

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

October 23, 2012

General Services Administration
Regulatory Secretariat (MVCB)
1275 First Street, N.E.
7th Floor
ATTN: Hada Flowers
Washington, DC 20417

Re: FAR Case 2011-020; *Basic Safeguarding of Contractor Information Systems*; 77 Fed. Reg. 51,496, August 24, 2012

Dear Ms. Flowers:

The Council of Defense and Space Industry Associations (“CODSIA”)¹ is pleased to submit these comments in response to the proposed rule dated August 24, 2012 (77 FR 51496; the “Proposed Rule”) issued by the Department of Defense, the National Aeronautics and Space Administration, and the General Services Administration (collectively, the “FAR Council” or the “Council”) in Federal Acquisition Regulation (“FAR”) Case 2011-020.

The Proposed Rule would add a new FAR Subpart 4.17 and associated contract clause intended to require certain “basic safeguarding” for contractor information systems where information provided by or generated for the Government will reside on or transit through those systems. The *Federal Register* notice accompanying the Proposed Rule defines “basic protection measures” as “first-level information technology security measures used to deter unauthorized disclosure, loss, or compromise.” 77 FR at 51496. The Proposed Rule would impose the safeguarding requirements through a new contract clause, FAR 52.204-XX, *Basic Safeguarding of Contractor Information Systems*, which it would prescribe for all solicitations and contracts above the simplified acquisition threshold when the prime contractor or any subcontractor at any tier “may have” information provided by or generated for the Government residing on or transiting through its information systems. See 77 FR 51498 (proposed FAR 4.1703).

¹ CODSIA currently consists of six industry trade associations and thus represents the comments of thousands of federal government contractors nationwide on acquisition policy issues. A CODSIA comment letter is not a letter from a single organizational entity but from thousands of affected stakeholders. This unique status as the conveyor of regulatory comments for some of the largest trade associations working on acquisition policy also represents the collective expertise of these associations and the companies they represent.

It also directs each contracting officer to address how government information will be protected as part of the planning for each acquisition. We applaud the Council for publication of the FAR rule as a proposed rule with sixty days to prepare comments.

We fully appreciate the need for the Government and its contractors to implement reasonable measures to protect sensitive, non-public government information wherever it resides. We also understand that implementing any requirement related to the safeguarding of government information involves a delicate balancing of various considerations, including but not limited to the sensitivity of the information at issue and the cost and burden associated with implementing safeguarding measures. We submit that the Council's attempt to strike a balance with these proposed requirements is askew in several ways. This government-wide rule would be imposed on virtually every contract (including contracts for commercial items and commercial off-the-shelf items), on virtually every federal contractor (and subcontractor) regardless of size or the nature of the federal transaction and contains a subset of information protection requirements that is derived from an earlier discredited Defense Department regulation on protecting unclassified information and contains several of the same issues and challenges that we found in that initiative.² The rule effectively sets minimum security standards for the networks of all federal contractors and subcontractors and should be promulgated and evaluated as such, not as a contractual requirement.

As discussed below, the Proposed Rule would cast far too broad a net in terms of the information that contractors and subcontractors would be required to safeguard and imposes an imprecise, continually evolving and potentially conflicting set of requirements. The proposed regulations would force companies to apply these imprecise safeguards to nearly all information obtained or generated by any contractor under any government contract or subcontract. Much of the information that is "generated" by a contractor is never transmitted outside the contractor's systems but would be subject to the coverage of the rule. Additionally, the nature of the specific safeguards is not reasonably calibrated to accomplish the stated purpose of protecting government information. In some cases, the proposed requirements are likely to be ineffective, and in other cases, the requirements are simply unrealistic, unachievable and potentially counterproductive.

A. The Council should clarify the scope of "information" and "information systems" to which the basic safeguarding requirements apply.

As the Proposed Rule is drafted, the scope of contracts and information under those contracts that would be subject to the requirements is very broad. The Proposed Rule

²CODSIA's comments on the DFARS rule were submitted on December 16, 2011 and are available at <http://www.regulations.gov/#!documentDetail;D=DARS-2011-0052-0051>.

would prescribe FAR 52.204-XX for nearly all procurements.³ The clause would require that the covered contractor implement certain “basic” safeguarding measures to “protect **information** provided by or generated for the Government (other than **public information**) which resides on or transits through its **information systems** from unauthorized access and disclosure.” 77 FR at 51499 (proposed FAR 52.204-XX(b) (emphasis added)). The clause would define “information” as “any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.” It would define “information system” as “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information,” and would define “public information” as “any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public.” 77 FR at 51499 (proposed FAR 52.204-XX(a)).

We are concerned that the reach of the Proposed Rule is overly and unnecessarily expansive. The definition of “information” is extremely broad and subject to almost no limit. The one carve out built into the clause is for “public information,” but that definition is narrow because it requires the actual disclosure, dissemination or making it available to the public. In essence, the regulation instructs every business with a government contract or subcontract to provide the same protection to information that would be released in response to a FOIA request as information that would be extremely valuable to US adversaries but is not so sensitive that it was classified. Thus the “public information” carve out does little to address concerns about the scope of the information that would be subject to these requirements. Furthermore, it will be nearly impossible for contractors to keep track of information that has been made public and which no longer needs or requires protection on the contractors’ network. Significant additional expense could be incurred by contractors and subcontractors protecting data that has been made public.

While we hope that the Council did not intend the requirements to have such a broad sweep, if the scope of 52.204-XX were to be adopted as proposed, the clause’s safeguarding requirements, as a practical matter, would apply to nearly all information and all information systems (including information captured on paper and paper systems, voicemails and fax transmission, and information residing on mobile devices) of any company that holds even a single government contract or subcontract. Such a regime is unnecessary and would be unduly costly and burdensome to both agencies and contractors and cannot practicably be implemented.

We strongly recommend that the Councils revise the rule to narrow the scope of information that is subject to the “safeguarding” requirements so that the scope coincides with the type of information for which safeguards are warranted based on a

³Although the clause is not required to be prescribed for procurements below the simplified acquisition threshold, contracting officers would have discretion to do so and we would expect the automatic contracting writing systems to default to including this clause in such solicitations and resulting contracts.

reasoned risk assessment and cost-benefit analysis. Such a narrowing would necessarily involve marking by the Government of any relevant information to be protected or at least identifying categories of information that must be protected, rather than the current blanket approach used in the proposed rule. This process must also involve some reasonable tailoring of the definitions of the “information” and “information systems” that are consistent with previously enacted definitions (e.g. DoD DIB) and are subject to those requirements. The Council should also expand the definition of “public information” to include information that would be subject to disclosure to the public under FOIA.

B. The Council should revisit each of the specific “basic safeguarding” requirements.

In the Regulatory Flexibility Act analysis accompanying the Proposed Rule, the Council states that “[t]he resultant cost impact is considered not significant since the first-level protective measures (*i.e.*, updated virus protection, the latest security software patches, etc.) are typically employed as part of the routine course of doing business.” 77 FR 51497. While many companies rely on certain of these safeguarding techniques to protect their information and information systems, it is an overstatement and an overgeneralization to suggest that companies “typically” implement *all* of these measures for *all* information.⁴ For more sensitive information, most companies will employ measures that go far above and beyond these proposed safeguarding requirements. In some cases, as discussed below, companies will make thoughtful, reasoned decisions not to implement some of these safeguards based on the conclusion that they will not provide additional protection and/or could weaken a company’s information systems. The following highlights some of our concerns about the specific safeguarding requirements that the Proposed Rule would impose.

First, some of the safeguarding requirements are too basic and rudimentary, and as such, may undermine the Proposed Rule’s intended purpose to “protect against the compromise of contractor computer networks on which information provided by or generated for the Government (other than public information) that will be resident on or transiting through contractor information systems.” 77 FR 51497. One example is the proposed requirement related to intrusion protection. See 77 FR at 51499 (proposed FAR 52.204-XX(b)(6)). The only proposed intrusion-protection safeguards relate to malware protection services and security-relevant software upgrades. These types of safeguards are generally not considered sufficient to provide a reasonable level of protection in a sophisticated enterprise environment. We are concerned that the rule

⁴The Council’s suggestion that the proposed safeguards are “typical” and will not have a significant cost impact calls into question whether the review of the Proposed Rule was meaningful. As discussed herein, due to the sweeping scope of “information” that would be subject to the requirements, the Proposed Rule would create substantial costs for government contractors and subcontractors and will be particularly burdensome for small businesses. CODSIA intends to also submit comments under the Regulatory Flexibility Act that will raise serious questions about the purpose of the proposed requirements and the attendant costs and other repercussions.

would suggest to companies that the identified protections are all that it is needed – not only contractually but also to protect their information systems from intrusion. We do not believe that is the case and such thin requirements are counterproductive.

Second, some of the safeguarding requirements are ambiguous. For example, proposed clause 52.204-XX would require that contractors and subcontractors “[t]ransit email, text messages, blogs, and similar communications that contain information provided by or generated for the Government (other than public information) using technology and processes that provide the **best level** of security and privacy available, given facilities, conditions, and environment.” 77 FR 51499 (proposed FAR 52.204-XX(b)(2) (emphasis added)). The use of the phrase “best level” is ambiguous and it does not have any common meaning in this area. If applied literally, this requirement would have significant consequences, including precluding contractors and subcontractors subject to 52.204-XX from using any type of mobile computers or smart phones (including Blackberries, Android phones, Windows phones, iPhone, and other similar devices), as those mobile technologies do not have the same levels of security and privacy as fixed systems. If the “best level” is required, then technologies that cannot meet that standard, such as mobile technologies, would be non-compliant even if they employ the best available protections for that communications platform. Moreover, it appears that the determination of “best level” may be a sliding standard that varies based on the situation, including the contractor’s or the Government’s “facilities, conditions, and environment.” We support the use of flexible safeguarding standards that vary based on the context, including such variables as the type of contract and the type of information being protected (e.g., at least partial carve outs for commercial item contracts), but we are concerned that the proposed regulatory language is far too vague and there is nothing in the proposed regulation or the accompanying commentary to explain how this sliding standard would be applied. Moreover, the requirement to use the best level of security means that all information is treated identically in this regard resulting in a situation where the most sensitive information will only get the same treatment as the least sensitive. Businesses seeking to upgrade communications security will need to scale the upgrade to handle all government data even if the more sensitive data could be made more secure for less cost sooner if the contractor could treat transmission of more sensitive data differently.

Third is the vague restriction in 52.204-XX that covered information can be transmitted orally “only when the sender has a **reasonable assurance** that access is limited to authorized recipients.” 77 FR 51499 (proposed FAR 52.204-XX(b)(3) (emphasis added)). The Proposed Rule would impose this “reasonable assurance” restriction effectively on all oral communications of all “information” as it is defined under the rule. Yet it provides no explanation of the Government’s expectations. There are similar problems with the requirement to implement physical and electronic barriers for all “information” in hard copy form not under a specific individual’s “control.” 77 FR 51499 (proposed FAR 52.204-XX(b)(4) (emphasis added)). For example, in the area of physical and electronic barriers, it is not clear if having devices and information encryption meets the need to have devices locked when not under direct supervision.

Could the rule require that every work station and laptop a contractor owns be locked in a room or drawer when not in use even when at home or in a building with access controls? Would companies be required to go through a secure third party to send RFP content or responses via email to the government to comply with this rule? If so, it is our belief that the government should not want the unintended consequence of inhibiting fair competition because it could not communicate with all potential competitors.

Fourth, some of the proposed safeguards are inconsistent with customary commercial practices and could potentially increase the vulnerability of contractor information systems. For example, the proposed clause would require “[p]rompt application of security-relevant software upgrades, e.g., patches, service-packs, and hot fixes.” 77 FR 51499 (proposed 52.204-XX(b)(6)(ii)). This requirement is too inflexible. In some cases, companies do not upgrade to the most recent software upgrade as soon as it is available for many legitimate reasons. For instance, implementation may be delayed because even the upgrade has glitches, the previous version is more stable or there are other operational implications that interfere with the company’s ongoing business. Most companies will refuse to implement software upgrades until the implications for their corporate enterprises (including commercial work) can be assessed. Moreover, security upgrades can be bundled with other upgrades that the business may not want or that contain other security vulnerabilities. These considerations apply in a significant number of situations that the rule ignores. That is why the Proposed Rule’s requirement to adopt all security-relevant upgrades, regardless of other considerations, is unreasonable and should be revised to give companies discretion to determine how best to maximize its security protections through software upgrades while still maintaining its normal operations.

Fifth, we are concerned that section 4.1702 prescribes these same requirements on solicitations – thus imposing this requirement as a barrier to even bidding on government work such that every business that wants to bid on government work must ensure its networks meet the requirements (or invest further if they do not) before the business will be eligible for any contract revenue. As a practical matter, if the FAR Council intends to impose these requirements on every bidder, it should make compliance part of the CCR process although we do not support such an approach. This further highlights the lack of clarity around this portion of the rule as it is unclear how the government or respondents can communicate with each other over email.

Sixth, the proposed addition of 42.302(a)(21) requires the contractor to have “protective measures” in place, consistent with the clause but the clause doesn’t use the term “protective measures.”

Finally, the proposed rule does not adequately address the need for government to proactively mark protected materials; instead it puts the onus on the contractor to create safeguards. CODSIA believes that a fundamental requirement for the protection of unclassified information is that the data must be identified and marked by the Government. The proposed rule places no requirements and creates no responsibilities

for the Government to appropriately mark any unclassified programmatic information. This absence of a requirement for the Government to identify the information that it deems critical and worthy of additional protections means that contractors will be required to protect all information related to any contract. Because of the lack of clarity in the proposal's definitions, the proposed rule will be essentially impossible to implement without a process for marking. Accordingly, we recommend that the Government establish, as part of the regulatory requirements, responsibilities for the Government at the program level to appropriately mark all data that requires enhanced protections, as well as clearly define how contractors will be able to discern what data they have collected, developed, received, transmitted, used or stored that must also be protected. A model for this protocol may be found in the National Industrial Security Program Operating Manual, which specifies which information created by the contractor does not require additional interaction with the program manager and clearly delineates how a contractor must handle that data.

All of these issues are significant and must be addressed before the Council issues an interim or final rule that would impose specific safeguarding requirements on contractors and subcontractors. The Council should consider adopting a "performance standard" for protecting specific types of information from unauthorized disclosure rather than the "design standard" included in this Proposed Rule, and engage more fully with industry and other stakeholders to assess the appropriate safeguards to accomplish the stated goals of the Proposed Rule.

C. The Council should limit contracting officer discretion to impose unique requirements on a contract-by-contract basis.

The Proposed Rule would amend FAR 7.105 to impose the requirement for contracting officials developing a written acquisition plan to address information protection. Specifically, it would add, among other things, a statement that "[f]or acquisitions that may require information provided by or generated for the Government (other than public information) to reside on or transit through contractor information systems, discuss how this information will be protected (see subpart 4.17)." 77 FR 51498.

CODSIA does not support this provision and instead believes that requirements for information protection systems must be established on a uniform governmentwide basis so that contractors do not have conflicting guidance on systemic security minimums. If some information on certain projects needs more secure handling but does not qualify for classification, the government needs to establish categories for the information and each contracting officer needs to designate the appropriate category for information being provided the contractor. Allowing each contracting officer to set minimum system security standards, which seems to be allowed under the proposed rule, will lead to chaos. The exercise of such authority in the past has led to the development of literally hundreds of classifications and an unmanageable information systems. In fact, industry believes that this element of the proposed rule contradicts Executive Order 13556 on "Controlled Unclassified Information." This rule should not recreate problems of the

past but instead direct contracting officers to identify applicable government-wide security criteria to ensure information is properly handled during contract performance.

D. The order of precedence provision in 52.204-XX is helpful, but it does not address the problems associated with conflicting standards.

The Proposed Rule states that the contract clause, 52.204-XX, is “subordinate” to any other contract clause or requirement that specifically addresses the safeguarding of information or information systems, and in the event of an inconsistency or conflict, the other clause or requirement takes precedence. See 77 FR 51499 (proposed 52.204-XX(d)). We commend the Council for including this “order of precedence” guidance. Because the safeguarding requirements in 52.204-XX are basic and general, it makes sense that other security requirements would take precedence when they conflict. We are concerned, however, that this language is not sufficient, standing alone, to address the potential problem associated with conflicting standards and that contracting officials would not normally possess the training and skills necessary to understand the technical nature of such conflicts and would not know how to address these types of issues when they arise. For example, where the acquisition strategy identifies that a contract will provide access to national security information, the contracting officer must have the authority to modify this “basic safeguarding” clause. To the extent the FAR Council allows contracting offices or contracting agencies to set differing network security standards, the FAR Council must also provide authority for the contractor who is subject to differing standards for safeguarding information or information systems to have the responsibility for determining how the contractor's system reconciles these multiple requirements. Furthermore, it is not clear how to address situations where one security standard is not clearly more secure than another, so requiring the contractor to apply the most secure will not provide adequate guidance. Finally, it must be recognized that requiring the choice of a standard would require locking a contractor's network into that particular set of technical requirements because costs and operational issues will limit the ability to make potential adjustments to meet a different standard.

E. The Council should revise the regulation relating to a purported non-compliance.

The Proposed Rule would inject information security into contract compliance in a way that goes beyond anything contemplated by the FAR in the past. For example, we are concerned that the imprecise nature of the compliance requirements imposed by the Proposed Rule and any inadvertent release of information could be turned into not only an information security issue but also a potential breach of contract. Yet the Proposed Rule does not indicate how the Government will address a situation in which an agency believes that a contractor is not in compliance with the requirements in proposed 52.204-XX. We recommend that the Council revise the rule to make clear that an

information release or other noncompliance, without more, does not provide a basis to terminate the contract for default or to withhold contract payments.

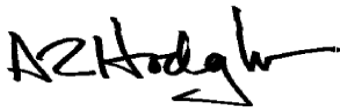
F. The Council should revise the regulation to state that prime contractors are not responsible for policing subcontractors' information systems.

The Proposed Rule would require that prime contractors subject to 52.204-XX flow down that clause to all subcontractors that may have information provided by or generated for the Government (except public information) residing in or transiting through their information systems. See 77 FR 51499 (proposed 52.204-XX(c)). In addition, proposed 52.204-XX(b)(7) imposes restrictions on the transfer of information only to those subcontractors that “both require the information for purposes of contract performance **and** provide at least the same level of security as specified in the clause” (emphasis added). We have concerns with the scope of the flow-down obligation because it would be coextensive with the definition of “information,” which, as discussed above, is overly broad and subject to almost no limits. In practice, the flow-down requirement would likely extend to all subcontracts for commercial items and commercially-available off-the-shelf (“COTS”) items and even to small dollar value sub-awards.

Even more troubling, however, is the possibility that prime contractors will be held responsible for policing all subcontractors for compliance with the safeguarding requirements and could be held liable for any non-compliance with the imprecise requirements or information releases by their subcontractors. This would be an unworkable framework with domestic subcontractors, and especially so in the case of non-U.S. subcontractors and the extreme difficulty in enforcing these standards with them. We recommend that the Council revise the proposed rule to state explicitly that prime contractors are not required to police subcontracts beyond flowing down the contract clause, that prime contractors and higher tier subcontractors are able to rely in good faith on a statement from their subcontractor that the subcontractor is in compliance with the basic safeguarding requirements, and that primes and higher tier subs are not liable for a subcontractor's noncompliance with the basic safeguarding requirements or any unauthorized release of information.

CODSIA appreciates this opportunity to comment on the Proposed Rule and we welcome the opportunity to meet with the Council and/or its experts to discuss these comments further. We would be pleased to respond to any questions the Council may have on these comments. Trey Hodgkins of TechAmerica serves as CODSIA's project leader and can be reached at 703-284-5310. Bettie McCarthy, CODSIA's administrative officer, can serve as an additional point of contact and can be reached at 703-875-8059.

Respectfully submitted,



A.R. "Trey" Hodgkins, III
Senior Vice President
Global Public Sector
TechAmerica



Alan Chvotkin
Executive Vice President & Counsel
Professional Services Council



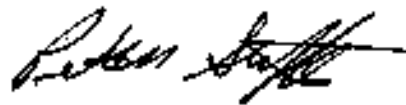
Bill Greenwalt
Vice President, Acquisition Policy
Aerospace Industries Association



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



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



Peter Steffes
Vice President, Government Policy
National Defense Industrial
Association

