

## Reclamation Manual

### SUBPART 1437.81 – SECURITY REQUIREMENTS

#### **WBR 1437.8100 Scope of subpart.**

This subpart prescribes policies and procedures for ensuring the security of Reclamation facilities and information technology resources during the performance of service and construction contracts.

#### **WBR 1437.8101 Authority.**

(a) Homeland Security Presidential Directive 12 (HSPD-12), issued on August 27, 2004, establishes a Government-wide policy titled “Policy for a Common Identification Standard for Federal Employees and Contractors.” HSPD-12 establishes a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(b) Federal Information Processing Standard Publication 201 (FIPS-201), titled “Personal Identity Verification of Federal Employees and Contractors” implements HSPD-12 and is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems, except for “national security systems” as defined by 44 U.S.C. 3542(b)(2).

(c) Department of the Interior Acquisition Policy Release (DIAPR) 2006-03, dated October 24, 2005, establishes procedures for standard implementation of HSPD-12 in DOI contracts.

(d) 375 DM 19 establishes responsibilities, policies, procedures, and minimum requirements for the development, implementation, and maintenance of an information technology (IT) security program for the Department of the Interior. The basis of authority includes public laws, Executive branch directives, Federal standards, and other DOI policies that provide direction and guidance concerning security planning. It establishes the DOI IT security program in compliance with: the Privacy Act of 1974; the Freedom of Information Act, as amended; the Paperwork Reduction Act; the Computer Fraud and Abuse Act of 1986; the Computer Security Act of 1987 (Public Law (P.L.) 100-235); the Information Technology Management Reform Act (ITMRA) of 1996; the Federal Information Security Management Act (FISMA) of 2002; OMB Circular No. A-130, Appendix III, Security of Federal Information Resources; National Institute of Standards and Technology (NIST) Special Publications addressing IT security; Federal Information Processing Standards Publications (FIPSPUBS); National Archives and Records Administration's regulations on records management; the Office of Personnel Management's (OPM) guidance on personnel security as it relates to IT resources; and DOI IT security policy guidance. References to various laws, regulations, directives, and other policy and procedure guidance applicable to IT security in DOI are located in Appendix 3 to 375 DM 19.

(e) 375 DM 19.7 and 19.9 require that appropriate safeguards must be determined before acquiring information technology resources not only to ensure the wise expenditure of funds but also to ensure that the resources may be protected from the time of installation or implementation. To accomplish this, all contract specifications for the acquisition of hardware, software, software development, equipment maintenance, facility management, and related services will contain requirements for safeguards that encompass technical, administrative, personnel, and physical security.

(f) Federal Information Processing Standard Publication 200 (FIPS-200), titled “Minimum Security Requirements for Federal Information and Information Systems” implements the E-Government Act of 2002 (Public Law 107-347 - Title III of which is FISMA) that established requirements for the categorizing of information and information systems and the establishment of protection requirements for those systems and information.

(g) 443 DM 1 specifies, “For any bureau or office entering into a classified contract, only DOD facility clearances and personnel security clearances will be issued to or within industry. Only those ... personnel security clearances granted by the Department of Defense ... will be acceptable to the Department of the Interior for access to its classified information.” Consequently, any classified contracts

## Reclamation Manual

will be coordinated through the Reclamation Chief Security Officer, or for IT requirements, the Bureau IT Security Manager.

### **WBR 1437.8102 Procedures.**

(a) The CO shall not provide contractor employees access to Government-controlled facilities until a PIV Card, temporary identification card, or visitor badge has been issued to the contractor employee in compliance with these regulations.

(b) The COR shall determine if any contractor employees will be required to have a Personal Identity Verification (PIV) Card based on DIAPR 2006-03, the contract paragraphs at WBR 1452.237-80 (c), or in consultation with the Chief Security Officer, Regional Security Officer, or appropriate IT Security Manager. In some cases, this determination may not be possible until after the contract is awarded. WBR 1437.8103 (b) specifies the appropriate clause paragraphs for each situation.

(c) For those contractor employees that will be required to have a PIV Card, a background investigation is required as described in contract paragraphs WBR 1452.237-80 (c)(5). The COR will determine the level of background investigation based on the risk and sensitivity level of each contractor employee position (or group of similar positions) as described in Reclamation's "Personnel Security and Suitability Directives and Standards," SLE 01-01, Appendix A.

(d) If Reclamation receives an unsuitable report on any contractor employee or if Reclamation finds a prospective contractor employee to be unsuitable or unfit for his or her assigned duties, the contract clause at WBR 1452.237-80, "Security Requirements", provides that such employee cannot continue to work (or be assigned to work) under the contract. In that event, the COR must notify the Chief Security Officer or the appropriate Regional Security Officer of what areas/duties this individual has been working on.

### **WBR 1437.8103 Contract Clause.**

(a) The CO shall insert the clause at WBR 1452.237-80, paragraphs (a) and (b), in all solicitations, contracts, purchase orders, orders under Federal Supply Schedules, and task orders issued under Government-wide Agency Contracts (GWACs) and Multi-Agency Contracts (MACs) for services (including construction).

(b) The COR shall determine if contractor employees will be required to have a PIV Card based on DIAPR 2006-03, the contract paragraphs at WBR 1452.237-80 (c), or in consultation with the Reclamation Security Officer, Regional Security Officer, or appropriate IT Security Manager.

(1) If any of the contractor employees will be required to have a PIV Card, or if this will not be determined until after the contract is awarded, the CO shall insert WBR 1452.237-80 paragraph (c).

(2) If it is known that no contractor employees will be required to have a PIV Card, the CO may omit paragraph (c) and insert any applicable local identification card or visitor badge issuance procedures that will be used, such as those used at the Denver Federal Center or in Federal Buildings.

(3) If the contract will have a combination of both PIV Cards and temporary identification cards (or visitor badges), then include paragraph (c). Paragraph (c)(4) is used to insert any applicable local identification card or visitor badge issuance procedures that will be used.

(c) In addition, the CO shall insert WBR 1452.237-80 paragraph (d) in all construction contracts and other contracts that have site security requirements.

(d) In addition, the following specific requirements shall apply to IT contracts:

(1) For all IT services, development, and support contracts, including site maintenance contracts, include clause paragraphs (e)(1), (2), and (3).

(2) For services including off-site processing and storage, or contractor-operated IT service solutions, use Alternate I of this clause, which requires inserting additional paragraphs (e)(4), (5), (6), (7) and (8) to the basic clause.

(3) For all IT products, development, support contracts, or systems provided as turn-key (not necessary for contracts involving only COTS products with no integration efforts), use Alternate II of this clause, which requires inserting additional paragraphs (e)(4), (5), (6), (7) and (8) to the basic clause.

## Reclamation Manual

### WBR 1452.237-80 Security Requirements Contract Clause.

Insert the following clause as prescribed in WBR 1437.8103.

#### SECURITY REQUIREMENTS – BUREAU OF RECLAMATION (OCTOBER, 2006)

##### (a) General Security Requirements:

(1) This clause addresses security requirements, including general procedural requirements, information security requirements, contractor employee suitability requirements, identification card requirements, site security requirements, and information technology security requirements. Within this clause, COR means Contracting Officer's Representative. If there is no COR appointed and identified to the Contractor, the term instead will mean the Program Manager or any other authorized individual responsible for technical oversight under the contract. "Work site" means the Government facility, office, construction site, and any other area within the Government office or facility that the Contractor must access to accomplish work under this contract.

(2) The work performed under this contract shall only be accomplished by individuals (in the employment of the Contractor or any subcontractors) whose conduct and behavior is consistent with the efficiency of the Federal Service and the requirements of this contract, and who are acceptable to the CO. If Reclamation finds a Contractor employee to be unsuitable or unfit for his or her assigned duties, the CO will direct the Contractor to remove the individual from the contract and access to the Federal facility at which the contract activities are occurring.

(3) The Contractor's employees governed by this contract may need access to sensitive information and/or may need access to designated Controlled Access Areas (CAAs). The Federal Government (Government) reserves the right, in its sole discretion, to determine suitability of Contractor personnel and deny access to any sensitive information or project specific area to any personnel for any cause.

(4) The Contractor is responsible for informing and ensuring compliance by its employees with any applicable security procedures of the Government facility where work may be performed under this contract.

(5) Any Contractor employee that will have access to a Federally-controlled facility or information system will be required to have a Government-issued identification card, consisting of either a Personal Identity Verification (PIV) Card, a temporary identification card, or a visitor badge. During performance of the contract, the Contractor shall keep the COR apprised of any changes in personnel, or changes in personnel access or duration, to ensure that performance is not delayed by compliance with credentialing processes.

(6) A Contractor employee will not be provided access to a Government facility or information system until a Government PIV Card, temporary identification card, or visitor identification badge has been issued to the Contractor employee. For those individuals that will be receiving a PIV Card, the Government may, at its discretion, issue a temporary identification card or visitor identification badge after the background investigation forms have been received and the investigation is initiated.

(7) All Contractor employees shall access the facility via the facility's entry screening system and visibly display the Government-issued PIV Card, temporary identification card, or visitor identification badge at all times. Contractor employees must visibly wear the Government-issued identification card at all times they are on Government facilities. Contractor employees are responsible for the safekeeping of all Government-issued identification cards, whether on-site or off-site. Cards that have been lost, damaged, or stolen must be reported to the COR within 24 hours. The Contractor shall return all identification cards and card keys and any other Government property and information upon completion of performance or when personnel depart permanently or for a period of 7 days or more. The Contractor may be required to turn in access control cards or identification cards on a daily basis.

(8) Misuse or loss of access control or identification cards, or failure to comply with required surrender of such cards may, at Government discretion, result in Contractor personnel being denied access to the work site, at no cost to Government. The Contractor may be charged up to \$500 for

## Reclamation Manual

each occurrence for any required replacement of Government-issued access control or identification cards due to loss or misuse. At the end of contract performance, or when a Contractor employee is no longer working under this contract, the Contractor shall ensure that all access control and identification cards are returned to the COR.

(9) All Contractor personnel, including subcontractor personnel, with access to the work site shall be U.S. citizens or foreign individuals legally residing in, or legally admitted to, the U.S. At the direction of the COR, the Contractor shall provide to the COR, in writing, the name and nationality of all non-U.S. citizens working under this contract. For those individuals with access to the work site, the Contractor shall also provide documentation that the foreign individual is legally residing in, or has been legally admitted to, the U.S.

(10) The Contractor shall report all contacts with entities, individuals, and counsel/representatives (including foreign entities and foreign nationals) who seek in any way to obtain unauthorized access to sensitive information or areas. The Contractor shall report any violations of contract provisions, laws, executive orders, regulations, and guidance to the CO. The Contractor shall report any information raising a doubt as to whether an individual's eligibility for continued employment or access to sensitive information is consistent with the interests of National Security and the Public Trust.

(11) Unsanctioned, negligent, or willful inappropriate action on the part of the Contractor (or its employees) may result in termination of the contract or removal of some Contractor employees from Reclamation facilities at no cost to the Government. These actions include, but are not limited to, exploration of a sensitive system and/or information, introduction of unauthorized and/or malicious software, or failure to follow prescribed access control policies and/or security procedures. Failure to comply with Reclamation policies, procedures, or other published security requirements may result in termination of the contract or removal of some contracted employees from Reclamation buildings and/or facilities at no cost to the Government.

(12) All provisions of this clause shall equally apply to all subcontractors. The Contractor shall incorporate the substance of this clause in all subcontracts.

(13) These security requirements apply to all sections of this Contract including Contract Drawings and other Contract Specifications as applicable. Related documents include other general provisions of Construction or Operations and Maintenance type Contracts, including FAR clauses by reference or as amended by related documents.

### **(b) Information Security Requirements.**

(1) The term "sensitive information" means any information which warrants a degree of protection and administrative control as defined by Reclamation or that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act. Sensitive information is generally categorized as FOR OFFICIAL USE ONLY (FOUO) information, but in some cases may include other unclassified information. (The protection of National Classified information is beyond the scope of this clause. If any work on Classified information is required under this contract, it is addressed under other contract clauses.) The Contractor shall protect this type of information from unauthorized release into public domain, or to unauthorized persons, organizations, or subcontractors. Information which, either alone or in aggregate, is deemed sensitive by Reclamation shall be handled and protected in accordance with Reclamation Directives and Standards for Identifying and Safeguarding FOR OFFICIAL USE ONLY (FOUO) Information, which is available at <http://www.usbr.gov/recman/DandS.html#sle>.

(2) Any Government-furnished information/material does not become the property of the Contractor and may be withdrawn at any time. Upon expiration of the contract, all documents released to the Contractor and any material created using data from such documents shall be returned to the COR for final disposition. Only with prior authorization from the CO may the Contractor retain the material. The Contractor or subcontractor shall not disclose or release the materials provided to the Contractor to any individuals of the Contractor's organization not directly engaged in providing services under the contract or that do not have a valid need-to-know. All technical data provided to the Contractor by the Government shall be protected from public or private disclosure in accordance with the markings printed on them. All other information relating to the items to be delivered or the services to be performed under this contract

## Reclamation Manual

shall not be disclosed by any means without prior approval of the CO. Prohibited dissemination or disclosure includes, but is not limited to: permitting access to such information by foreign nationals or by immigrant aliens who may be employed by the Contractor, publication of technical or scientific papers, advertising, and disclosure to Contractor staff not investigated and deemed acceptable at the appropriate contract/information sensitivity level, or any other proposed public release. The Contractor shall maintain, and furnish upon demand of the CO, records of the names of individuals who have access to sensitive material in its custody. All questions regarding information security, access, and control shall be referred to the COR.

(3) The Contractor shall not release to anyone outside the Contractor's organization any sensitive, or otherwise protected information, regardless of medium in which it is contained (for example, film, tape, document, electronic), pertaining to any part of this contract or any Reclamation program or activity, unless the CO has given prior written approval. This includes, but is not limited to, news releases, marketing promotions, articles, interviews, reports, and any other media releases. Requests for approval shall identify the specific information to be released, the medium to be used, the purpose for the release, and a description of the need-to-know. The Contractor shall submit its request to the CO before the proposed date for release. Subcontractors shall submit requests for authorization to release through the prime Contractor to the CO.

(4) The Contractor shall notify the COR immediately when known or suspected loss/compromise of sensitive information or other documents, notes, drawings, sketches, reports, photographs, exposed film or similar information which may affect the security interests of Government has occurred. This requirement extends to employees and other personnel working on behalf of the Contractor, and expands responsibility to include prompt reporting of security issues, including observed or subsequently discovered efforts by unauthorized persons to gain unauthorized access to sensitive information.

### **(c) Contractor Employee Suitability and Issuance of Government Identification Cards:**

(1) Performance of this contract requires Contractor personnel to have a Federal Government-issued Personal Identification Verification (PIV) Card before being allowed unsupervised access to a Federally-controlled facility or information system.

(2) At the Government's sole discretion, the Government may issue a temporary identification card or visitor identification badge, in lieu of a PIV Card, under one of the following conditions:

(i) The individual will only be associated with Reclamation for a period of 180 days or less, will not have access to sensitive information, and any access to a Controlled Access Area or Federal-controlled information system will be fully supervised. The 180 calendar day period begins on the first day of the individual's affiliation with Reclamation (in this case, the date that the individual's contract performance begins) and ends exactly 180 days later, regardless of the number of times the individual actually accesses a Government facility or information system.

(ii) The individual will only have sporadic access to Federal facilities and information systems, will not have access to sensitive information, and any access to a Reclamation Controlled Access Area or Federal-controlled information system will be fully supervised.

(iii) The individual will work exclusively outdoors, will not have access to sensitive information, and any access to a Reclamation Controlled Access Area or Federal-controlled information system will be fully supervised.

(iv) In paragraphs (i) through (iii), supervised access means the individual's access to, and movement within, a facility is monitored and controlled sufficiently to prevent access to any unauthorized areas, equipment, or information; and the individual's access to an information system is monitored and controlled sufficiently to ensure appropriate use of the system and information, and to prevent access to any unauthorized systems or information. Supervision must be performed by an individual with an active Government-issued PIV Card.

## Reclamation Manual

(3) The Contractor shall furnish to the COR an alphabetical list of contract personnel, to include subcontractors, who will require access to a Government facility or information system. The list shall provide the full name, social security number, date of birth, place of birth, purpose or job title, and the estimated duration of access. If the Contractor believes an individual should be issued a temporary identification card or visitor identification badge in lieu of a PIV Card based on the conditions in paragraph (4), then the Contractor must also submit a sufficient written justification as to why the specific individual or individuals will not need a PIV Card. The Contractor shall provide this information before the start of contract performance, or before the start of an individual's performance when there is a change or addition of personnel, with sufficient time to ensure that performance is not delayed by compliance with credentialing processes.

(4) Any contract employees that will be issued a temporary identification card or visitor identification badge, in lieu of a PIV Card, at the Government's sole discretion, will be subject to the following credentialing procedures:

*[Insert any local identification card or visitor badge issuance procedures that will be used, such as those used at the Denver Federal Center or in Federal Buildings.]*

(5) Any contract employees that will be issued a PIV Card will be subject to the following credentialing procedures:

(i) For Contractor employees needing a PIV Card, as determined by the Government, the CO or COR will provide the appropriate background investigation forms to the Contractor, or initiate the electronic background investigation process, and give the Contractor instructions for completing the background investigation, fingerprinting, and PIV Card process. After the background investigation forms are completed, each Contractor employee shall be required to appear in person before a Government PIV Registrar to submit the background investigation forms, have personal identity verification documents verified, have a photograph taken, and sign the PIV Card Request Form. The Contractor must make its personnel available at the place and time specified by the COR in order to initiate this process. The following forms shall be used to initiate the background investigation and PIV process: OPM Standard Form 85, 85P, or 86; OF 306; Fingerprint Card FD-258; Fair Credit Reporting Act Authorization Form; and PIV Card Request Form (paper or web-based).

(ii) The cost of completing and submitting the above forms, including any charges for obtaining fingerprints, shall be borne by the Contractor. The cost of the background investigation shall be borne by Reclamation.

(iii) Contractor employees are required to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed to reach a suitability determination. Refusal or failure to furnish or authorize provision of information may constitute grounds for denial or revocation of credentials. Government personnel may contact the Contractor personnel being investigated in person, by telephone, or in writing, and the Contractor agrees to make them available for such contact.

(iv) For each Contractor employee that will be issued a PIV Card, the Government will conduct a background investigation. The level of background investigation for each Contractor employee will be determined by the Government based on the risk and sensitivity levels as described in Reclamation's Personnel Security and Suitability Directives and Standards," SLE 01-01, which is available at <http://www.usbr.gov/recman/DandS.html#sle>. At a minimum, each Contractor employee that will be issued a PIV Card will receive a National Agency Check with Written Inquiries (NACI) Background Investigation. The minimum standards which will be used in suitability determinations are contained in the DOI Departmental Manual Part 441, Chapter 5, which is available at [http://elips.doi.gov/app\\_dm/act\\_getfiles.cfm?relnum=3290](http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3290).

(v) Each Contractor employee in a position designated as higher than Low Risk Non-Sensitive shall be reinvestigated on a periodic basis as described in Reclamation's Personnel Security and Suitability Directives and Standards. A reinvestigation may also be initiated when the Contractor or the Government believes that a particular individual's continued ability to meet the contract's minimum standards is in question.

## Reclamation Manual

(vi) If a Contractor employee has worked under a Federal agency contract within the past two years, and that contract required a successfully-adjudicated background investigation at the same risk level as (or higher than) this contract, further investigation may not be necessary. The Contractor shall provide the COR with documentation that supports the individual's previous contract work and any information, including name and social security number, date of birth, and place of birth, needed for Government verification of previous background investigation.

(vii) If the final adjudication is unfavorable on a Contractor employee, or if Reclamation finds a Contractor employee to be unsuitable or unfit for his or her assigned duties, the CO will direct the Contractor to remove the individual from the contract and access to the Federal facility at which the contract activities are occurring. In the event of a disagreement between the Contractor and the Government concerning the suitability of a particular employee to perform work under this contract, the Government shall have the right of final determination. Determinations under this requirement are subject to the Disputes Clause. Failure of the Contractor to comply with the requirements of this clause could constitute grounds for termination for default.

(viii) Reclamation will not allow a Contractor employee access to their investigation files. An individual may request, under the provisions of the Privacy Act and/or Freedom of Information Act, copies of their files from the investigative agency (Office of Personnel Management). Reclamation will not release a copy of any investigative file, in whole or part, to the Contractor or any Contractor representative.

(ix) Upon completion of a favorably-adjudicated background investigation, Contractor employees will be issued a Government PIV Card. When the PIV Card is printed, each Contractor employee shall be required to appear in person before the Reclamation PIV Card Issuer for identity verification, to sign the PIV Request Form, and receipt of the PIV Card.

### (d) Site Security Requirements

**(1) General Description.** This section provides provisions to ensure the full security integrity of the facility and personnel working at the facility. The work of this section may involve interfaces with a number of Government security personnel, normally coordinated through the designated COR. The Contractor is responsible for ensuring that activities are accomplished in a manner that complies fully with applicable security statutes, regulations, policies, directives, and standards.

**(2) Government Security Personnel.** When and where applicable, security personnel may be assigned to control access, secure materials or activities at the work site, or escort Contractor personnel in CAAs or other sensitive areas. Personnel may include security managers, security guards, security contractors acting as agents of the Government, law enforcement personnel, or others. These individuals may be used to ensure the overall security and integrity of the site or building and may provide controlled access to designated CAAs. These individuals may conduct inspection of all workers, vehicles, equipment, or materials entering, or re-entering the work site. The inspection may be done with walk-through and/or hand-held metal detectors or by other means as may be deemed necessary by Reclamation.

**(3) Contractor Guard Force.** At the Contractor's sole discretion, and at the Contractor's own expense, with prior written Government approval, a Contractor may be authorized to hire its own guards to secure Contractor-owned equipment and/or to protect Contractor employees or subcontractors. If such a relationship is permitted, the Contractor shall be exclusively liable for all guard activities to include action or inaction of Contractor's guard personnel. The Government will not offer nor provide any indemnification. Contractor shall be solely responsible for guards at all times to include any supervision, oversight, and for the development of local guard orders and or procedures. The Contractor shall be responsible for coordinating all guard activities with the COR and shall develop and submit to the COR, for advance approval, any guard orders and/or guard procedures.

### (4) Additional Security-Related Submittals

**(i) Visitor List.** The Contractor shall furnish to the COR, in advance, notification of visit of any Contractor-sponsored visitor to a Government-controlled facility. This notification should be in writing and must include the purpose or nature of the visit, the full name of the

## Reclamation Manual

visitor, and the full name and phone number of the designated sponsor who will be physically responsible for escorting the visitor for the duration of the scheduled visit.

**(ii) Delivery Schedule.** The Contractor shall furnish to the COR, in advance, a schedule for all deliveries. This list shall include estimated delivery date, time, nature of the materials being delivered, and – where available – the name of delivery company and type of vehicle.

**(iii) Explosive Security Plan.** The Contractor shall furnish to the COR for approval, in advance, an explosive security plan at any work site where explosives will be stored or used.

### **(5) General Provisions.**

**(i) General.** The Contractor shall comply with the Government's site security procedures as specified, and as requested subsequent to award of Contract. Failure of the Contractor to comply with required access controls, information handling procedures, or any other security controls or procedures, may result in revocation of Contractor personnel access to the work site. The Government reserves the right to modify or clarify security provisions of this contract based on changing political and civil circumstances, and perceived threats to personnel or the facility.

**(ii) Security Facilities and Equipment.** The Contractor shall use security facilities and equipment only for the purposes intended and as directed by the COR. The Contractor shall comply with the Government's instructions for use of secure storage areas, site enclosure and gates, temporary security lighting, building space enclosure, and lockup devices and systems established for detection, monitoring, signaling, and alarming field office facilities. Measures necessary to secure the integrity of materials, equipment, and tools installed or used in furtherance of this contract shall be at no cost to the Government.

**(iii) Security Personnel Availability/Work Schedules.** The Contractor shall notify the COR at least 24 hours in advance of any projected work which might impact on security or require the scheduling of extended security personnel support. The Contractor shall provide a weekly work schedule which may have security implications, such as anticipated delivery of materials, use of explosives or heavy machinery, and extra time needed for continuous or inherently lengthy construction or project specific operations (such as concrete placement).

**(iv) Deliveries.** The Contractor shall provide at least one day's advance notice of major deliveries, including time of arrival and trucks/carriers/documentation to be expected for arrival at work site. The Contractor shall provide reasonable advanced notice of deliveries which must be accommodated/accepted at times other than the Government's established working hours. Failure to provide adequate advanced notice may result in delivery delays at the Contractor's expense.

**(v) Site Access.** All Contractor personnel will be issued appropriate identification and must comply with all local access control procedures. The Government reserves the exclusive right to refuse or disallow any vehicular or pedestrian access to any Government-controlled facility or for any deliveries to the work site, regardless if access was scheduled or unscheduled.

**(vi) Inspections and Searches.** The Government reserves unqualified and unlimited right at any time to conduct security-related inspections or searches of work, material, equipment, personnel, and temporary facilities at the work site. The Contractor shall afford unrestricted access to work and allow surveillance and inspection by any Government personnel as authorized by the COR. The Government reserves the right to conduct searches of articles and personal effects of all Contractor personnel, both at point of entry and exit from the work site or Government facility. All Contractor personnel entering and leaving the work site may be required to pass through a Walk-Through-Metal-Detector device and/or other detection devices.

**(vii) After Duty Hours.** No Contractor personnel shall be permitted access to the work site after the Government's established working hours without prior authorization from the Government. All personnel seeking access to the site after the Government's established working hours may be required to sign in and out in a visitor's log that may be maintained by the on duty security personnel (if any).

**(viii) Access Procedures at CAAs.** In some instances, the Contractor may be required to erect temporary security barriers and doors to isolate a CAA, as instructed by the Government. The Contractor may be required to install locks and thereafter control access. The Contractor shall comply

## Reclamation Manual

with the Government's requirement for limited and escorted access to a CAA. The Contractor shall notify the COR at least one day prior to each requested access to a CAA that is outside of the Government's established working hours.

**(ix) Reported Violations.** Where an indication, report, or observation of unauthorized access or performance of unauthorized work has occurred, the Government reserves the right to stop work and deny access until the circumstance and work can be investigated, inspected, tested, and resolved. The entire cost of such stoppages and resolutions shall be borne by Contractor, except when alleged violations of established security requirements, after investigation, are found not to be the fault of the Contractor.

**(x) Briefings.** Contractor personnel who will be assigned to this project, and who will have access to the work site, may be required to attend Government-conducted security briefings. The Government reserves the right to conduct security briefings for Contractor personnel and visitors at all levels of involvement in performance of work and maintenance of security. Required briefings may include, but are not limited to, the following: Information Security, Site Security Requirements and Procedures, Delivery Methods and Inspections, Storage Requirements, Reporting Requirements, Supervisory Procedures, Contractor Employee Conduct, Visitor Control, and Threats.

**(xi) Key Control.** Control of keys/access codes and lock combinations is essential for the Government's project security. The Contractor shall not allow keys or access codes to be duplicated or removed from the work site, nor allow lock combinations to be divulged without specific written advanced authorization from the COR. Such loss of control, observed or suspected, may result in a requirement to change locks involved at the Contractor's expense. At the direction of the COR, the Contractor shall provide duplicate keys and lock combinations to Government security personnel when requested for the purpose of security inspections and emergency actions, including keys/combinations/access codes needed for unrestricted access to every area and element of the project. The Contractor may be required to establish a key control program that is acceptable to the Government for Government-issued keys and for heavy machinery parked at the construction site (if this is a construction contract).

**(xii) Vehicle Control.** In general, parking of vehicles on the work site shall not be permitted, except for tractors, cranes, and similar equipment used directly in performance of work, for delivery of materials/supplies, and for removal of waste and surplus material. The Government may designate an approved contractor employee parking area. Upon entering the work site, vehicles and drivers may be subject to search and inspection. The Contractor shall obtain authorization from the COR to park the Contractor's official vehicles and motorized vehicular construction equipment that are required/desired to be parked on the work site. Vehicles in violation may be towed off the work site at the Contractor's expense. Where Government-designated employee parking is not available, parking of construction employees' automobiles and similar transportation vehicles may be excluded from the work site. It is the Contractor's responsibility to arrange for suitable accommodation for these vehicles.

**(xiii) Prohibited/Restricted Items.** Prohibited/restricted items and activities on the work site include but are not limited to the following: firearms and other weapons, except as specifically authorized by the COR; drugs, including narcotics, barbiturates, marijuana, alcoholic beverages, and similar substances, except for use with valid medical prescription; and explosives.

**(xiv) Exceptions for Explosives.** When needed for use in specifically limited amounts and controlled circumstances for construction work, explosives may be brought onsite with written prior authorization from the COR. As a hazardous material, the Contractor shall treat the use of explosives in accordance with regulations and guidance provided by Federal, State, and local authorities. The storage of explosives shall be in accordance with requirements of the Bureau of Alcohol, Tobacco, and Firearms or the State in which they are stored. If onsite storage of explosives is necessary, explosives shall be stored at a pre-designated, secure site approved by the COR. Prior to Government approval of storage, the Contractor shall develop and submit to the COR a complete storage/security/retrieval plan for approval. The storage/security plan can be included in a "Blasting Safety Plan." The plan shall make accommodations for surveillance, detection, and response. Explosives firing systems shall be stored off-site and under no circumstances shall be stored together with explosives.

## Reclamation Manual

(xv) **Photography.** The use of photographic equipment and taking of photographs shall only be allowed as authorized by the COR.

**(e) Information Technology Security – Basic Security Requirements:**

(1) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in Reclamation IT Security policies, procedures, computer ethics, and best practices in accordance with Reclamation Directive IRM 08-09, September 21, 2001, Subject: Reclamation Information Technology (IT) Security Program (ITSP): IT Security Awareness and Training Requirements. This document is available, upon request, from the CO. The Contractor may use web-based training available from Reclamation to meet this requirement.

(2) The Contractor shall afford Reclamation, including the Department of the Interior Office of Inspector General, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of Reclamation data or to the function of computer systems operated on behalf of Reclamation, and to preserve evidence of computer crime. If the Contractor has a question regarding the access rights or identity of Government employees requesting access to Contractor-operated IT facilities, it should be referred to the COR for resolution before access is granted.

(3) In addition to the notification requirements (b)(4), the Contractor shall immediately notify the COR, of all cyber-related incidents (including the compromise of Contractor- or Government-owned systems for which the Contractor bears operational or management responsibility), regardless of location.

(End of clause)

*Alternate I* (OCT 2006) As prescribed in WBR 1437.8103(a), for all IT services which include off-site processing and storage, or Contractor-operated IT service solutions, add the following additional subparagraphs (4), (5), (6), and (7) to paragraph **(e) Information Technology Security - Basic Security Requirements**.

(4) Contractor staff with significant IT security responsibilities associated with systems connected to or being delivered to Reclamation (such as those responsible for supporting or developing Internet accessible systems, supporting or developing systems containing personal identification information, or supporting or developing systems containing financial information), must complete annual role-based IT security training (over and above that required in (e)(1).) If requested by the Contractor, Reclamation will assist on-site Contractor staff in identifying suitable annual role-based training options throughout the contract performance period.

(5) The Contractor shall be responsible for the Information Technology security of all contractor-owned systems connected to a Bureau of Reclamation network or Reclamation-owned systems operated or maintained by the Contractor for Reclamation, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services to which the Contractor must have physical or electronic access and which may contain Reclamation's sensitive information on unclassified systems directly supporting the mission of Reclamation. This includes information technology, hardware, software, databases, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require these security provisions include:

- (i) The acquisition, transmission or analysis of data owned by Reclamation; and
- (ii) Access to Reclamation networks or computers at a level beyond that granted to the general public, such as access to control rooms, computer rooms, or controlled access through a firewall or other security control measure.

## Reclamation Manual

(6) The Contractor shall 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, stored, or used under this contract. The Contractor's IT Security Plan shall be compliant 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. The plan shall meet IT security requirements in accordance with Federal and Reclamation policies and procedures that include, but are not limited to:

(i) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources; and

(ii) National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems and Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

(7) Within *[Insert number of days]* days after contract award, the Contractor shall submit to the COR its IT Security Plan for Reclamation approval. This plan must be consistent with and further detail the approach contained in the offeror's quotation, proposal, or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the CO, shall be incorporated into the contract as a compliance document.

*Alternate II* (OCT 2006) As prescribed in WBR 1437.8103(a), for all IT products, development, support contracts, or systems provided as turn-key (not necessary for contracts involving only Commercial off-the-Shelf [COTS] software products with no integration efforts), add the following additional subparagraphs (4), (5), (6), and (7) to the paragraph (e) **Information Technology Security - Basic Security Requirements**.

(4) Contractor staff with significant IT security responsibilities associated with systems connected to or being delivered to Reclamation (such as those responsible for supporting or developing Internet accessible systems, supporting or developing systems containing personal identification information, or supporting or developing systems containing financial information), must complete annual role-based IT security training (over and above that required in (e)(1).) If requested by the Contractor, Reclamation will assist on-site Contractor staff in identifying suitable annual role-based training options throughout the contract performance period.

(5) The Contractor shall be responsible for the Information Technology security for all non-Government-owned systems used in the development of turn-key applications (not including Commercial-off-the-Shelf [COTS] software) and systems intended for eventual turn-key delivery to the Bureau of Reclamation in fulfillment of contract requirements. This clause is applicable to all or any part of the contract that includes information technology resources the Contractor is developing on behalf of Reclamation. This includes information technology, hardware, software, databases, networks, and telecommunications systems. Examples of tasks that require these security provisions include:

(i) The design of IT systems or applications that meet overall data processing performance criteria described elsewhere in this contract. Security designs shall be consistent with the requirements of FIPS Publication 200 and the security categorization of the system.

(ii) The development of turn-key control systems, such as Supervisory Control and Data Acquisition (SCADA) or similar systems where improper security functionality and performance of the system could result in misoperation of Government resources; and

(iii) The development of or integration of applications (including COTS) and/or hardware, networks, and telecommunications systems into turn-key products where the improper security functionality and performance of the integrated system could result in loss of integrity, confidentiality, or availability of electronic information or data.

(6) The Contractor shall 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, stored, or used under this contract. The Contractor's IT Security Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of

## Reclamation Manual

1987 (40 U.S.C. 1441 et seq.) and the Federal Information Security Management Act of 2002. The plan shall meet IT security requirements in accordance with Federal and Reclamation policies and procedures that include, but are not limited to:

(i) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources; and

(ii) National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems and Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

(7) Within *[Insert number of days]* days after contract award, the Contractor shall submit to the COR its IT Security Plan for Reclamation approval. This plan must be consistent with and further detail the approach contained in the offeror's quotation, proposal, or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the CO, shall be incorporated into the contract as a compliance document.

*Alternate III* (OCT 2006) As prescribed in WBR 1437.8103(a), for all contracts which include outsourced IT services (off-site, contractor-operated processing and storage of Reclamation or other DOI information) add the following additional subparagraph (8) to paragraph (e) **Information Technology Security - Basic Security Requirements**. This clause can be used in conjunction with either Alternate clause I or II, as applicable. This is not a stand-alone clause.

(8) The Contractor shall afford Reclamation or Reclamation's duly-appointed security assessment agents access to the Contractor's systems, documentation, facilities, and personnel for the purpose of security Certification and Accreditation (C&A) reviews consistent with Reclamation's obligations under FISMA requirements and NIST guidance. These obligations are outlined in more detail in NIST Special Publication 800-37. If deemed appropriate by both the Contractor and Reclamation, cognizant Reclamation staff or authorized representatives will, where necessary, execute a mutually agreeable Non-Disclosure Agreement to protect any of the Contractor's trade secrets, sensitive, or proprietary information that may be either intentionally or inadvertently disclosed to Reclamation during the required review(s).