COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
703-875-8059

Defense Acquisition
Regulations System
Attn: Mr. Julian Thrash
OUSD(AT&L)/DPAP(DARS)
3060 Defense Pentagon
Room 3B855
Washington, DC 20301-3060

Re: Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Information (DFARS Case 2008-D028)

CODSIA Case No. 05-10

Dear Mr. Thrash:

The Council of Defense and Space Industry Associations[1] (CODSIA) appreciates the opportunity to provide comments on the advanced notice of proposed rulemaking (ANPR) published in the Federal Register on March 3, 2010, that would add a new subpart and associated contract clauses to the Defense Federal Acquisition Regulation Supplement (DFARS) for the safeguarding, proper handling, and cyber intrusion reporting of unclassified DoD information within industry. Cyber security is vitally important to industry. We applaud DoD for opening a dialogue on this issue and believe there are some good ideas contained in the ANPR. We welcome the opportunity to participate in the discussion concerning how defense contractors can protect DoD information from cyber attacks.

However, CODSIA has four general areas of concern with the ANPR. First, we believe that its scope is too broad in some areas, too narrow in other areas, and many of the definitions are ambiguous and require clarity. Second, we believe that the technical standards cited are too specific. Third, we have concerns about the absence of an unequivocal approach to the provision, use, and protection of the required data as that data is currently classified in the ANPR Fourth, we have concerns about how the

[1] CODSIA was formed in 1964 by industry associations with common interests in federal procurement policy issues at the suggestion of the Department of Defense. CODSIA consists of eight associations – the Aerospace Industries Association (AIA), the American Shipbuilding Association (ASA), the National Defense Industrial Association (NDIA), the Professional Services Council (PSC), the American Council of Engineering Companies (ACEC), TechAmerica, the Chamber of Commerce of the United States, and the Association of General Contractors (AGC). CODSIA's member associations represent thousands of government contractors nationwide. The Council acts as an institutional focal point for coordination of its members' positions regarding policies, regulations, directives, and procedures that affect them. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.

ANPR would be implemented. Finally, in response to the Council's request for comments addressing specific questions in the ANPR, we have included a separate attachment to this letter.

The Scope of the ANPR is Too Broad in Some Areas, Too Narrow in Other Areas, and Definitions are Ambiguous

Our first major concern is with the scope of the ANPR. First and foremost, the ANPR states in 204.7XX2(d)(1) that a contractor will be required to provide a "basic" level of protection for "any DoD information." That term is defined in 252.204-7XXX(a) as "unclassified information that has not been cleared for public release in accordance with DoD Directive 5230.09." Furthermore, the designation procedures in the ANPR at 252.204-7XXX(b)(1) provide essentially that contractors are to assume that all information is DoD information unless otherwise determined by the cognizant DoD activity. This requirement is excessively broad and is not commensurate with a risk-based security system also contemplated by the ANPR. Contractors cannot possibly know what information has been cleared unless DoD marks every piece of information with a legend that indicates whether or not that information has been cleared for public release. Even if every piece of information is marked in such a way as to allow contractors to discern its proper level of classification; however, the requirement to protect all such marked data would be onerous for contractors. It is reasonable to conclude that such a process would easily overwhelm any contractor information system, particularly for small businesses, and dictate a level of virtually unachievable controls. An approach more consistent with the intent of the rulemaking would be to limit coverage to specific sensitive contracts, especially since the technology is dynamic and the appropriate remedies may change.

Second, for those companies that have both military and commercial business, it is essential that the rule establish a definitive process for identifying what needs to be protected and how it needs to be protected. Great caution must be taken in this area. A rule that states or implies that the protections needed for DoD sensitive information must be applied across an entire corporation would be unreasonable, extraordinarily expensive and potentially crippling to the commercial enterprise. Requirements that create substantial administrative and financial burdens on any company that wants to contract directly with DoD or serve as a subcontractor could be a significant barrier to market entry for many commercial companies. This will reduce competition and ultimately limit DoD's access to the full range of innovation developed in the commercial marketplace. This potential burden is contrary to both DoD and Administration initiatives to identify and reduce barriers to federal market entry and engage with more small businesses in the federal acquisition process.

Third, the ANPR defines "adequate security" as protection measures that are commensurate with risk. However, the ANPR at 252.7XXX (b)(3) requires that the "best level of security and privacy available" be used. Notwithstanding the ambiguity of the term itself, the direction to use the "best level of security" is not a risk-based standard, and will have significant adverse impact on small businesses which may not be able to

afford that level of protection, especially when the risk does not justify it. Any DoD initiative in this area should be focused on risk-based solutions.

Fourth, to ensure success in this area, any DoD rule needs to articulate objective, mutually understood, measurable standards of performance. Of greatest importance is a clear set of objective standards defining "adequate security." While we agree that adequate security should be risk-based, how should one judge whether protection measures are commensurate with the identified risks and what exactly is an acceptable risk? Further, there are some examples, such as in the discussion of encryption/storage in the ANPR at 252.7YYY (b)(3)(i), that address only one transmission medium (in the example cited, wireless) and not another (in the example cited, wired). We see no justification for addressing one medium and not others. Additionally, the ANPR includes a number of terms, for example, "appropriate," "adequate," or "prompt," that are subjective. An objective standard for each of these undefined descriptors is needed in order to make these terms meaningful in context.

Finally, cyber security is a national priority for industry and government alike. Since many of our members have contracts with multiple federal agencies, differences in requirements for safeguarding information by defense and civilian agencies will create burdens for contractors and additional compliance cost to the government. A better approach to this issue may be a government-wide FAR rule that is coordinated with key federal agencies and precludes agencies from imposing different substantive identification, handling and reporting information.

Technical Standards are Too Specific

Our second major concern is that many of the requirements in the ANPR are too specific. For example, in the requirements for" basic" safeguarding of information at 252.204-7XXX, the ANPR identifies specific malware protection services (anti-virus, anti-spyware) and specific software upgrades (patches, service packs, hot-fixes). While many companies use these packages, not all do and making these specific services part of the contract may unnecessarily limit a firm's ability to apply a wide range of protective measures suitable to its business or may lead contractors to believe that specific solutions are needed to comply with the requirements of the ANPR.

Any DoD rule should set out an objective standard for risk-based protection and allow for flexibility in meeting the standards. Static standards are unlikely to be able to be reviewed and updated at the pace of innovation. So, reliance on them may actually restrict the adoption of technology to keep pace with threats.

Better Reporting Mechanisms are Needed

The third major area of concern is in reporting. Some contractors have already established voluntary Framework Agreements with DOD to report cyber intrusions into their information systems and other contractors have developed or implemented other mechanisms to combat cyber intrusions for their own business protection. The ANPR

does not address how the rule will fit with a company's voluntary Framework Agreement or other already implemented information protection systems. If the rule is to replace any of those established protocols or protections, a transition plan will be needed. DoD must also align any new rule with the broader government initiative regarding critical unclassified information. DoD's failure to make this alignment risks creating multiple, possibly conflicting, requirements regarding the handling of unclassified information by contactors.

Furthermore, the whole discussion of reporting intrusions is ill-defined. The ANPR policy at 204.7XX2(b) requires contractors to report certain cyber intrusion events. Will compliance with this be required to be included in past performance evaluations? Will information security breaches be considered violations that must be tracked in the Federal Awardee Performance and Integrity Information System? Will contracting officers be required to use this information in future source selection decisions? The ANPR uses general incident type terms rather than specific events that will require reporting. A definition of classes of intrusion (i.e., levels of severity) is needed. The data reported to the government will have to be protected by the government. This is especially true given that most companies have flat networks that contain a mixture of basic, enhanced, proprietary, and third party information.

Finally, the ANPR at 252.204-7YYY(c)(5)(ii) states that contractors will preserve and protect images of known affected systems for forensic analysis and preliminary damage assessment. Notwithstanding the implications of large scale business interruption associated with an intrusion event, this imaging can be very costly and may be impossible for storage area networks or similar systems. Costs will include off-line storage, administrative burden of a 72 hour turnaround, as well as the maintenance of redundant servers so that business will not be disrupted. We note also that, to date, the DoD Damage Assessment Management Office has not completed a number of assessments that have commenced since signing the voluntary Framework Agreements in 2008. Considering that example, DOD should insure prior to implementing any new rule that it has trained and staffed the forensic functions sufficiently to timely accomplish its purposes and, additionally, DoD must make any costs to comply with the rule affirmatively and specifically reasonable and allowable under the Cost Accounting Standards and the cost principles in FAR Part 31.2.

<u>Implementation Requirements are Not Adequately Considered</u>

The final area of major concern is with implementation. The ANPR at 252.204.7YYY(b)(3)(iii) specifies the use of NIST Special Publication 800-53 as the standard for information security controls, tailored in scope and depth appropriate to the effort and information. What is left unsaid is who determines what level of 800-53 to apply (low, moderate, or high) and what constitutes "appropriate?" Could another standard, for example, ISO 27000, be equally effective or more appropriate? If a standard is set, whether NIST 800-53, ISO 27000, or another standard, would contractors be certified as compliant so that when they work as subcontractors to multiple prime contractors, those prime contractors have assurance that appropriate

controls are in place? Self-certification is preferred. Would this certification also apply program by program so that contractors supporting multiple programs are not required to meet multiple definitions of "adequate" from each program's contracting officer? The ANPR does not address what happens when a contractor is found to have adequate compliance but then experiences a network intrusion.

In addition, the ANPR at 252.204-7XXX(c) and -7YYY(f) requires contractors to flow down the safeguarding clause in all subcontracts. However, the prime contractor cannot be liable for a subcontractor's control environment nor for the environment for subcontractors below the first tier where the contractor does not have privity of contract. This ANPR contemplates mechanisms that place the burden of protection solely and squarely on the contractor. DoD must share the risk and responsibility with industry to better protect unclassified information.

Finally, the ANPR is silent on which contracts are affected. Does this requirement include all types of contracts, including commercial contracts and contracts for components or spare parts? We would recommend that the rule apply only to FAR Part 15 contracts with a specified dollar threshold for compliance, and any flow down be limited to first-tier subcontractors.

More Work is Needed Before a Proposed Rule is Published

The ANPR requires extensive rework to address these issues. For example, the ANPR addresses both system protection and handling/releasibility of information. A more manageable approach may be to re-scope any future rule to focus only on system protection and address handling and releasibility requirements in a separate rule.

Conclusion

We appreciate the opportunity to submit these comments. Written responses to the questions posed in the notice accompanying the ANPR are attached. If you have any questions or need any additional information, please do not hesitate to contact Ms. Susan Tonner, the CODSIA project officer for this case, who can be reached at susan.tonner@aia-aerospace.org or at 703-358-1087.

Sincerely,

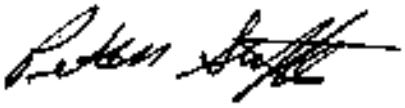
Susan Tonner
Assistant Vice President,
Procurement & Finance
Aerospace Industries Association

Alan Chvotkin
Executive Vice President & Counsel
Professional Services Council

A.R. “Trey” Hodgkins, III
Vice President for National Security
and Procurement Policy
TechAmerica

Cynthia Brown
President
American Shipbuilding Association

Richard L. Corrigan
Policy Committee Representative
American Council of Engineering
Companies



Peter Steffes
Vice President, Government Policy
National Defense Industrial Association

R. Bruce Josten
Executive Vice President, Government
Affairs
U.S. Chamber of Commerce

Attachment:
Response to Questions

ATTACHMENT

ANSWERS TO THE QUESTIONS ASKED IN THE ANPR

1. What is not addressed in the draft clauses that could potentially help industry to feasibly comply with the intent of the clauses?

- Protection levels are not commensurate with the overall risk of unauthorized release of data by type/sensitivity (e.g., FOUO requires enhanced protection, yet this marking is commonly overused).
- DoD needs to provide more specifics around the types of data to be protected, identification of said data types by DoD, and specific protection requirements based on risk level.
- DoD should focus on network and cyber attack threats and vectors and share information to raise awareness of the threat, assuming the intent is to protect data from espionage.
- Changes to any compliance standards during the course of a contract period should be addressed.

2. What part of the draft clauses are viewed as potentially being the most burdensome?

- Basic safeguarding of all DoD data at the enterprise level. Without a clearer distinction between protected DoD information and non-protected information, contractors could potentially be required to report any and all security related incidents involving all systems and data on their networks.
- Enhanced controls for the broad data set defined in the ANPR and enterprise implications.
- Sub-contractor and tiered approach to flow down of requirements and reporting.
- Small businesses compliance.
- Identification and tagging of DoD information and information types throughout enterprise systems and data lifecycle.
- Compliance enforcement at the user level.
- Imaging and Damage Assessment requirements; image retention; legal coordination and compliance; file-by-file and system-by-system data reviews.
- Reporting of “generic” threats to DoD data in 252-204.7YYY(c) (2) (iii).
- Requirement to provide “adequate protection” against network intrusions and data exfiltration without providing a standard by which “adequate protection” can be measured.
- No clear understanding of how to segregate information.

3. What are the potential ways to mitigate burden?

- Focus on high risk espionage threats.
- Limit to Tier 1 contractors and specific contract thresholds.
- Identify specific high-risk data to protect in DoD-specific environments
- Eliminate mandatory Damage Assessment and detailed reporting.

- Limit the scope of “DoD information” to direct and exclusive support of official DoD activities that is not already public.

4. Are there any important information safeguarding aspects that the clauses omit that should be addressed?
- Network and host detection.
- Counter-APT strategies.

5. Do the clauses as written provide clear and adequate guidance to perform safeguarding of DoD information?
- No.
- Requirements are extremely vague; basic controls appear to apply to everything; and enhanced controls appear to apply to nearly all DoD information. The ANPR appears to include protection and reporting well beyond threats to networks (e.g., printouts and peripheral devices).

6. What impact will the reporting requirement in 252.204–7YYY have on small businesses?
- This could be a major problem for small businesses that may not have any dedicated security staff and or the ability to perform analysis to the level indicated.
- When a small business is the prime contractor, there is the potential for the elimination of some small businesses from the competition based on their inability to comply with any similar DFARS requirement.

7. In what ways could DoD minimize the burden of the reporting requirements on respondents, including the use of automated collection techniques or other forms of information technology?
- Focus on highest-risk espionage events.
- Eliminate reporting time requirement (72 hours).
- Eliminate need to report on individual program and file information or provide automated technologies to identify such data.
- Eliminate speculative reporting.

8. What are industry best practices for cyber security?
- Information and intel sharing.
- Focus on detection and response capabilities vs. controls.
- E-mail scanning.
- Local admin removal.
- Multi-factor authentication.
- Virtual browsing.
- Authenticated proxies with strong restrictions.
- Packet capture and intrusion detection monitoring.
- Host-based intrusion prevention system (HIPS).
- Signature-based instead of behavior-based detection and blocking.

9. Should the Government establish standard information assurance criteria for all contractors as a condition of award (e.g., strong passwords, virus protection)? If so, are there existing international/national standards that should be cited or considered in building the criteria and what impediments exist to achieving this goal?

- No. FISMA and similar approaches have proven to add little to no value to the overall security posture. Focus on counter-APT strategies and awareness.
- If standards are to be used, follow commercially-accepted, international standards (e.g., ISO 27001).

10. Would it reduce the burden without reducing effectiveness for contractors and subcontractors if the ‘‘basic’’ clause were replaced with an Online Representations and Certifications Application (ORCA) certification?

- No. The only difference would be certification to Basic controls.

11. Would it result in a more accurate cost management strategy if the ‘‘enhanced’’ clause were split into a safeguarding plan/program clause and a reporting clause?

- No. Cost management would be more effective if enhanced requirements were applied to specific identified DoD data and limited to enclaves within the network.

12. If a contractor believes that it would have significant difficulty implementing these requirements in-house, could it out-source its information technology to a firm with specific competency in this area? If not, what are the barriers to doing so?

- Yes it is possible; however, it would come at a significant cost for third party services and reengineering of existing DoD contractor business processes and information systems.

13. Are there any additional safeguarding or restrictions that should be implemented to protect information reported or otherwise provided to the Government under the ‘‘enhanced’’ clause?

- Exemption from public release (FOIA).
- Named access to attribution information, limited to on-site at DC3.
- Specify handling and destruction requirements for DoD.