of the proposed rule also reveals certain ambiguities, which, absent clarification, could potentially lead to inconsistent or incorrect application by DOD and/or misinterpretation by a contractor. For example the proposed rule does not include a detailed definition for the term, ''DOD information.'' Rather, the proposed rule cross references another internal DOD document, and defines ''DOD information'' as ''unclassified information that has not been cleared for public release in accordance with DOD Directive 5230.09. . .'' to support an official DOD activity. As written, this definition could create significant confusion for contractors

  FCR ISSN 0014-9063

that are unfamiliar or inexperienced with this particular DOD Directive.

Perhaps DOD should determine what information is to be protected by contractors and should be under an affirmative obligation to mark all such data to be protected—as it is obligated to do with any level of national security classification or with procurement sensitive information and as a contractor is required to do to protect its rights in technical data. Contractors should not have to guess whether such important DOD information has complied with internal DOD procedures.

Likewise, the proposed rule's definition of ''adequate security'' includes protective measures that are commensurate with risk, which is a sensible concept. At the same time, however, section 252.7XXX(b)(3) requires that the ''best level of security and privacy available'' be used — a subjective standard that leaves much room for debate or confusion. Some may turn to their established security protocols, while others may interpret this to mean that contractors must continuously invest in and ensure compliance with every newly developed security protocol.

Comments submitted on the proposed rule have also noted that certain terms are left undefined entirely, leaving questions as to their meaning. For instance, terms such as ''Regularly updated,'' ''Appropriate,'' and ''Adequate: and ''Prompt'' remain undefined. Again, these ambiguous standards could lead to disparate interpretation and application of these critical IT security requirements.

C. Reporting Burdens - How Much is Too Much? As explained above, the proposed rule sets forth new reporting requirements, which raise significant concerns across the contracting community, one of which is the reporting of cyber intrusions. Section 204.7XX2(b) of the proposed rule requires that contractors report certain cyber intrusion events, without articulating whether there are ''types'' of events that generally require reporting. Absent further guidance, contractors may take the approach of reporting every single cyber intrusion—regardless of the degree of severity, or nature of the event. Given the number of DOD contractors operating with unclassified data, DOD could find itself quickly overwhelmed by its own reporting requirement. It also remains unclear whether this type of information could then be used as part of a contractor's past performance evaluation, or available through the Federal Awardee Performance and Integrity Information System (FAPIIS). A number of industry comments have expressed concern that this information could potentially be used by contracting officers in future source selection processes.

In addition to administrative burdens, the proposed rule imposes significant technical costs on contractors. It would require contractors to preserve and protect images of known affected systems for forensic analysis and preliminary damage assessment. Such imaging, such as off-line storage or maintenance of redundant systems so that the contractor's business will not be disrupted, can be very costly. It also remains unclear whether the related cost of reporting would be deemed reasonable and allowable under the FAR's cost principles.

Yet another unexpected consequence of proposed rule's incident reporting requirement relates to the protection of any ''reported'' data. For example, many contractors store proprietary, third party information. Under the proposed rule, if a contractor experiences a ''reportable incident'' and grants DOD access to review compromised data or to inspect the contractor's system, this could lead to improper release or disclosure of third party proprietary data stored on the contractor's system.

While many large, established DOD contractors will readily accept these potential administrative and financial burdens as the cost of doing business with DOD, the proposed rules could prove to be particularly burdensome to small and mid-sized firms, with limited financial and technical resources.

D. Risk Sharing As stated above, the proposed rule also requires prime contractors to include these requirements to all subcontractors. However, generally prime contractors have little to no control or insight into their subcontractors' IT security protocols. Nevertheless, because there is no privity, or direct legal relationship, between the Government and the subcontractor, the rule leaves only the prime able to ensure that, at every tier, its subcontractors' IT safeguards comply with the proposed rule. This is yet another significant administrative burden which many in industry feel should be shared by both the contractor and DOD.

Given the constant evolution of technology, and the ever increasing sophistication of cyber threats, the only way to ensure that the proposed rule is properly implemented is to ensure that contractors have the proper training, education, updates and resources to defend against cyber attacks and intrusions. However, it remains unclear if or how DOD would share internal training and resources with industry, or whether contractors will be responsible for identifying and investing in such training. This is yet another cost and administrative burden which may need to be borne by both DOD and the contractor.

E. Other Issues Cyber security is of critical importance to ensuring our national security. Cyber threats are constantly evolving and become more sophisticated each day. DOD and other agencies work tirelessly to identify and eliminate these threats using both classified and unclassified techniques and resources. With this rule, DOD seeks industry to be a more integral part of the national defense against cyber crime and terror. However, concerns remain regarding DOD's ''partnership'' with industry in this area.

For instance, private industry is often not privy to the most recent, classified detailed threat information collected by DOD and other Government agencies. This may leave private firms at a strategic disadvantage and limit their ability to defend against the latest cyber threats. Absent detailed cyber threat information, contractors lack critical insight into how best to protect themselves and may be forced to expend time and resources to identify, mitigate and/or report cyber threats that the Government knows exist, but is not prepared to share across industry.

Without these detailed and accurate cyber threat briefings, contractors would be left to expend their own resources to identify and document such threats to their own IT system. Failure to do so could leave a firm exposed to a potential network intrusion, which, under the proposed rule, must be reported to DOD. In sum, the inability to access the most current cyber threat in-

formation could potentially subject contractors to an endless cycle of business costs and compliance risks.

Implementation of the proposed rule may also prove challenging as it seeks to establish a fixed regulatory scheme on ever-changing technology. Over time, data has become increasingly portable, and data networks now includes technologies as cloud computing and Voice over IP (VoIP). However, in contrast to the rapid evolution of hardware, software and virtual technology, the federal rulemaking process is deliberately slow and methodical. Thus, it is unclear whether the language of the proposed rule will be sufficient to ''keep up'' with the technology.

As currently written, the proposed rule also does not contemplate certain unique circumstances which will undoubtedly arise over time. For instance, how will DOD respond when a contractor has ''adequate'' compliance with these cyber security requirements, but then, unexpectedly experiences a network intrusion? Such gray areas have generated concern across the contracting community and have yet to be addressed in detail.

F. DOD's Response to Industry Comments To date, DOD has not yet issued a formal response or report on the comments on the proposed rule. However, given the number of issues and questions industry has raised, it is hoped that DOD will amend the rule to better address these issues. Nevertheless, the fact of the matter remains— threats, missions, technology, and operational environments are constantly changing and both the government and industry face ever-increasing cyber risks in a highly dynamic environment. Whether these proposed rules provide the right answer remains to be seen, but one thing is certain— as with every challenging task, the devil is in the details.

  FCR ISSN 0014-9063