UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

OCT 10 2002

PROCUREMENT MEMORANDUM 2002-01

ACTION

MEMORANDUM FOR: HEADS OF CONTRACTING OFFICES

FROM: Signed
Michael S. Sade
Director for Acquisition Management and
Procurement Executive

SUBJECT: Importance of Information Technology Security to Acquisition

Information security is as much a business process as it is a technical one. No longer can security be viewed as a backroom operation, separate from the essential activity of an organization. Security is a key to the success of all operations, especially to acquisition.

The Department's Office of Inspector General (OIG) conducted a review of sample Information Technology (IT) contracts issued by the Department, and found that information security provisions in these contracts are inadequate, primarily because of a lack of specific federal and departmental guidance on safeguarding sensitive information in federal procurements.

As a result of the OIG review and in concert with the current environment surrounding IT security, (i.e. heightened visibility and increased concentration of the need to secure government data and privacy of personal information), I am re-emphasizing the importance of IT security to acquisition. In that vein, I am reissuing Procurement Memorandum 2001-03, dated September 13, 2001 to include updates and provide reference documents and resources.

On April 4, 2002, Thomas Pyke, the Department's Chief Information Officer (CIO) issued a memorandum to all Commerce operating unit CIOs, informing them of their responsibility to ensure that all Commerce employees - - federal and contractors, must complete IT Security awareness training by June 2002. Completion of this training, on an annual basis, is a requirement of the Computer Security Act (Public Law 100-235) and Appendix 3 to OMB Circular A-130. In addition, his office is finalizing the Department's IT Security Program Policy.

In FY 2001, Commerce obligated $703 million for information technology- - the largest single area of contract expenditure. The collection and dissemination of information is critical to the Department's mission. Under the leadership of the Chief Information Officer, the Department is working with the operating units to improve IT security.

I want to emphasize that contracting officers can provide a valuable service by bringing customers together with their CIO and security representatives as early as possible in the acquisition process to help identify and mitigate IT contract security issues.

The following resources are to help you and your customers address IT security issues:

1. Commerce Acquisition Manual (CAM), section 1337.70 (Security Processing Requirements for On-Site Security Requirements), and related CAM Notice 00-02 – Requires the customer to work with their security office before a solicitation is released to designate contract risk levels and then after award to arrange background investigations on contractor employees. (This applies to all requirements, not just IT requirements).
http://oamweb.osec.doc.gov/app/cam.htm

2. National Institute of Standards and Technology (NIST) Special Publication 800-4 (Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials) – Provides additional guidance for security considerations in procurements.
http://csrc.ncsl.nist.gov/publications/nistpubs/

3. NIST Special Publication 800-16 (Information Technology Security Training Requirements: A Role – and Performance-Based Model) – Provides criteria for specialized security training to help all personnel involved in acquisitions learn to build security into the process from the start.
http://csrc.ncsl.nist.gov/publications/nistpubs/

4. FAR Part 39 – Requires incorporation of the clause at 52.239-1, Privacy or Security Safeguards, for IT acquisitions which require security of information technology and/or are for the design, development, or operation of a system or records using commercial IT services or support services.
http://www.arnet.gov/far/

5. The CIO's IT Security Program site, which includes applicable Departmental policy, OMB guidance, relevant legislation, and more, at
http://www.doc.gov/cio/oipr/ITSec/ITSECDOC1.HTML

6. The CIO's list of DOC Chief Information Officers at
http://www.doc.gov/cio/DOCCIOMEMBERS.htm

7. The CIO's list of Information Technology Security Officers at
http:www.osec.doc.gov/cio/oipr/ITSec/ITSO%20LIST%20LINK.htm

It is imperative that these additional reference documents are used and adhered to as appropriate.

For further information, contact Dao Vissering at Dvissering@doc.gov in OAM or Nancy DeFrancesco, the Department's IT Security Program Manager at Ndefrancesco@doc.gov.

O. Wolff, CFO/AS for Administration
T. Pyke, Chief Information Officer
J. Frazier, Inspector General
R. Yamamoto, Director for Security
M. Langstein, OGC, Contract Law Division