U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

NOV 12 2004

MEMORANDUM FOR DHS HEADS OF CONTRACTING ACTIVITIES
USCG, USSS, FLETC, ICE, CBP, TSA, OPO, FEMA

FROM: **Gregory D. Rothwell**
Chief Procurement Officer Gregory D. Rothwell

SUBJECT: **QUALIFICATIONS OF CONTRACTOR EMPLOYEES AND INFORMATION TECHNOLOGY SYSTEM ACCESS FOR CONTRACTORS**

When the Homeland Security Acquisition Regulation (HSAR) was published as an interim rule, public comments were requested. Public comments were received regarding the breadth of the clauses at HSAR 3052.237-70 and 3052.237-71 concerning sensitive information, security requirements, and limitations on the employment of foreign nationals. To ensure our Nation's allies are given the opportunity to support Homeland Security initiatives, a class deviation to the interim HSAR is established and enclosed. This deviation will affect the clauses at HSAR 3052.237-70 and 3052.237-71. The deviation at HSAR 3052.237-70 and HSAR 3052.237-71 shall be used with the revised Non-Disclosure Agreement, DHS Form 11000.6, dated August 2004. The revised form can be found at DHS Online Forms, Security. The clauses should be used as prescribed immediately. Modification of existing contracts is not necessary.

3052.237-70 Qualifications of Contractor Employees

Contracting officers shall insert the basic clause at (HSAR) 48 CFR 3052.237-70, Qualifications of Contractor Employees, in solicitations and contracts when contract employees require recurring access to Government facilities or access to sensitive information. Contracting Officers shall insert the basic clause with its Alternate for acquisitions in which the contractor will not have access to IT resources, but the Department has determined contractor employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents.

This clause shall not be used if contractor employees will not require recurring access to Government facilities or access to sensitive information.

QUALIFICATIONS OF CONTRACTOR EMPLOYEES
(NOV 2004) (Deviation)

(a) "Sensitive Information" means information that is:

(1) Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. sections 211-224; its implementing regulations, 6 CFR Part 29; or the applicable PCII Procedures Manual; or

(2) Sensitive Security Information (SSI), as described in 49 CFR Part 1520; or

(3) Sensitive but Unclassified Information (SBU), which consists of any other unclassified information which:

(i) if lost, misused, modified, or accessed without authorization, could adversely affect the national interest, proprietary rights, the conduct of Federal programs, or individual privacy under 5 U.S.C. section 552a; and,

(ii) if provided by the government to the contractor, is marked in such a way as to place a reasonable person on notice of its sensitive nature.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms, as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated

background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

Alternate (NOV 2004) Deviation. If the Department has determined that the contractor will not have access to Information Technology (IT) resources, but contractor employee access to other sensitive information or Government facilities must nonetheless be limited to U. S. citizens and lawful permanent residents, add the following paragraph:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by an Alien Registration Receipt Card Form I-151. Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of personnel who are non-U.S. citizen after contract award shall also be reported to the contracting officer.

(End of clause)

3052.237-71 Information Technology Systems Access for Contractors

Contracting officers shall insert the clause at (HSAR) 48 CFR 3052.237-71, Information Systems Access for Contractors, in solicitations and contracts for acquisitions requiring contractor access to IT resources.

INFORMATION TECHNOLOGY SYSTEMS ACCESS FOR CONTRACTORS (NOV 2004) (Deviation)

(a) "Sensitive Information" means information that is:

(1) Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. sections 211-224; its implementing regulations, 6 CFR Part 29; or the applicable PCII Procedures Manual; or

(2) Sensitive Security Information (SSI), as described in 49 CFR Part 1520; or

(3) Sensitive but Unclassified Information (SBU), which consists of any other unclassified information which:

(i) if lost, misused, modified, or accessed without authorization, could adversely affect the national interest, proprietary rights, the conduct of Federal programs, or individual privacy under 5 U.S.C. section 552a; and,

(ii) if provided by the government to the contractor, is marked in such a way as to place a reasonable person on notice of its sensitive nature.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms, as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of personnel who are non-U.S. citizen after contract award shall also be reported to the contracting officer.

(g) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(h) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the COTR will arrange, and complete any nondisclosure agreement furnished by DHS.

(i) The contractor shall have access only to those areas of DHS Organizational Element (OE) information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(j) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS OE. It is not a right, a guarantee of access, a condition of the contract, nor is it Government Furnished Equipment (GFE).

(k) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(l) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Organizational Element or designee, with the concurrence of the Office of Security and Department's CIO or designee. In order for a waiver to be granted:

(i) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State.

(ii) All required security forms specified by the government and any necessary background check must be satisfactorily completed.

(iii) There must be a compelling reason for using this individual as opposed to a U.S. citizen.
(iv) The waiver must be in the best interest of the Government.

(End of clause)