The Contracting Officer shall insert a clause the same as the following in all DOC solicitations and contracts for services. The following language may only be modified by adding more restrictive agency or bureau specific guidance

CAR 1352.239-73- SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES

(a) This clause is applicable to all contracts that include information technology resources or services in which the Contractor must have physical or electronic access to DOC's sensitive or classified information, which is contained in systems that directly support the mission of the Agency. For purposes of this clause the term "Sensitive" is defined by the guidance set forth in:

(1) The *DOC IT Security Program Policy and Minimum Implementation Standards* (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html);

(2) The Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, (http://csrc.nist.gov/secplcy/a130app3.txt) which states that there is a "presumption that all [general support systems] contain some sensitive information."; and

(3) The Computer Security Act of 1987 (P.L. 100-235) (http://www.epic.org/crypto/csa/csa.html), including the following definition of the term sensitive information "… any information, the loss, misuse, or unauthorized access, to or modification of which could adversely affect the national interest or the, conduct of federal programs, or the privacy to which individuals are entitled under section 552 a of title 5, Unites States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

For purposes of this clause, the term "Classified" is defined by the guidance set forth in:

(1) The *DOC IT Security Program Policy and Minimum Implementation Standards, Section 3.3.1.4* (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html).

(2) The *DOC Security Manual, Chapter 18* (http://www.osec.doc.gov/osy/).

(3) Executive Order 12958, as amended, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

Information technology resources include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. The Contractor shall be responsible for implementing sufficient Information Technology security, to reasonably prevent the

compromise of DOC IT resources for all of the contractor's systems that are interconnected with a DOC network or DOC systems that are operated by the Contractor.

(b) All Contractor personnel performing under this contract and Contractor equipment used to process or store DOC data, or to connect to DOC networks, must comply with the requirements contained in the DOC *Information Technology Management Handbook* (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html), or equivalent/more specific agency or bureau guidance as specified immediately hereafter [insert agency or bureau specific guidance, if applicable].

(c) For all Contractor-owned systems for which performance of the contract requires interconnection with a DOC network or that DOC data be stored or processed on them, the Contractor Shall:

(1) Provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq*.) and the Federal Information Security Management Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946-2961 (2002); Pub. L. No. 107-296, 116 Stat. 2135, 2259-2273 (2002). 38 WEEKLY COMP. PRES. DOC. 51, 2174 (Dec. 23, 2002) (providing statement by President George W. Bush regarding Federal Information Security Management Act of 2002). The plan shall meet IT security requirements in accordance with Federal and DOC policies and procedures that include, but are not limited to:

(a) OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (http://csrc.nist.gov/secplcy/a130app3.txt);
(b) National Institute of Standards and Technology Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems* (http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF) ; and
(c) DOC Procedures and Guidelines in the *Information Technology Management Handbook* (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html). .
(d) National Industrial Security Program Operating Manual (NISPOM) for classified systems (http://www.dss.mil/isec/nispom.htm); and
(e) [Insert agency or bureau specific guidance].

(2) Within 14 days after contract award, the contractor shall submit for DOC approval a System Certification and Accreditation package, including the IT Security Plan and a system certification test plan, as outlined in *DOC IT Security Program Policy*, Sections 3.4 and 3.5 (http://home.osec.doc.gov/DOC-IT-Security-Program-Policy.htm). The Certification and Accreditation Package must be consistent with and provide further detail for the security approach contained in the offeror's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The Certification and Accreditation Package, as approved by the Contracting Officer, in consultation with the DOC IT Security

Manager, or Agency/Bureau IT Security Manager/Officer, shall be incorporated as part of the contract. DOC will use the incorporated IT Security Plan as the basis for certification and accreditation of the contractor system that will process DOC data or connect to DOC networks. Failure to submit and receive approval of the Certification and Accreditation Package, as outlined in *DOC IT Security Program Policy*, Sections 3.4 and 3.5 (http://home.osec.doc.gov/DOC-IT-Security-Program-Policy.htm) may result in termination of the contract.

(d) The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)