1352.237-71

(e) Notification of Disqualifying Information. If the Office of Security receives disqualifying information on a contract employee, the COR will be notified. The Sponsor, in coordination with the Contracting Officer, will immediately remove the contract employee from duties requiring access to Departmental facilities or IT systems. Contract employees may be barred from working on the premises of a facility for any of the following:

(1) Conviction of a felony crime of violence or of a misdemeanor involving moral turpitude;
(2) Falsification of information entered on security screening forms or on other documents submitted to the Department;
(3) Improper conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government, regardless of whether the conduct was directly related to the contract;
(4) Any behavior judged to pose a potential threat to Departmental information systems, personnel, property, or other assets.
(5) Failure to comply with security processing requirements may result in termination of the contract or removal of contract employees from Department of Commerce facilities or denial of access to IT systems.

(g) Access to National Security Information. Compliance with these requirements shall not be construed as providing a contract employee clearance to have access to national security information.

(i) The contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

(End of clause)

[75 FR 10570, Mar. 8, 2010; 75 FR 14496, Mar. 26, 2010]


As prescribed in 48 CFR 1337.110–70(c), insert the following clause:

SECURITY PROCESSING REQUIREMENTS—LOW RISK CONTRACTS (APR 2010)

(a) Investigative Requirements for Low Risk Contracts. All contractor (and subcontractor) personnel proposed to be employed under a Low Risk contract shall undergo security processing by the Department’s Office of Security before being eligible to work on the premises of any Department of Commerce owned, leased, or controlled facility in the United States or overseas, or to obtain access to a Department of Commerce IT system. All Department of Commerce security processing pertinent to this contract will be conducted at no cost to the contractor.

(b) Investigative requirements for Non-IT Service Contracts are:

(1) Contracts more than 180 days—National Agency Check and Inquiries (NACI).
(2) Contracts less than 180 days—Special Agency Check (SAC).
(3) Any contract employee with a favorable investigation completed under a NACI or SAC may be employed under this contract within the United States.
(4) For Low Risk non-IT service contracts, the scope of the SAC will include checks of the Security/Suitability Investigations Index (SII), other agency files (INVA), Defense Clearance Investigations Index (DCII), FBI Fingerprint (FBIF), and the FBI Information Management Division (FIBN).
(5) In addition, for those individuals who are not U.S. citizens (lawful permanent residents), the Sponsor should request a Customs Enforcement SAC on Form OFI–86C, by checking Block #7, Item 1. In Block 13, the Sponsor should enter the employee’s Alien...
Registration Receipt Card number to aid in verification.

(6) Copies of the appropriate forms can be obtained from the Sponsor or the Office of Security. Upon receipt of the required forms, the Sponsor will forward the forms to the servicing Security Officer. The Security Officer will process the forms and advise the Sponsor and the Contracting Officer whether the contract employee can commence work prior to completion of the suitability determination based on the type of work and risk to the facility (i.e., adequate controls and restrictions are in place). The Sponsor will notify the contractor of favorable or unfavorable findings of the suitability determinations. The Contracting Officer will notify the contractor of an approved contract start date.

(g) Security Processing Requirements for Low Risk IT Service Contracts. Processing of a NACI is required for all contract employees employed under Low Risk IT service contracts.

1) Contract employees employed in all Low Risk IT service contracts will require a National Agency Check and Inquiries (NACI) to be processed. The Contracting Officer’s Representative (COR) will invite the prospective contractor into e-QIP to complete the SF-85. Fingerprints and a Credit Release Authorization must be completed within three working days from start of work, and provided to the Servicing Security Officer, who will forward the investigative package to OPM.

2) For Low Risk IT service contracts, individuals who are not U.S. citizens (lawful permanent residents) must undergo a NACI that includes an agency check conducted by the Immigration and Customs Enforcement Service. The Sponsor must request the ICE check as a part of the NAC.

(h) Notification of Disqualifying Information. If the Office of Security receives disqualifying information on a contract employee, the Sponsor and Contracting Officer will be notified. The Sponsor shall coordinate with the Contracting Officer for the immediate removal of the employee from duty requiring access to Departmental facilities or IT systems. Contract employees may be barred from working on the premises of a facility for any of the following reasons:

1) Conviction of a felony crime of violence or of a misdemeanor involving moral turpitude.

2) Falsification of information entered on security screening forms or of other documents submitted to the Department.

3) Improper conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government regardless of whether the conduct was directly related to the contract.

4) Any behavior judged to pose a potential threat to Departmental information systems, personnel, property, or other assets.

(i) Failure to comply with security processing requirements may result in termination of the contract or removal of contract employees from Department of Commerce facilities or denial of access to IT systems.

(j) Access to National Security Contracts. Compliance with these requirements shall not be construed as providing a contract employee clearance to have access to national security information.

(k) The contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

(End of clause)