



NOV 30 2005

GSA Office of the Chief Acquisition Officer

MEMORANDUM FOR DAVID CAPITANO
DIRECTOR
DEFENSE ACQUISITION REGULATIONS COUNCIL

FROM: RALPH J. DESTEFANO, DIRECTOR
REGULATORY AND FEDERAL ASSISTANCE
PUBLICATIONS DIVISION

SUBJECT: FAR Case 2004-018, Information Technologu Security

Attached are comments received on the subject FAR case published at 70 FR 57449; September 30, 2005. The comment closing date was November 29, 2005.

<u>Response Number</u>	<u>Date Received</u>	<u>Comment Date</u>	<u>Commenter</u>
2004-018-1	11/02/05	11/02/05	Karen R. Kibble
2004-018-2	11/17/05	11/17/05	EPA
2004-018-3	11/29/05	11/29/05	Sungard Availability Services
2004-018-4	11/29/05	11/29/05	NDIA
2004-018-5	11/29/05	11/28/05	Coalition of Journalists for Open Government

Attachments

2004-018-1



Karen.Kibble@bpd.treas.gov

11/02/2005 02:01 PM

To farcase.2004-018@gsa.gov

cc Sheila.Aldsworth@bpd.treas.gov

bcc

Subject Request for Comments - FAC 2005-06, FAR Case 2004-018

The Bureau of the Public Debt submits a "No Comments" response for the subject data call.

Karen R. Kibble
IT Program Specialist
304-480-7580
karen.kibble@bpd.treas.gov



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

2004-018-2

NOV 17 2005

General Services Administration
Regulatory Secretariat (VIR)
1800 F Street, NW, Room 4035
ATTN: Laurieann Duarte
Washington, DC 20405

OFFICE OF
ADMINISTRATION
AND RESOURCES
MANAGEMENT

Dear Ms. Duarte,

Thank you for the opportunity to comment on the interim rule to amend Parts 1, 2, 7, 11, and 39 of the Federal Acquisition Regulation (FAR) regarding the implementation of the information security provisions of the Federal Information Security Act of 2002 (FISMA). The Environmental Protection Agency (EPA) has reviewed the interim rule, FAR Case 2004-018, published in the Federal Register on September 30, 2005. We support the interim rule and encourage the Councils to move forward with implementation of a final rule.

We offer the following comments for your consideration:

- The term "Sensitive But Unclassified Information (SBU)" is defined in the definition of Words and Terms section, Part 2. However, the use of the term is not found in the text of the interim rule. Please consider deleting the term or adding language to support the definition. We believe use of the term SBU implies that a definition for *sensitive and classified information* should also be included.
- Although, the FAR clause at 52.239-1(b) is not included in this interim rule, revisions to the clause in this interim rule would be beneficial to support contractor requirements regarding specific security programs that satisfy FISMA. Please consider including revisions to FAR 52.239-1(b) in the interim rule to include security programs under FISMA. We recommend the following revisions to FAR 52.239-1(b):

To the extent required to carry out a **security program under FISMA** and a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases, **and shall support security program implementation, evaluation and reporting as described in 44 U.S.C. 3544 (b).**

2004-018-2

- 2 -

If you have questions or require additional information, I can be reached on (202) 564-4315, or you may contact Brian Long in our Policy and Oversight Service Center on (202) 564-4737 (long.brian@epa.gov).

Sincerely,



Ronald L. Kovach, Director
Policy, Training and Oversight Division

2004-018-3



James.Poffel@sungard.com

11/29/2005 04:52 PM

To farcase.2004-018@gsa.gov

cc Joan.Nazarene@sungard.com

bcc

Subject 2004-018

The new FAR regulation is stimulating among the suppliers looking to maximize their security offerings & data center offerings. The new FAR deems a focus on compliance with the Federal Information Security Management Act (FISMA), enterprise security architecture development, and security procurement. A major issue is the lack of recognition of a simple process that can be adopted by all agencies to allow for suppliers to leverage their facility & personnel clearances across multiple Federal agencies.

Elevating the importance of information security to the level of a national security priority is something we must do. The major issue is however, the FAR regulation inhibits those still struggling to obtain or be sponsored for clearances. The winners are those suppliers who have clearances today and this may stifle acquisition competition

Regards,
Jim Poffel
Alliance Program Manager-Public Sector
SunGard Availability Services
505 Huntmar Park Drive
Suite 100
Herndon, VA 20170

(703) 326-4980 Tel
(410) 882-3566 Mobile
(703) 326-4929 FAX

james.poffel@sungard.com
www.sungard.com



2004-018-4

2111 Wilson Boulevard, Suite 400
Arlington, Virginia 22201-3061
Tel: (703) 522-1820 • Fax: (703) 522-1885
Web page: <http://www.ndia.org>

The Voice of the Industrial Base

November 29, 2005

General Services Administration
Regulatory Secretariat (VIR)
ATTN: Laurieann Duarte
Room 4035
1800 F Street, N.W.
Washington, DC 20405

Ref: FAC 2005-06, FAR Case 2004-018: Information Technology Security

Dear Ms. Duarte:

The National Defense Industrial Association ("NDIA") is pleased to submit these comments on the interim FAR rule that adds provisions related to implementation of the Federal Information Security Management Act of 2002 ("FISMA") (Title III of the E-Government Act of 2002).

NDIA is a non-partisan, non-profit organization with a membership that includes 1,150 companies and over 38,000 individuals. NDIA has a specific interest in government policies and practices concerning the government's acquisition of goods and services, including research and development, procurement, and logistics support. Our members, who provide a wide variety of goods and services to the government, include some of the nation's largest defense contractors.

NDIA supports the interim rule, which seeks to ensure that, in furtherance of FISMA, Federal contracting officials and other personnel involved in the acquisition of information technology ("IT") goods and services consider information security as an important factor throughout the acquisition lifecycle. And we agree with the observation of the CAA and DAR Councils, in the preamble to the interim rule, that "[s]ince FISMA requires that agencies establish IT security policies that are commensurate with agency risk and potential for harm and that meet certain minimum requirements, the real implementation of this will occur at the agency level." 70 Fed. Reg. 57450 (Sept. 30, 2005). We feel it is essential, however, that in implementing information security requirements for contractors, each agency strive for an approach that, to the maximum extent practicable, leverages its contractors' existing policies and practices and is also consistent with the approach of other Federal agencies.

The Federal government is not alone in viewing the need to secure confidential or proprietary information from theft or other unauthorized access as a top priority. During the past two years, there have been a number of well-publicized incidents in which companies in industries as diverse as banking and consumer credit, manufacturing and retail have fallen victim to computer hackers or others who managed to gain unauthorized access to non-public data regarding the companies' business operations, customers or employees. These incidents vividly demonstrate how recent advances in technology have increased the vulnerability of information that is stored or transmitted electronically, and many companies have responded by devoting significant time, energy and resources to reviewing their existing approaches to computer and network security and implementing new measures designed to better protect their non-public information from unauthorized access or disclosure. In developing information security policy and requirements applicable to their contractors, we believe agency policymakers should be mindful of the

"Publishers of National Defense Magazine"

recent steps taken by those in private industry, and they should seek to leverage the additional security measures many companies already have adopted by allowing those measures to serve as the foundation for ensuring the protection of non-public agency information that a contractor may possess or control.

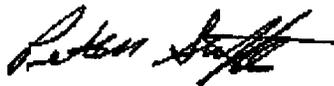
In addition, policymakers should aim for requirements that are as uniform and consistent as possible. While we agree with the Councils that “agency-specific policy and implementation will evolve differently across the spectrum of Federal agencies, depending on their missions,” *id.* at 57450, it is important that in developing its own policy each agency proceed from a common baseline of requirements or standards – an observation that the Government Accountability Office (“GAO”) recently offered in a report issued earlier this year. *See* Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk, GAO-05-362, at 24-25 (April 2005). In response to the GAO’s report, the Department of Commerce, which oversees the National Institute of Standards and Technology (“NIST”), the agency charged with developing standards and guidelines for the implementation of FISMA, advised that it would work to “build the necessary framework for a more consolidated delivery of [] contractor related guidelines.” *Id.* at 31. In keeping with the GAO’s recommendation and the Commerce Department’s response, we believe the interim rule should be revised to place greater emphasis on the importance of agencies adhering to the NIST framework and guidelines when developing information security policies and requirements for agency contractors.

For the reasons discussed above, we recommend that FAR 39.101(d) be revised to read as follows:

“(d) In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements. The security policies and requirements included by agencies shall (i) be consistent with applicable guidelines provided by the Commerce Department’s National Institute of Standards and Technology, and (ii) to the maximum practicable extent, accommodate contractors’ existing policies and practices for preventing the unauthorized access or disclosure of non-public information.”

We appreciate the opportunity to comment on the proposed rule. If you need additional information, please contact NDIA Procurement Division Director Ruth Franklin at (703) 247-2598 or rfranklin@ndia.org.

Sincerely,



Peter M. Steffes
Vice President, Government Policy

2004-018-5



no-reply@erulemaking.net
11/28/2005 06:03 PM

To farcase.2004-018@gsa.gov
cc
bcc
Subject Public Submission

Please Do Not Reply This Email.

Public Comments on Federal Acquisition Regulation; Information Technology Security:=====

Title: Federal Acquisition Regulation; Information Technology Security
FR Document Number: 05-19468
Legacy Document ID:
RIN:
Publish Date: 09/30/2005 00:00:00
Submitter Info:

First Name: Pete
Last Name: Weitzel
Mailing Address: 1101 Wilson Blvd
City: Arlington
Country: United States
State or Province: VA
Postal Code: 20007
Organization Name: Coalition of Journalists for Open Government

Comment Info: =====

General Comment:TO: FAR Secretariat
RE: FAC 2005-06, FAR case 2004-018
The Coalition of Journalists for Open Government (CJOG) is an alliance of journalism-related organizations that came together out of concern over diminishing access to public records and meetings at all levels of government. This withholding of information prevents citizens, directly and through the media, from being fully informed and prepared to participate in the democratic process. We believe it is detrimental to public policy and a principal factor in the public's growing distrust of and disengagement from government. Along with the undersigned organizations, we write to urge that you revise the proposed final rule drafted as it pertains to the definition of "Sensitive But Unclassified" information.

The new regulation would add this definition under Section 2.101, paragraph (b):

Sensitive But Unclassified (SBU) information means unclassified information, which, if lost, misused, accessed or modified in an unauthorized way, could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals. Examples include information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life; loss of property or funds by unlawful means; violation of personal privacy or civil rights; gaining of an unfair commercial advantage; loss of advanced technology, useful to competitor; or disclosure of proprietary information entrusted to the Government.

We recognize that this definition of "Sensitive But Unclassified" is not without precedent. Indeed, the term has been given a variety of meanings over

2004-018-5

several decades by scores of federal departments and agencies. The University of Maryland's Center for Information Policy counts 65 separate definitions of SBU in use today. This inconsistency has resulted in confusion and uncertainty. In some situations, it has resulted in the wrongful denial of public access to information. The public's right to government information is a universal grant in the Freedom of Information Act, now almost 40 years old. The government terminology or markings used to limit that public's right of access to government information should have clear and common meaning.

Unfortunately, the proposed definition is most likely to perpetuate misuse. It is overbroad and ambiguous. It will surely result in gross over-marking, and the withholding of information that does not pose a security concern and should not be withheld for any other reason.

The definition inappropriately combines information exemption categories that are wholly unrelated to national defense or foreign relations under a single marking that suggests these elements create a threat to the security of this nation.

? Loss of property or funds by unlawful means? is not a national security issue.

? Violations of personal privacy and civil rights? are not national security issues.

? The gaining of an unfair commercial advantage, loss of advanced technology to a competitor, and disclosure of proprietary information entrusted to the government? are not national security issues.

? The conduct of a federal program? is not, per se, a national security issue.

We believed it was wrong in early 2002 when White House Chief of Staff Andrew Card urged federal agencies to use existing Freedom of Information Act exemptions ? exemptions that are not related to internal defense or foreign policy ? to justify the withholding of data and records viewed as posing security concerns. The proposed definition compounds that mistaken approach by incorporating these independent and non-relevant exemption criteria into a marking that is intended as an extension of our national security classification system. The use of the word ?unclassified? implies a national security consideration. There is no other reason for its presence.

The Congressional Research Service notes in its comprehensive report on ?Sensitive But Unclassified? usage (February 2004) that many agencies have applied SBU to seal information that falls short of classification standards but is nonetheless believed potentially valuable to a national enemy: ?Even before the terrorist attacks of 2001, federal agencies used the label SBU to safeguard from public disclosure information that does not meet standards for classification.? There is more than ample evidence that in the post -9/11 environment any public information request which raises even a modest national security concern will be met by an automatic default to denial.

As far back as 1984, the Government Accountability Office challenged the ambiguity of an SBU definition because it encompassed ?possibly innocuous information.? A 1986 definition quite similar to the one now being proposed was criticized as too broad because it went beyond national security concerns. It was ultimately withdrawn in negotiations that followed congressional hearings. Today, SBU is again being criticized by many members of Congress who view it as one of the ?pseudo-classifiers? that extend the cloak of official secrecy to information that is not, in fact, classified.

We believe there is not and should not be any equivalency between national security and privacy or trade secrets or general governmental agency interest. The standards which any agency sets for the protection of its security

2004-018-5

information should be separate and distinct from the criteria it establishes for discretionary review of its non-security information. We believe that any rule, which by definition and subsequent marking calls upon government employees to treat security and non-security information equally, can only result in endangering one, or both, categories of information.

We urge you to write a new definition of "Sensitive But Unclassified" that deals strictly with information truly related to national security.

We also urge that with each of those definitions you include a statement affirming that all the information involved is subject to review and possible public disclosure under the Freedom of Information Act. That is the law and it should be explicit in regulation.

We believe it is time to restore clarity and universality to the language of government and to set out definitions that are, in fact, meaningful. The Department of Defense, the General Services Administration and the National Aeronautics and Space Administration, have an opportunity in promulgating this rule to establish a valuable new standard: a narrow and explicit definition of "Sensitive But Unclassified" that focuses on information that is strictly security related, and to make sure that its guidance on how to handle information carefully and thoughtfully is not perceived as a blanket directive that will keep that information from the American people.

Pete Weitzel, for
The Coalition of Journalists for Open Government and
American Society of Newspaper Editors
Associated Press Managing Editors
Committee of Concerned Journalists
National Conference of Editorial Writers
National Freedom of Information Coalition
Reporters Committee for Freedom of Information