



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

JUL 22 2003

MEMORANDUM FOR DIRECTOR, DEFENSE ACQUISITION REGULATION COUNCIL

SUBJECT: Defense Federal Acquisition Regulation Supplement Case No. 2002-D020,  
Information Assurance

We have reviewed the proposed Defense Federal Acquisition Regulation Supplement (DFARS) Case No. 2002-D020, "Information Assurance," and generally agree with the intent of proposed amendments to DFARS Section 239, "Security and Privacy for Computer Systems," and Section 252.239, "Protection Against Compromising Emanations." However, we recommend that the following clarifying points also be included in the proposed revisions.

Section 239.7100, "Scope of subpart." This section should further specify that the acquisition of information technology includes equipment (hardware and software), capabilities (building of enterprise architectures), and information technology services. This clarification would help ensure that the appropriate information assurance requirements are included in all information technology acquisition contracts. The inclusion of such provisions is especially important with the increased emphasis on the protection of sensitive but unclassified information and the additional statutory requirements for the protection of individual privacy information.

Section 239.7103-1, "General." Subsection (a) should also include, as item (7), Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," (HIPAA) that addresses the security and privacy of health data. Although provisions to protect the privacy of individuals are generally mentioned in Federal Acquisition Regulation subpart 24.1, "Protection of Individual Privacy," the new requirements of HIPAA should also be included in this DFARS subsection to ensure that the statute's requirements are addressed.

Section 239.7103-1 (b), "Policy and Responsibilities." Subsection (b)(1) should also specify that the statement of work provided to the contracting officer contain a requirement that offerors provide a list to the contracting officer identifying any foreign nationals that may work on the contract by name, social security number (or other identifying number), and country of origin. In addition, the requiring activity should provide the requirements for disposal of or destruction of information technology storage media. Therefore, a subsection (b)(4) should be added as follows:

"(b)(4) The required procedures for disposal or destruction of information technology storage media such as hard drives, compact disks, or floppy disks, that supports the processing, storing, display of, or transmission of sensitive or official use only contractual or program information and data."

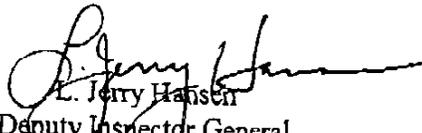
Section 239.1103-2, "Compromising emanations-TEMPEST or other standard."

Subsection (c) should be amended to include a date after which the accreditation would be considered current for purposes of this proposed contract. Requiring a current, valid accreditation is important to ensure that all appropriate and applicable information assurance requirements were complied with during the accreditation process.

Section 252.239-7000, "Protection Against Compromising Emanations."

Section (a) of the contract clause should be amended to provide a date after which the required accreditation would be considered current or valid for the contract.

Thanks you for the opportunity to comment on the proposed rule. If you have any questions, please contact Ms. Donna A. Roberts at (703) 604-8752.

  
L. Jerry Hansen  
Deputy Inspector General  
for Inspections and Policy