U.S. Citizenship and Immigration Services
Office of Security and Integrity – Personnel Security Division

SECURITY REQUIREMENTS

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Counterintelligence and Security Agency.

Any firm or business under contract with the Department of Homeland Security (DHS), which requires access to classified information, will require a Facility Security Clearance (FCL) commensurate with the level of access required. Firms that do not possess a FCL, or the requisite level FCL, will be sponsored by DHS to obtain one.

FITNESS DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees to government facilities and/or access of Contractor employees to sensitive but unclassified information based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment Fitness authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment Fitness determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No Contractor employee shall be allowed unescorted access to a Government facility without a favorable EOD decision or Fitness determination by the Office of Security & Integrity Personnel Security Division (OSI PSD).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information and/or classified information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the DHS Form 11000-25, Contractor Fitness/Security Screening Request Form and the USCIS Continuation Page to the DHS Form 11000-25. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, Security Questionnaire for Public Trust Positions via e-QIP:

- DHS Form 11000-6, Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement
- FD Form 258, Fingerprint Card **(2 cards)**
- DHS Form 11000-25, Contractor Fitness/Security Screening Request Form
- USCIS Continuation Page to DHS Form 11000-25
- OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
- Foreign National Relatives or Associates Statement

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information and/or classified information has resided in the U.S. for three of the past five years, OSI PSD may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

VISIT AUTHORIZATION LETTER (VAL)

The Contractor is required to submit a VAL for those individuals who require access to classified information during performance on this contract and who have an active Personnel Security Clearance (PCL). The letter will be valid for a period not to exceed one year. If the requirement to access classified information no longer exists, or if access eligibility changes, OSI PSD will be notified immediately. The VAL must be submitted to OSI PSD in accordance with, and contain information as required by, Chapter 6 of the NISPOM.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer's Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract. In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a

contractor's reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than December 31st each year, or prior to any accelerated deadlines designated by USCIS, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- USCIS Security Awareness Training (required within 30 days of entry on duty for new contractors, and annually thereafter)
- USCIS Integrity Training (annually)
- DHS Insider Threat Training (annually)
- DHS Continuity of Operations Awareness Training (one-time training for contractors identified as providing an essential service)
- Unauthorized Disclosure Training (one-time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- USCIS Fire Prevention and Safety Training (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- USCIS PKI Initiative Training (if supervisor determines the need for a PKI certificate)
- Computer Security Awareness Training (if contractor requires access to USCIS IT systems, training must be completed within 60 days of entry on duty for new contractors, and annually thereafter)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire or on any security form listed above.

In accordance with Homeland Security Presidential Directive-12 (HSPD-12) http://www.dhs.gov/homeland-security-presidential-directive-12 contractor employees who require access to United States Citizenship and Immigration Services (USCIS) facilities and/or utilize USCIS Information Technology (IT) systems, must be issued and maintain a Personal Identity

Verification (PIV) card throughout the period of performance on their contract.

Government-owned contractor- operated facilities are considered USCIS facilities.

After the Office of Security & Integrity, Personnel Security Division has notified the Contracting Officer's Representative that a favorable entry on duty (EOD) determination has been rendered, contractor employees will need to obtain a PIV card.

For new EODs, contractor employees have [*10 business days unless a different number is inserted*] from their EOD date to comply with HSPD-12. For existing EODs, contractor employees have [*10 business days unless a different number of days is inserted*] from the date these requirements are incorporated into the contract to comply with HSPD-12.

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:
https://ecn.uscis.dhs.gov/team/mgtosi/Offices/osi/FSD/HSPD12/PIV/default.aspx

Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.

Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing out so that it is visible at all times while in a USCIS facility
- Keep their PIV card current
- Properly store the PIV card while not in use to prevent against loss or theft
  http://dhsconnect.dhs.gov/org/comp/mgmt/ocso/Documents/DHS%20Authorized%20Authoritative%20Credential%20Holder%20Responsibility%20Agreement.pdf

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Facility Security Officer. The individual will interface with OSI through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the

Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

In the event classified information is inadvertently received by a contractor who does not hold an active security clearance at the Secret level, a Government employee or Contractor with the appropriate security clearance equal to or higher than the classified information received, will take possession of the material and shall safeguard and store the information in accordance with standards set forth in the NISPOM. The inadvertent disclosure will be immediately reported to their supervisor and then to the designated OSI Local Security Officer or OSI Field Security Manager for action as appropriate.

Subpart 4.4—Safeguarding Classified Information Within Industry
4.402 General.

(a) Executive Order 12829, January 6, 1993 (58 FR 3479, January 8, 1993), entitled "National Industrial Security Program" (NISP), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829 amends Executive Order 10865, February 20, 1960 (25 FR 1583, February 25, 1960), entitled "Safeguarding Classified Information Within Industry," as amended by Executive Order 10909, January 17, 1961 (26 FR 508, January 20, 1961).
(b) The National Industrial Security Program Operating Manual (NISPOM) incorporates the requirements of these Executive orders. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of Central Intelligence, is responsible for issuance and maintenance of this Manual. The following DoD publications implement the program:
(1) National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M). (2) Industrial Security Regulation (ISR) (DoD 5220.22-R).
(c) Procedures for the protection of information relating to foreign classified contracts awarded to U.S. industry, and instructions for the protection of U.S. information relating to classified contracts awarded to foreign firms, are prescribed in Chapter 10 of the NISPOM.
(d) Part 27—Patents, Data, and Copyrights, contains policy and procedures for safeguarding classified information in patent applications and patents.

4.403 Responsibilities of Contracting Officers.
(a) *Presolicitation phase*. Contracting officers shall review all proposed solicitations to determine whether access to classified information may be required by offerors, or by a contractor during contract performance.
(1) If access to classified information of another agency may be required, the contracting officer shall—
(i) Determine if the agency is covered by the NISP; and
(ii) Follow that agency's procedures for determining the security clearances of firms to be solicited. (2) If the classified information required is from the contracting officer's agency, the contracting officer shall follow agency procedures.
(b) *Solicitation phase*. Contracting officers shall—
(1) Ensure that the classified acquisition is conducted as required by the NISP or agency procedures, as appropriate; and

(2) Include—
(i) An appropriate Security Requirements clause in the solicitation (see 4.404); and
(ii) As appropriate, in solicitations and contracts when the contract may require access to classified information, a requirement for security safeguards in addition to those provided in the clause (52.204-2, Security Requirements).
(c) *Award phase*. Contracting officers shall inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract as follows:
(1) Agencies covered by the NISP shall use the Contract Security Classification Specification, DD Form 254. The contracting officer, or authorized representative, is the approving official for the form and shall ensure that it is prepared and distributed in accordance with the ISR.
(2) Contracting officers in agencies not covered by the NISP shall follow agency procedures.

4.404 Contract Clause.
(a) The contracting officer shall insert the clause at 52.204-2, Security Requirements, in solicitations and contracts when the contract may require access to classified information, unless the conditions specified in paragraph (d) of this section apply.
(b) If a cost contract (see 16.302) for research and development with an educational institution is contemplated, the contracting officer shall use the clause with its Alternate I.
(c) If a construction or architect-engineer contract where employee identification is required for security reasons is contemplated, the contracting officer shall use the clause with its Alternate II.
(d) If the contracting agency is not covered by the NISP and has prescribed a clause and alternates that are substantially the same as those at 52.204-2, the contracting officer shall use the agency- prescribed clause as required by agency procedures.

52.204-2 Security Clause Requirements.
As prescribed in 4.404(a), insert the following clause: Security Requirements (Aug 1996)
(a) This clause applies to the extent that this contract involves access to information classified "Secret."
(b) The Contractor shall comply with—
(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DOD 5220.22-M); and
(2) Any revisions to that manual, notice of which has been furnished to the Contractor.
(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.
(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.
(End of clause)
Alternate I (Apr 1984). If a cost contract for research and development with an educational institution is contemplated, add the following paragraphs (e), (f), and (g) to the basic clause:
(e) If a change in security requirements, as provided in paragraphs (b) and (c), results (1) in a change in the security classification of this contract or any of its elements from an unclassified status or a lower classification to a higher classification, or (2) in more restrictive area controls than previously required, the Contractor shall exert every reasonable effort compatible with the Contractor's established policies to continue the performance of work under the contract in compliance with the change in security classification or requirements. If, despite reasonable efforts,

the Contractor determines that the continuation of work under this contract is not practicable because of the change in security classification or requirements, the Contractor shall notify the Contracting Officer in writing. Until resolution of the problem is made by the Contracting Officer, the Contractor shall continue safeguarding all classified material as required by this contract.
(f) After receiving the written notification, the Contracting Officer shall explore the circumstances surrounding the proposed change in security classification or requirements, and shall endeavor to work out a mutually satisfactory method whereby the Contractor can continue performance of the work under this contract.
(g) If, 15 days after receipt by the Contracting Officer of the notification of the Contractor's stated inability to proceed, (1) the application to this contract of the change in security classification or requirements has not been withdrawn, or (2) a mutually satisfactory method for continuing performance of work under this contract has not been agreed upon, the Contractor may request the Contracting Officer to terminate the contract in whole or in part. The Contracting Officer shall terminate the contract in whole or in part, as may be appropriate, and the termination shall be deemed a termination under the terms of the Termination for the Convenience of the Government clause.
Alternate II (Apr 1984). If employee identification is required for security or other reasons in a construction contract or architect-engineer contract, add the following paragraph (e) to the basic clause:
(e) The Contractor shall be responsible for furnishing to each employee and for requiring each employee engaged on the work to display such identification as may be approved and directed by the Contracting Officer. All prescribed identification shall immediately be delivered to the Contracting Officer, for cancellation upon the release of any employee. When required by the Contracting Officer, the Contractor shall obtain and submit fingerprints of all persons employed or to be employed on the project.