The Coalition for Government Procurement

October 23, 2012

Subject: FAR Case 2011-020; Basic Safeguarding of Contractor Information Systems

The Coalition for Government Procurement (Coalition) appreciates the opportunity to comment on the above referenced case. The Coalition is a non-profit association of firms selling commercial services and products to the Federal government. Our members collectively account for approximately 70% of the sales generated through the General Services Administration's (GSA's) Federal Supply Schedule (FSS) program and about half of the commercial item solutions purchased annually by the Federal Government. Coalition members include small, medium and large business concerns. The Coalition is proud to have worked with Government officials over the past 30 years towards the mutual goal of common sense acquisition.

1. Summary of the Rule

The subject rulemaking proposes to amend the Federal Acquisition Regulation (FAR) to include requirements for safeguarding contractor information systems that contain non- public information provided by or generated for the Government that will reside on or transit through contractor information systems. The proposed rule would add a new FAR subpart 4.17 and contract clause 52.204-XX, Basic Safeguarding of Contractor Information Systems. DoD, GSA, and NASA have concluded that these requirements are an extension of the requirements, under the Federal Information Security Management Act (FISMA) of 2002, for Federal agencies to provide information security for information and information systems that support the operations and assets of the agency, including those managed by contractors.

The requirements of the proposed rule apply to virtually all government contractors that receive or generate non-public information on behalf of the Government.

1990 M Street NW
Suite 450
Washington, DC 20036

Phone: 202.331.0975
Fax: 202.822.9788
www.thecgp.org

- FAR subpart 4.1702 applies to: "all solicitations, contracts (including orders and those for commercial items and commercially available off-the-shelf items)
- FAR subpart 4.1703 requires that the proposed clause be inserted in solicitations or contracts above the simplified acquisition threshold under which the contractor or ***subcontractor*** at any tier may have non-public information provided by the Government or generated for the Government on their information systems . The clause may also be used in contracts below the simplified acquisition threshold when the contracting officer determines that inclusion of the clause is appropriate.
- Paragraph c of the proposed clause 52.204-XX Basic Safeguarding of Contractor Information Systems. Requires the prime to include the substance of the clause in relevant subcontracts.

The proposed rule outlines specific safeguarding requirements for:

- Public computers and websites
- Transmission of electronic information
- Voice and fax transmissions
- Physical and electronic barriers
- Media sanitization
- Intrusion protection
- Transfers to subcontractors

2. Impact of the Rule

The introductory language of the proposed rule states that the cost of this rule making is insignificant because it requires first level protective matters that are typically employed as part of the routine course of doing business. We disagree with the government's assessment. Our members have concluded that the rule suffers from a lack of clarity. The requirements for information security can be interpreted in various ways. The audience of contractors to whom the rule applies is very broad. The lack of clarity imposes significant risks of disputes and

noncompliance on both government and industry. If this rule is adopted government contractors must review their systems, and procedures to determine if their systems are adequate and to make changes if they are not. A realistic review can be conducted only where there are clear standards. In this case the standard is not clear. The lack of clarity itself increases costs since a contractor must design processes to the most stringent standard in an attempt to assure compliance. The risks and costs to contractors is exacerbated by the fact that prime contractors must flow down the requirements to subcontractors. Further, paragraph (b) (7) of the clause provides that a contactor may transfer information covered by the rule to only to subcontractors that provide at least the same level of security specified in the clause. This provision puts the contractor in the position of not only determining compliance of its own systems but compliance of subcontractor systems as well.

3. Proposed Changes to the Rule

There are significant terms that require clarification, least they give rise to disputes.

A. Section 4.1702 provides that the subpart applies when a "contractor's information system may contain information provided by or generated for the Government (other than public information). The scope of the term "generated for the government" is not clear. Most Coalition members are GSA Schedule contractors. As a part of the evaluation process, and as a part of contract administration, Schedule contractors generate information about their own proprietary commercial practices and submit that information to the government. It is not clear whether this type of evaluation information is covered by the rule or rather that "generated for the government" applies to information that is a part of a contract deliverable. We recommend that this term be defined.

B. Paragraph (b) (2) of contract clause provides when transmitting electronic information that contains non-public information provided by or generated for

the Government, the contractor must use "…technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment." This standard is subject to various interpretations. For example is it the best available based on currently available technology? the best available at the contractors facility? We recommend that the government clarify the standard of security required.

C. When transmitting non-public information provided by or generated for the Government, contractors may only transmit via voice or fax when "the sender has a reasonable assurance that access is limited to authorized recipients". The rule is not clear as to what constitutes "reasonable assurance" and we recommend clarification.

D. When non-public information provided by or generated for the Government is not under direct individual control, such information must be protected by at least one physical barrier and one electronic barrier. We note that this provision may philosophically conflict with government and commercial efforts to create and accommodate a mobile workforce. The broader the applicability of the proposed rule, the more difficult it will be to reconcile these two federal priorities.

4. Summary

Our members acknowledge that information security is a shared priority of industry and government. The rule as drafted, however, poses significant implementation problems. Essential terms need to be defined or clarified to permit rational implementation and reduce the risk of non-compliance on the contractor community. The introductory language of the proposed rule suggests that the Government's intent in drafting this rule was to require first level protective strategies that are typically employed as a routine course of doing business. Until the government is capable of more specifically stating a standard of information security, we suggest that the proposed clause simply state that information security is a high priority of the government and at a minimum the contractor shall protect information provided to or generated for the government

at a level no less than what the company provides for its own confidential and proprietary business information.

Sincerely,

Roger Waldron