# U.S. Department of Energy
## Washington, D.C.

**ORDER**

**DOE O 142.3**

Approved: 6-18-04
Review: 6-18-06
Expires: 6-18-08

**SUBJECT:** UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS PROGRAM

1. OBJECTIVES. To define a program for unclassified foreign national access to Department of Energy (DOE) sites, information, and technologies by establishing requirements for the following.

   a. An approval process for foreign national visits and assignments consistent with U.S. and DOE national security and program-specific policies, requirements, and objectives.

   b. Reviews of foreign national access requests to ensure that unauthorized access to information, equipment, or technologies is denied.

   c. A process for documenting and tracking visits and assignments by foreign nationals to DOE sites or involving DOE information or technologies.

2. CANCELLATIONS. This Order cancels the Directives and memorandums listed below.

   a. DOE P 142.1, *Unclassified Foreign Visits and Assignments,* dated 7-14-99;

   b. DOE N 142.1, *Unclassified Foreign Visits and Assignments,* dated 7-14-99;

   c. Secretarial Memorandum *Unclassified Foreign Visits and Assignments*, dated 7-14-99;

   d. Memorandum for Distribution from Francis S. Blake, Deputy Secretary of Energy, *Departmental Use of Foreign Access Central Tracking System,* dated 11-05-01;

   e. Memorandum for Distribution from Kyle E. McSlarrow, *Interim Guidance for Implementation of the Department's Unclassified Foreign Visits and Assignments Program,* dated 12-17-02; and

   f. Secretarial Memorandum, *Policy Exclusion for Unclassified Foreign National's Access to Department of Energy Facilities in Urgent or Emergency Medical Situations,* dated 4-10-01.

   Cancellation of an Order does not, by itself, modify or otherwise affect any contractual obligation to comply with the Order. Cancelled Orders that are incorporated by reference in a contract remain in effect until the contract is modified to delete the references to the requirements in the cancelled Orders.

3. APPLICABILITY.

a. Primary DOE Organizations, Including National Nuclear Security Administration (NNSA) Organizations. Except for the exclusions in paragraph 3c, this Order applies to all Primary DOE Organizations, including NNSA Organizations (see Attachment 1 for a complete list of Primary DOE Organizations). This Order automatically applies to Primary DOE Organizations created after it is issued.

The Administrator of NNSA shall assure that NNSA employees and contractors comply with their respective responsibilities under this Order.

b. Site/Facility Management Contractors.

(1) The Contractor Requirements Document (CRD), Attachment 2, sets forth the requirements of this Order that will apply to site/facility management contractors whose contracts include the CRD.

(2) The CRD must be included in all site/facilities management contracts that contain DOE Acquisition Regulation (DEAR) clause 952.204-2, "Security requirements."

(3) This Order does not automatically apply to other than site/facility management contractors. Any application of any requirements of this Order to other than site/facility management contractors will be communicated separately from this Order.

(4) As the laws, regulations, and DOE Directives clause of a site/facility management contract states, regardless of the performer of the work, site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD.

(a) Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontractors at any tier to the extent necessary to ensure compliance with the requirements.

(b) Contractors must not unnecessarily or imprudently flow down requirements to subcontractors. That is, contractors will—

1 ensure that they and their subcontractors comply with the requirements of the CRD and

2 incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

(5) The officials identified in paragraph 5, Responsibilities, are responsible for notifying contracting officers of which contractors are affected. Once

notified, contracting officers are responsible for incorporating this Order into the affected contracts via the laws, regulations, and DOE Directives clauses of the affected contracts.

c. Exclusions.

(1) Events or activities that are determined to be open to the general public (such as public lectures, community meetings, cultural or entertainment events, or open house events) and that are held in locations that are determined to be open to the general public by the hosting site approval authority in coordination with subject matter experts (SMEs) in security [to include cyber security, technical security, and operations security (OPSEC)], export control, technology transfer, counterintelligence and intelligence (when there is a field intelligence element onsite), are exempt from this Order. The site security plan must document the conditions where this exemption applies.

(2) Access by foreign nationals 17 years of age or younger, who are involved in non-work-related activities (school tours, family days, etc.) does not have to be documented in the Foreign Access Central Tracking System (FACTS). Access for work-related activities by foreign nationals 17 years of age or younger, however, does require adherence to requirements of this Order.

(3) Unclassified events and activities that occur outside the United States or its territories do not have to be documented in FACTS, but may require documentation in the Foreign Travel Management System or reporting to counterintelligence.

(4) In accordance with the responsibilities and authorities assigned by Executive Order 12344 (as prescribed by 42 U.S.C. 7158), and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this DOE Order for activities under his cognizance.

4. REQUIREMENTS. DOE is a leader in science and technology and is responsible for advancing U.S. capabilities in energy supply, related environmental cleanup and management, and economical energy sources while protecting U.S. national security interests associated with these energy technologies. DOE values the contributions of international collaborations to the scientific and technological strength of the United States and to Departmental mission success and offers foreign national visitors and assignees access to DOE's facilities, staff, and information as participants in a broad range of unclassified work. Foreign national access to DOE sites, programs, information, and technologies will be approved provided the access is needed to support the program

objectives of DOE and/or U.S. national interests [with the exception of foreign nationals 17 years old or younger as specified in paragraph 3c(2) above].

a. Implementation Plans must be developed if requirements cannot be implemented with existing resources within 6 months of the effective date of this Order. These plans must be developed within 90 days of the effective date of this Order and submitted to the cognizant LPSO. Copies of approved plans must be sent to the Office of Security. Plans must ensure that full implementation of this Order is accomplished within 1 year of the effective date of this Order.

b. Definitions. Terms commonly used in the program are defined in Attachment 3 of this Order and in the Safeguards and Security Glossary of Terms (available online at http://directives.doe.gov/references/index.html#security).

c. Documentation. FACTS is the Department's official national database of information on unclassified foreign visits and assignments (UFVAs). Access to FACTS is limited to U.S. citizens. All UFVAs that require documentation, as detailed in paragraph 4i, Graded Approach, will be documented in FACTS. The designated approval authority is responsible for ensuring that documentation occurs.

d. Passport, Visa, and Immigration and Naturalization Service Information. Sufficient documentation of immigrant or nonimmigrant status, identity, and citizenship is required for all foreign visitors and assignees at all DOE sites, facilities, and laboratories to verify the foreign national's identity and authority to work (when applicable for the activities involved) and ensure that the foreign national is eligible (in lawful immigration status) to be in the United States.

The passport, visa, and/or other U.S. Citizenship and Immigration Services (USCIS) information that has been provided to verify identity, authority to work, and lawful immigration status must be documented in FACTS and reviewed annually for all foreign national assignees, including nonsensitive country nationals, sensitive country nationals (individuals who were born in; are citizens of; or represent a company, business, organization or institute from countries identified as sensitive), and nationals of state sponsors of terrorism (individuals who were born in; are citizens of; or represent a company, business, organization, or institute from countries identified as state sponsors of terrorism).

Passport, visa, and other USCIS information will be documented and maintained by the site, facility, or laboratory for those UFVAs which are not to public areas and open information and which are not otherwise required to be documented in FACTS, as detailed in paragraph 4i. For assignments, this information will be reverified annually. All passport, visa, and other USCIS information must be made available to the appropriate LPSO and the Office of Security upon request.

(1) Lawful Permanent Residents of the United States. Documentation required for lawful permanent residents (previously called permanent resident aliens) includes a permanent resident card (Green Card or USCIS Form I-551) and Government-issued identification documentation which includes a photograph, such as a passport or driver's license.

(2) Nonimmigrant Visitors and Assignees. Data required includes documents supporting valid nonimmigrant status and a valid passport with an expiration date which matches or exceeds the expiration date of the nonimmigrant status.

(a) The Visa Waiver Program (VWP). Foreign nationals entering the United States under the VWP are not required to have nonimmigrant visas. Data required for a nonimmigrant visitor or assignee admitted to the United States under the VWP includes a valid passport and documentation of USCIS status (I-94W Nonimmigrant Visa Waiver Arrival/Departure Form). A list of countries participating in the Visa Waiver Program is maintained by the U.S. Department of State.

(b) Citizens of Canada. With the exception of Treaty Traders, Treaty Investors, or fiancés, most Canadian citizens entering the United States are not required to have a visa. A Canadian citizen is required to have documentation establishing Canadian citizenship (such as birth certificate, citizenship certificate, or passport) and a Government-issued identification document that includes a photograph, such as a passport or driver's license.

(c) Citizens of Mexico. A visitor or assignee who is a Mexican citizen must have a valid passport and documentation of a nonimmigrant visa or Form DSP-150 (laser visa).

e. Security Plans. Each foreign national visit or assignment must be covered by an approved security plan that addresses the sensitivity factors (including area type to be visited, determination of whether information containing sensitive subjects will be shared, and affiliation with sensitive countries or countries identified as state sponsors of terrorism) and the results of SME reviews consistent with the specific requirements of this Order.

(1) Specific Security Plan. A security plan is required to address specific site security concerns relating to foreign national visits or assignments. Specific security plans are required for access by foreign nationals to areas other than laboratories or facilities that perform no classified work and at which no classified materials are stored or property protection areas (PPAs), for access to information on the Sensitive Subjects List, or for foreign national affiliation with a sensitive country (with the exception of

laboratories or facilities that perform no classified work and at which no classified materials are stored) or a country identified as a state sponsor of terrorism. A specific security plan is also required if the site safeguards and security plan (SSSP) or site security plan (SSP) does not provide sufficient protection of DOE facilities, programs, and information for the conduct of the foreign national visit or assignment. The specific security plan must be approved by the site security representative and by the site approval authority and will be used in conjunction with the SSSP or SSP.

(2) Generic Security Plan. If SME review determines that none of the requirements for a specific security plan exist, and that the SSSP or the SSP provides sufficient protection of DOE facilities, programs, and information for the conduct of the foreign national visit or assignment, no further documentation of security measures for that visit or assignment is required.

f. Subject Matter Expert Reviews.

(1) SMEs will review requests for foreign national visits and assignments when required, as detailed in paragraph 4i. These reviews include—

(a) security, including cyber security, technical security, and OPSEC, and determination of sufficiency of the security plan for the specific visit or assignment;

(b) export control and determination of export license requirements;

(c) technology transfer;

(d) counterintelligence; and

(e) intelligence, when there is a field intelligence element onsite.

(2) SME reviewers will consider factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities and determinations of whether legal and policy-related terms and conditions associated with the proposed visit or assignment have been met.

(3) SME reviews will ensure that any identified risk to the Government associated with access approval for each visit or assignment has been appropriately evaluated and mitigated.

(4) SMEs will advise the approval authority regarding access requests and before access approval is determined will document and provide to the approval authority any concerns regarding access requests. For requests

involving nationals of state sponsors of terrorism, SMEs will provide advice to the site approval authority.

(5) SME reviews will be documented in FACTS. Documentation will include the date the review was completed and the name of the reviewer.

g. Indices Checks. All UFVAs involving nationals of state sponsors of terrorism, sensitive country nationals, sensitive subjects, or security areas other than laboratories or facilities that perform no classified work and at which no classified materials are stored or PPAs require indices checks, which are coordinated by the Office of Counterintelligence. (See paragraph 4i for requirements.)

Indices checks are requested electronically through the process of documenting visit and assignment access requests in FACTS. In cases where indices checks must be completed before access approval determination, the request must be documented 30 days before the first day of access.

In cases when there is insufficient time to complete an indices check before the first day of access, the approval authority may request a counterintelligence consultation in lieu of the completion of the indices check for sensitive country and nonsensitive country nationals. Counterintelligence consultations may not be employed as a standard alternative to indices checks.

Counterintelligence consultations may not be used in lieu of indices checks for nationals of state sponsors of terrorism.

h. Access Approval. All foreign national access to DOE, programs, information, and technologies for unclassified purposes must be approved by either the Secretary of Energy or an assigned approval authority. Access approvals are subject to validation and verification of the information submitted for the access request when the visit or assignment begins.

(1) Access Approval Determinations. For all foreign national access approval requests, the following apply.

(a) The approval authority must take into consideration all information from the review process, including SME reviews, and must evaluate potential impacts on local site operations.

(b) Determination of access approval must ensure that any identified risk to the Government associated with the access granted has been appropriately evaluated and mitigated.

(c) For the request to be approved, it must be determined that the benefits to the Government are greater than the risks associated with the presence of the foreign national at a DOE site. If the request is for a national of a state sponsor of terrorism, it must be

determined that the potential visit or assignment is extraordinary (i.e., impossible to achieve through any other means).

(d) Legal and policy-related terms and conditions associated with the proposed visit or assignment must be met before approval. Those terms and conditions include, but are not limited to, consideration for other activities at the site, visa sponsorship requirements, visa status conditions and requirements, right-to-work requirements, and international agreements.

(e) Approval determinations will be documented in FACTS. Documentation will include the date of the determination, whether the request was approved or denied, and the name of the approval authority.

(2) Assignment of Approval Authority. Approvals for foreign national access must be consistent with line management accountability requirements.

(a) Approval Authorities. Approval authorities must be U.S. citizens.

(b) Field Sites. Line management accountability flows from the Secretary through the Deputy Secretary or Under Secretaries, to program Secretarial Officers (PSOs), to the head of the DOE field element,[1] to the site management official or laboratory director for the hosting site, who has been assigned specific authority and responsibility to approve access. When the site management official or laboratory director is not a U.S. citizen, the head of the cognizant DOE field element will assign the approval authority. Final approval authority can be assigned to hosting site management officials or laboratory directors for access requests for sensitive country nationals and nonsensitive country nationals.

For a hosting site management official or laboratory director to further assign approval authority, he or she must first develop a plan and related procedures for that assignment. The plan must be approved by the head of the cognizant DOE field element. Once the plan is approved, approval authority may be re-assigned to another U.S. citizen employee. All assignments of approval authority must be in writing and be promulgated by the approval authority, and copies must be provided to the cognizant DOE field element and LPSO, the hosting site foreign visits and assignments office, and the Office of Security. Site management officials and laboratory directors will be held accountable for all approval decisions made by themselves or by those to whom they re-assign

[1]Field elements include operations offices, service centers, site offices, area offices, and regional offices of federally staffed laboratories.

approval authority. Employees to whom approval authority has been re-assigned may not further re-assign this authority.

(c) Headquarters Elements. Headquarters staff and support office accountability flows from the Office of the Secretary to heads of program offices. Final approval authority can be assigned to Headquarters heads of program offices for access requests for sensitive country nationals and nonsensitive country nationals. The head of a Headquarters staff or support office may re-assign his or her approval as appropriate. All re-assignments of approval authority must be in writing, and a copy must be provided to the Office of Security. Heads of Headquarters staff and support offices will be held accountable for all decisions made by themselves or by those to whom they re-assign approval authority. Employees to whom approval authority has been re-assigned may not further re-assign this authority.

(d) Nationals of State Sponsors of Terrorism. Access requests for nationals of state sponsors of terrorism require approval by both the site approval authority and the sponsoring Headquarters program office before final approval determination. Final approval authority is held by the Secretary of Energy and can only be assigned to the Under Secretary for Nuclear Security / Administrator for the National Nuclear Security Administration or the Under Secretary for Energy, Science and Environment.

The Headquarters Management Panel consists of the Directors of the Offices of Security, Counterintelligence and Intelligence, and of representatives designated by the Undersecretary for Nuclear Security / Administrator for the National Nuclear Security Administration and the Under Secretary for Energy, Science and Environment. The Headquarters Management Panel will review requests submitted by sponsoring Headquarters program offices and provide advisory recommendations either to the Secretary of Energy or to the appropriate Under Secretary for review and final approval determination.

The Office of Security will coordinate reviews by the Headquarters Offices of Security, Intelligence, Counterintelligence, Defense Nuclear Nonproliferation, and any other reviews required by DOE security Directives before submitting requests for review and final approval determination.

i. Graded Approach. DOE, to include NNSA, will follow a graded approach for reviewing and approving access by foreign nationals to DOE sites, programs,

information, and technologies based on location, country, subject, and requested length of time.

(1) Public Areas and Open Information.

(a) Public areas are those locations which are accessible by the general public and for which there are no requirements for security clearances, security escorts, or security logs, as documented in the site security plan. Open information is that which is not protected by statute and would be considered releasable to the general public. Events or activities that are determined to be open to the general public (such as public lectures, community meetings, cultural or entertainment events, or open house events), and that are held in public areas, may occur without documentation in FACTS. However, counterintelligence reporting may be required.

(b) Before an event or activity can occur, the hosting site approval authority must consult with SMEs in security (including cyber, technical and OPSEC), export control, technology transfer, counterintelligence, and intelligence (when there is a field intelligence element onsite) and then provide written determination that the subject matter is releasable to the public. Event or activity submissions must include an agenda and brief discussion of technical areas being discussed.

(2) Laboratories or Facilities That Perform No Classified Work and at Which No Classified Materials Are Stored. For these sites, the following requirements apply. (Note: If at any time classified work is performed or classified materials are stored at one of these laboratories or facilities, the laboratory or facility must meet all requirements of the appropriate section of paragraph 4i.)

(a) Passport, visa, and USCIS information for all foreign visitors and assignees must be validated before access is granted.

(b) SME reviews for requests involving nationals of state sponsors of terrorism must be completed before site approval determination.

(c) Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access and must be approved in accordance with paragraph 4h(2)(d) of this Order.

(d) All sensitive country national assignees and all visitors whose visits involve sensitive subjects must be documented in FACTS.

(e) Indices checks for nationals of state sponsors of terrorism must be completed before site approval determination.

(f) Indices checks for sensitive country assignments, and for assignments involving sensitive subjects, are required but do not have to be completed before access is granted. Indices checks for all visits involving sensitive subjects are required and must be completed before access is granted.

(g) For visits and assignments involving access to sensitive subjects, a specific security plan must be developed and approved by the site approval authority.

(3) Property Protection Areas.

(a) Property Protection Areas Without Access to Sensitive Information. These areas must be documented in the site security plan.

1 Passport, visa, and USCIS information for all visitors and assignees must be validated before access.

2 SME reviews for access requests for nationals of state sponsors of terrorism are required and must be completed before site approval determination.

3 Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access and must be approved in accordance with paragraph 4h(2)(d) of this Order.

4 Indices checks for requests involving nationals of state sponsors of terrorism are required and must be completed before site approval determination.

5 Sensitive country national and nonsensitive country national access requests must be documented in FACTS no later than the first day of access.

6 Closeout information must be documented in FACTS at the end of the visit or assignment.

(b) Property Protection Areas With Access to Sensitive Information.

1 Passport, visa, and USCIS information for all foreign visitors and assignees must be validated before access is granted.

2 SME reviews in security (including cyber, technical, and OPSEC), export control, and technology transfer are required for nonsensitive country nationals. SME reviews in security (including cyber, technical, and OPSEC), export control, technology transfer, counterintelligence, and intelligence (when there is a field intelligence element onsite) are required for nationals of state sponsors of terrorism, sensitive country nationals, and requests involving access to sensitive subjects. If an export license is required, it must be granted before the first day of access.

3 Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access and must be approved in accordance with paragraph 4h(2)(d) of this Order.

4 Access requests for sensitive country national assignees, and requests involving access to sensitive subjects must be entered into FACTS 30 days before access. Access requests for nonsensitive country nationals must be entered in FACTS prior to access.

5 Indices checks for all nationals of state sponsors of terrorism must be completed prior to site approval determination. Indices checks for sensitive country national assignees and for requests involving access to sensitive subjects must be completed before final access approval determination. Indices checks for sensitive country national visitors are required but do not have to be completed prior to access.

6 Closeout information must be documented in FACTS within 15 days of the last day of access by the visitor or assignee.

(4) Offsite Locations. These include meetings and other offsite activities that have not been determined to be public events by the site approval authority.

(a) Passport, visa, and USCIS information for all foreign visitors and assignees must be validated before access is granted.

(b) SME reviews in security (including cyber, technical, and OPSEC), export control, and technology transfer are required for nonsensitive country nationals. SME reviews in security, (including cyber, technical, and OPSEC), export control,

technology transfer, counterintelligence, and intelligence (when there is a field intelligence element onsite) are required for nationals of state sponsors of terrorism, sensitive country nationals, and requests involving access to sensitive subjects. If an export control license is required, it must be granted before the first day of access.

(c) Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access and must be approved in accordance with paragraph 4h(2)(d) of this Order.

(d) Access requests for sensitive country national assignees and visitors and requests involving access to sensitive subjects must be entered into FACTS 30 days before access. Access requests for nonsensitive country nationals must be entered in FACTS prior to access.

(e) Indices checks for all nationals of state sponsors of terrorism, sensitive country national assignees, and requests involving access to sensitive subjects must be completed before final access approval determination. Indices checks for sensitive country national visitors are required, but do not have to be completed prior to access.

(f) Closeout information must be documented in FACTS within 15 days of the last day of access.

(5) All Other Security Areas. These include physical spaces that contain materials and/or information that requires physical protection measures. (Those areas described above are not included.) The following requirements apply.

(a) Passport, visa, and USCIS information for all foreign visitors and assignees must be validated before access is granted.

(b) SME reviews in security (cyber, technical and operations), export control, technology transfer, counterintelligence, and intelligence (when there is a field intelligence element onsite) are required.

(c) Access requests for nationals of state sponsors of terrorism must be approved in accordance with paragraph 4h(2)(d) of this Order.

(d) Requests for visits and assignments must be entered into FACTS 30 days before the first day of access.

(e) Indices checks are required for all nationals of state sponsors of terrorism and must be completed before site approval determination. Indices checks are required for all sensitive country nationals and nonsensitive country nationals and must be completed before final approval determination.

(f) Closeout information must be documented in FACTS within 15 days of the last day of access.

(6) Special Situations.

(a) Foreign national emergency response and medical personnel who require access to medical facilities or services for medical emergencies are excluded from the preaccess approval requirements of this Order. This exclusion is expressly conditioned upon a facility's compliance with site-specific security measures.

(b) Policy for remote cyber access by foreign nationals will be drafted by the Office of the Chief Information Officer and issued by the Secretary of Energy.

(c) International Atomic Energy Agency (IAEA) visits that are not inspection activities, as defined in the agreement between the United States and the IAEA, or that otherwise do not involve classified information or technologies are unclassified visits and will be documented in accordance with this Order. IAEA inspection activities and other classified visits involving foreign nationals are governed by the requirements for classified visits.

(d) Visits by foreign national delivery, service, and vendor personnel must be covered by site security plans and procedures. If fully escorted, these foreign nationals do not require documentation in FACTS. If not escorted, the visits must be in compliance with requirements for the location of access, as described above.

(e) Visits by foreign press to the Headquarters offices in the Forrestal Building are conducted through the Office of Public Affairs and involve official press interviews. Press representatives from nonsensitive countries will follow specific Headquarters procedures and security plans, will be fully documented in FACTS within 2 working days of access, and will be validated with front desk access logs. Press representatives from sensitive entities or representing press services of sensitive entities require full previsit reviews and approvals documented in FACTS before access. Foreign press visits to sites and facilities other than the

Headquarters Forrestal Building will be in accordance with all requirements of this Order.

(f) High-level protocol visits to Headquarters at the Forrestal Building are limited to meetings with the Secretary of Energy, the Deputy Secretary, the Under Secretaries of Energy, or PSOs in the Forrestal Building. Advance approval reviews may be suspended if requested by these senior Departmental managers subject to compliance with the security plans and procedures developed for high-level protocol visits to the Forrestal Building. Documentation of these visitors in FACTS is required the day of the visit and will be validated with front desk access logs.

(g) Protocol visits to other DOE or NNSA sites or facilities are not considered high-level protocol visits and will be approved in accordance with all requirements of this Order.

(h) Foreign National participation in Work for Others projects which involves access to DOE sites, facilities, or laboratories, or to DOE information that is not releasable to the public, are considered visits and assignments and will be in accordance with all requirements of this Order.

5. RESPONSIBILITIES.

a. Secretary of Energy.

(1) Establishes DOE policies, procedures, and requirements for foreign national access to DOE sites, programs, information, and technologies.

(2) Assigns access approval authority to Headquarters program offices and LPSOs and through LPSOs to the heads of DOE field elements and heads of local DOE sites for access by foreign nationals, except for those from countries identified as state sponsors of terrorism, consistent with the policies and requirements of this Order.

(3) Assigns access approval authority to the Undersecretary for Nuclear Security / Administrator for National the National Nuclear Security Administration or the Under Secretary for Energy, Science and Environment, as appropriate, for access by foreign nationals born in, citizens of, employed by, or representing entities in countries identified as state sponsors of terrorism, consistent with the polices and requirements of this Order.

b. Lead Program Secretarial Officers and the Administrator, NNSA.

(1) Ensure that facilities under their cognizance have implemented this Order.

(2) Notify contracting officers of affected site/facility management contractors to incorporate the CRD of this Directive into their contracts.

(3) Ensure that procurement requests for new non-site-/non-facility-management contracts require inclusion of the CRD to this Order in the resulting contracts, if appropriate.

(4) Assign foreign national access approval authority to heads of DOE field elements reporting directly to the LPSO.

(5) Provide systematic program review of field and local site approvals for which the LPSO has responsibility to ensure that program-specific guidance is followed, corrective action is taken as appropriate, and line management responsibilities associated with the presence of foreign nationals are met.

(6) Ensure that the work to be accomplished as a result of the visit or assignment adds value to DOE programmatic responsibilities.

(7) Ensure that the requirements of this Order are applied to non-DOE-funded work performed within the operating programs over which the LPSO has responsibility.

(8) Ensure that all required UFVA information is documented in FACTS as required by this Order.

(9) Ensure that appropriate security plans and countermeasures are in place for all foreign national visits and/or assignments.

(10) Ensure that procedures are in place to make all employees and contractors fully aware of the security requirements for UFVAs at their sites/facilities.

c. Heads of Primary DOE Organizations (see Attachment 1 for a complete listing).

(1) Review procurement requests for new non-site-/non-facility-management contracts, and if appropriate ensure that the CRD of this Directive is included in the contracts.

(2) Serve as UFVA approval authorities for Headquarters activities and/or offices within their organizations. This authority may be re-assigned in writing to another employee who is a U.S. citizen. A copy of each reassignment must be provided to the Office of Security at the time it becomes effective. Employees to whom approval authority has been re-assigned may not further re-assign this authority.

(3) Develop and implement operating procedures for approving UFVA access to Headquarters program and contractor program personnel, facilities, information, and organizations.

(4) Ensure that all requirements of this Order are incorporated into processes established to approve access by foreign visitors including full documentation in FACTS.

(5) Designate a point of contact (POC) for UFVA program management and provide contact information to the Office of Security.

(6) Provide program-specific guidance to Headquarters program mangers and field elements, including program policy regarding foreign nationals' access to potentially sensitive subjects, technologies, and information in unclassified program activities.

(7) Establish program priorities and requirements for performance reporting, evaluation, and accountability for foreign national contributions to the program mission. Provide copies of all program-specific guidance to the LPSO with line management responsibility for DOE and contractor operated field sites and to the Office of Security.

(8) Ensure that a systematic and effective process to provide program managers, planners, and hosts with appropriate guidance and insight regarding all technologies and information that could lead into sensitive or export controlled areas before approving access to these program activities by foreign nationals. This process will include programmatic reviews to ensure that sensitive or export controlled technologies and information is properly identified. Reviews should be conducted at least annually and more often if changes in circumstances indicate the need for a subject matter review.

(9) Ensure that all UFVA requests are fully documented in FACTS as required by this Order.

(10) Are responsible for directing contracting officers in their organization to incorporate the CRD for UFVA program implementation into all program contracts which may involve contract with foreign national visitors or assignees.

(11) Ensure that appropriate security plans and countermeasures are in place and followed as required to ensure only authorized access is granted to foreign nationals.

d. Heads of Field Elements (for the purpose of this Order, this includes operations offices, service centers, site offices, area offices, and regional offices of federally staffed laboratories).

(1) Review procurement requests for new non-site-/non-facility-management contracts, and if appropriate, ensure that the requirements of the CRD of this Directive are included in the contracts.

(2) Develop and submit implementation plans as required.

(3) Serve as approval authorities for UFVAs to the DOE field element. This authority may be re-assigned to another employee who is a U.S. citizen within the field element site. All reassignments must be in writing and promulgated by the head of the field element, and copies must be provided to the LPSO and the Office of Security at the time the reassignment becomes effective. Employees to whom approval authority has been re-assigned may not further re-assign this authority.

(4) Assign foreign national access approval authority for UFVAs to the heads of hosting sites reporting directly to the DOE field element or, when the head of the hosting site is not a U.S. citizen, to another management official.

(5) Serve as approval authorities for redelegation plans and procedures for cognizant sites/facilities.

(6) Designate POCs for UFVA program management and provide contact information to the Office of Security and the LPSO. Ensure that POCs are fully knowledgeable of program issues and activities.

(7) Incorporate all PSO guidance into local management processes for approving foreign national access to field element facilities, information, and organization.

(8) Ensure that appropriate security plans and countermeasures are in place for UFVA at their sites/facilities.

(9) Ensure that PPAs with no sensitive information are identified and included in SSPs or SSSPs for cognizant sites/facilities**.**

e. Heads of Hosting Sites/Facilities. Hosting sites may include Headquarters, Federal, or contractor operated field sites; national laboratories; and other DOE operating entities.

(1) Consistent with the assignment of authority through the line management chain, serve as approval authorities for UFVA activities and programs within their organizations.

(2) Develop plans and procedures to be approved by the cognizant DOE field element for reassignment of approval authority to other employees who are U.S. citizens.

(3) Provide written reassignment of approval authority after approval of related plans and procedures, and provide copies of reassignment to the cognizant DOE field elements, cognizant LPSOs, local foreign visits and

assignments offices, and the Office of Security. Employees to whom approval authority has been re-assigned may not further re-assign this authority.

(4) Ensure that all persons who are re-assigned approval authority are fully aware of their roles and responsibilities.

(5) Implement the UFVA program consistent with guidance and direction from the head of the DOE field element with direct responsibility for program performance.

(6) Incorporate all program-specific guidance into local program management processes and procedures, and ensure that all technical and management control requirements of this Order are incorporated into the local management process established to approve access by foreign nationals, including full documentation in FACTS.

(7) Designate POCs for UFVA program management, and provide contact information to the Office of Security, the head of the DOE field element, and the LPSO. Ensure that POCs are fully knowledgeable of program issues and activities.

(8) Ensure that program-specific guidance is issued and is being followed, corrective actions are being implemented as appropriate, and program responsibilities associated with the presence of foreign nationals are being met.

(9) Ensure systematic, effective processes to provide program managers, planners, and hosts with appropriate guidance and insight regarding all technologies and information that could lead into sensitive or export controlled areas before approving access to these program activities by foreign nationals. These systematic processes will include programmatic reviews to ensure the appropriate identification of any sensitive or expert controlled technologies and/or information. Reviews should be conducted at least annually and more often if changes in circumstances indicate the need for a subject matter review.

(10) Ensure that the requirements of this Order are applied to non-DOE-funded work performed within the operating programs for which the local site managers have responsibility.

(11) Ensure that the UFVA program is included in organizational self-assessments.

(12) Ensure that security incident reports are filed for violations or for deviations in the status of a foreign national in accordance with DOE requirements and U.S. law.

f. Hosts for Unclassified Foreign Visitors and Assignees are DOE Federal representatives directly responsible for the activities associated with the successful accomplishment of foreign visits or assignments. For a foreign national to host another foreign national, the host must first be a DOE employee. For laboratories or facilities that perform no classified work, and at which no classified materials are stored, sensitive country nationals (to exclude nationals of state sponsors of terrorism, who may not host other foreign nationals) may host only nonsensitive country nationals for visits and assignments that do not involve access to sensitive subjects. For all other sites, facilities and laboratories, sensitive country nationals (to include nationals of state sponsors of terrorism) may not host other foreign nationals. The host must be identified to the visitor or assignee as his/her POC and must meet the following requirements.

(1) Ensure compliance with all requirements for access approval and conduct, including timely, complete, and accurate information for FACTS documentation; security plans; SME reviews; environment, safety, and health reviews and requirements; program sponsorship (such as exchange visitor programs); and notification to workers regarding these requirements as appropriate.

(2) Serve as the individual responsible for the conduct and activities of the foreign nationals for which he/she is identified as host.

(3) Complete annual DOE security briefing/certification.

(4) Report suspicious activities in accordance with local reporting requirements to include the local counterintelligence office and the local incidents and infractions reporting office.

(5) Provide the following information to the foreign nationals for whom they have been identified as hosts.

(a) The terms and conditions of access approval, including restrictions and requirements to notify the host of changes in name or status (e.g., passport, visa, or other USCIS information), as required.

(b) The requirement to notify the responsible host of any civil or criminal problems that could affect their status and association with DOE.

(c) That failure to provide appropriate documentation when required or providing fraudulent documentation will result in suspension of access approval, removal from the site/facility, and possible cancellation of future access.

g. Escorts. An escort is a DOE employee who is assigned responsibility for a foreign national working or traveling within a site/facility to ensure there is no

unauthorized access. With the exception of authorized hosts at laboratories or facilities that perform no classified work, and at which no classified materials are stored, sensitive country foreign nationals may not serve as escorts. Escorts are responsible for the following:

(1) Familiarity with the site/facility, including security areas.

(2) Full understanding and knowledge of security plan requirements.

(3) Knowledge of specific information or technologies to which the foreign national has been authorized access to ensure that there is no unauthorized access.

(4) Appropriate clearance required for escort duties as required by hosting site security.

h. Headquarters Departmental Staff and Support Offices.

(1) Director, Office of Security.

(a) Develops the policy baseline and incorporates operational requirements into DOE-wide procedural guidance for the UFVA program.

(b) Develops and oversees the process to document and track access approvals for foreign national visitors and assignees to DOE facilities, technologies, and information to ensure consistency with U.S. and DOE national security policies, requirements, and objectives, including export control and cyber security laws and regulations.

(c) Establishes and chairs UFVA working groups as required to identify procedural concerns and recommend revisions that facilitate the processing and access approval of UFVA within established DOE policy.

(d) Ensures that program and staff Secretarial Office policy requirements for foreign national access approvals are incorporated into UFVA policy and coordinates technical and procedural solutions that ensure requirements are met.

(e) Defines, develops, and manages FACTS capabilities to provide operational and analytical program support and accountability.

(f) Develops and implements user training for FACTS.

(g) Provides policy and technical assistance and support to Headquarters and field elements.

(h) Participates in intra- and inter-Agency working groups to discuss, develop, and present recommendations to address issues affecting policy, operations, processes, and program outcomes.

(i) Develops the Departmental strategic plan for the Unclassified Foreign Visits and Assignments Program to ensure recognition of the important benefits derived from international collaborations and the important U.S. and DOE national security policies, requirements, and objectives that must be met while involving foreign nationals with DOE programs.

(j) Develops and coordinates resource requirements, testimony, internal and external reporting, and responses to requests for information regarding any aspect of DOE's UFVA program.

(k) Develops security policy for to the UFVA program access approval process and establishes, coordinates, implements, and evaluates the DOE-wide policy context for physical security reviews including security plans and badging processes as applied to foreign national visitors and assignees.

(l) Maintains liaison with Departmental emergency management, inter-Agency counterterrorism, and homeland security components.

(m) Provides information on the requirements of UFVA policy for inclusion in Security Survey Program.

(2) Director, Office of Counterintelligence.

(a) Identifies counterintelligence policy and information requirements applicable to the management of unclassified access approval for foreign nationals to DOE sites, programs, technologies, and information for Office of Security program implementation.

(b) Provides advice to Headquarters approval authorities and supports field counterintelligence officers with guidance on foreign national access issues to consider in performing reviews.

(c) Ensures that local capability and expertise are available to provide effective counterintelligence advice to local approval authorities regarding access approval requests.

(d) Develops and provides counterintelligence awareness training modules for UFVA training.

(e) Coordinates the external indices check process with the appropriate U.S. Government agencies.

(f) Documents and maintains DOE-wide information on requests for and completion of indices checks.

(3) Headquarters and Field Counterintelligence Officers.

(a) Review requests for foreign national access approval, including visits involving information and technologies that are releasable to the public for counterintelligence and counterterrorism implications.

(b) At the request of the local hosting site, provide counterintelligence consultations to the approval authority, or to his or her designees, to evaluate foreign national access in the absence of a required, completed indices check, and document the consultation in FACTS.

(c) Conduct briefings and debriefings of hosts, sponsors, and escorts of foreign visitors and assignees.

(4) Director, Office of Intelligence.

(a) Analyzes and coordinates issues of field intelligence with other Federal agencies.

(b) Supports the unclassified foreign national access approval process by analyzing and coordinating issues of field intelligence with other Federal agencies, and provides general and specific advice to DOE elements, including the Offices of Counterintelligence and Security. The general and specific guidance to be provided addresses the objectives of the intelligence reviews with respect to potential risks associated with foreign national requests for access to DOE sites, programs, technologies, and information.

(c) Reviews access approval requests for nationals from countries listed as state sponsors of terrorism, and advises the Secretary of Energy, Under Secretary for Nuclear Security / Administrator for the National Nuclear Security Administration or Under Secretary for Energy, Science and Environment regarding requests.

(5) Deputy Administrator, Defense Nuclear Nonproliferation.

(a) Analyzes and develops policy guidance for the UFVA access approval process in the areas of technology transfer, export controls, and nonproliferation.

(b) Provides expert advice as needed to the Offices of the Secretary, Counterintelligence, and Security and other DOE elements as required.

(c) Coordinates and maintains sensitive subjects and sensitive countries lists relating to nonproliferation, technology transfer, and export controls. These lists are incorporated into the foreign national access approval review procedures and are reviewed, validated, and revised annually.

(d) Provides guidance to DOE program elements regarding technology transfer, export controls, and nonproliferation issues. This guidance enhances program consideration of potential and actual foreign visits and assignments access approvals.

(e) Performs specific technology transfer, nonproliferation, and export control reviews of UFVA and for all foreign nationals from countries identified as state sponsors of terrorism and ensures that these reviews are documented in FACTS.

(6) Director, Office of Independent Oversight and Performance Assurance. Incorporates the requirements of the UFVA program into the comprehensive, independent assessment of the effectiveness of safeguards and security policies and programs of immediate interest to the Secretary, the Deputy Secretary, and the NNSA Administrator.

(7) Assistant Secretary for International Affairs and Policy. As the DOE point of contact with the Department of State and international organizations, provides advice and information to the Office of Security concerning the policies and procedures promulgated in this Order.

(8) General Counsel. Provides timely review and advice on all legal issues relating to approval of unclassified foreign national access to DOE facilities and information.

(9) Chief Information Officer (CIO).

(a) Drafts policy for issuance by the Secretary of Energy or Deputy Secretary of Energy to line program managers, contracting officers, security managers, local CIOs, local counterintelligence officers, and the Office of Security regarding protective measures required for cyber security access approval, whether onsite or by remote access.

(b) Ensures that security plans and access approval processes incorporate specific guidance for approving foreign national access based on cyber security issues and objectives.

(10) Deputy Administrator for Naval Reactors. In accordance with the responsibilities and authorities assigned by Executive Order 12344 [statutorily prescribed by Public Law 98-525 (42 U.S.C. 7158)] and to ensure consistency through the joint Navy/DOE organization of the Naval Nuclear Propulsion Program, implements and oversees requirements for activities under the Deputy Administrator's cognizance.

i. Contracting Officers.

(1) After notification by the appropriate program official, incorporate the CRD into affected contracts via the laws, regulations, and DOE Directives clauses of the contracts.

(2) Assist originators of procurement requests who want to incorporate the CRD of this Directive in new non-site-/non-facility-management contracts, as appropriate.

6. REFERENCES. The following references include program and technical areas of responsibility and policy that define the UFVA program requirements.

a. DOE P 205.1, *Departmental Cyber Security Management Policy,* dated 5-8-01.

b. DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03.

c. DOE N 205.2, *Foreign National Access to DOE Cyber Systems,* dated 11-1-99.

d. DOE O 413.1A, *Management Control Program,* dated 4-18-02.

e. DOE O 440.1A, *Worker Protection Management for DOE Federal and Contractor Employees*, dated 3-27-98.

f. DOE G 440.1-1, *Worker Protection Management for DOE Federal and Contractor Employees Guide for Use with DOE O 440.1,* dated 7-10-97.

g. DOE P 450.1, *Environment, Safety, and Health Policy for the Department of Energy Complex,* dated 6-15-95.

h. DOE P 450.2A, *Identifying, Implementing and Complying with Environment, Safety and Health Requirements,* dated 5-15-96.

i. DOE G 450.4-1B, *Integrated Safety Management System Guide (Volume 1) for Use with Safety Management System Policies (DOE P 450.4, DOE P 450.5, and DOE P 450.6); the Functions, Responsibilities, and Authorities Manual; and the Department of Energy Acquisition Regulation,* (Chapter IV), dated 3-1-01.

j. DOE G 450.4-1B, *Integrated Safety Management System Guide (Volume 2) for Use with Safety Management System Policies (DOE P 450.4, DOE P 450.5, and*

*DOE P 450.6);* the *Functions, Responsibilities, and Authorities Manual;* and the *Department of Energy Acquisition Regulation,* dated 3-1-01.

k. DOE O 470.1, *Safeguards and Security Program,* dated 9-28-95.

l. DOE O 471.2A, *Information Security Program,* dated 3-27-97.

m. DOE M 472.1-1B, *Personnel Security Program Manual,* dated 7-12-01.

n. DOE M 481.1-1A, *Reimbursable Work for Non-Federal Sponsors Process Manual,* dated 1-03-01.

o. DOE M 471.2-1B, *Classified Matter Protection and Control Manual,* dated 1-6-99.

p. DOE M 471.2-1C, *Classified Matter Protection and Control Manual,* dated 4-17-01.

q. DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual,* dated 6-30-00.

r. DOE 1270.2B, *Safeguards Agreement with the International Atomic Energy Agency,* dated 6-23-92.

s. DOE 5670.3, *Counterintelligence Program,* dated 9-4-92.

t. Agreement Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States (and Protocol thereto), signed 11-18-77, and entered into force 12-9-80 and all subsidiary arrangement, agreements and amendments.

u. Homeland Security Presidential Directive-2, *Combating Terrorism through Immigration Policies,* dated October 29, 2001.

7. CONTACT. Questions concerning this Order should be addressed to the Director, Office of Security, or the Office of Foreign Visits, Assignments and Travel, U.S. Department of Energy, 1000 Independence Avenue SW, Washington, DC 20585.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

**PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, IS APPLICABLE**

Office of the Secretary
Chief Information Officer
Departmental Representative to the Defense Nuclear Facilities Safety Board
Energy Information Administration
National Nuclear Security Administration
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Office of Economic Impact and Diversity
Office of Electric Transmission and Distribution
Office of Energy Assurance
Office of Energy Efficiency and Renewable Energy
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation and Chief Financial Officer
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security
Office of Security and Safety Performance Assurance
Office of the Inspector General
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

# CONTRACTOR REQUIREMENTS DOCUMENT

## DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*

This Contractor Requirements Document (CRD) establishes requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration (NNSA) contractors, whose contracts involve foreign national access to DOE owned or leased sites/facilities or information, technologies, or equipment that is not releasable to the public.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor must not unnecessarily or imprudently flow down requirements to subcontractors. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

1. PURPOSE. This CRD defines a program for unclassified foreign nationals' access to DOE contractor sites, information, and technologies by establishing requirements for the following.

    a. An approval process for foreign national visits and assignments consistent with U.S. and DOE national security and program-specific policies, requirements, and objectives.

    b. Reviews of foreign national access requests to ensure that unauthorized access is denied.

    c. A process for documenting and tracking foreign nationals' visits and assignments to DOE contractor sites or involving DOE contractor information or technologies.

2. EXCLUSIONS.

    a. Events or activities that are determined to be open to the general public (such as public lectures, community meetings, cultural or entertainment events, or open house events), and that are held in locations that are determined to be open to the general public by the hosting site approval authority in coordination with subject matter experts (SMEs) in security [to include cyber security, technical security, and operations security (OPSEC)], export control, technology transfer, counterintelligence and intelligence (when there is a field intelligence element onsite), are exempt from this Order. The site security plan must document the conditions where this exemption applies.

    b. Access by foreign nationals 17 years of age or younger who are involved in non-work-related activities, such as school tours, family days, etc., does not have to be documented in the Foreign Access Central Tracking System (FACTS).

Access for work-related activities by foreign nationals 17 years of age or younger, however, does require adherence to this CRD.

c. Unclassified events and activities that occur outside the United States or its territories do not have to be documented in FACTS but may require documentation in the Foreign Travel Management System, or may require reporting to counterintelligence.

3. REQUIREMENTS. DOE is a leader in science and technology and is responsible for advancing U.S. capabilities in energy supply, related environmental cleanup and management, and economical energy sources while protecting U.S. national security interests associated with these energy technologies. DOE values the contributions of international collaborations to the scientific and technological strength of the United States and to Departmental mission success and offers foreign national visitors and assignees access to DOE's facilities, staff, and information as participants in a broad range of unclassified work. Foreign national access to DOE sites, programs, information, and technologies will be approved provided the access is needed to support the program objectives of DOE and/or objectives of U.S. national interests (with the exception of foreign nationals 17 years old or younger as specified in paragraph 2b above).

a. Implementation Plans. If requirements cannot be implemented with existing resources within 6 months of the date this CRD is attached to the contract, contractors must develop implementation plans within 90 days and submit these plans to the cognizant lead program Secretarial Office (LPSO) for approval. Copies of approved implementation plans must be sent to the Office of Security. Implementation plans must ensure that full implementation of this CRD is accomplished within 1 year of the effective date.

b. Definitions. Terms commonly used in the program are defined in the Safeguards and Security Glossary of Terms and in Attachment 3 of DOE O 142.3, *Unclassified Foreign Visits and Assignments Program,* dated 6-18-04.

c. Documentation. FACTS is the Department's official national database on unclassified foreign visits and assignments (UFVAs). Access to FACTS is limited to U.S. citizens. All UFVAs that require documentation, as detailed in paragraph 3i below will be entered in FACTS. The designated approval authority is responsible for ensuring that documentation occurs.

d. Passport, Visa, and U.S. Citizenship and Immigration Services (USCIS) Information. Sufficient documentation of immigrant or nonimmigrant status, identity, and citizenship is required for all foreign visitors and assignees at DOE sites, facilities and laboratories to verify identity and authority to work (when applicable for the activities involved) and to ensure that the foreign national is eligible (in lawful immigration status) to be in the United States.

The passport, visa, and/or USCIS information that has been provided to verify identity, authority to work, and lawful immigration status must be documented in

FACTS and reviewed annually for all foreign national assignees, including nonsensitive country nationals, sensitive country nationals (individuals who were born in; are citizens of; or represent a company, business, organization or institute from countries identified as sensitive), and nationals of state sponsors of terrorism (individuals who were born in; are citizens of; or represent a company, business, organization, or institute from countries identified as state sponsors of terrorism).

Passport, visa, and other USCIS information will be documented and maintained by the site, facility, or laboratory for those UFVAs which are not to public areas and open information and which are not otherwise required to be documented in FACTS, as detailed in paragraph 4i, Graded Approach, below. For assignments, this information will be reverified annually. All passport, visa, and other USCIS information must be made available to the appropriate LPSO and the Office of Security upon request.

(1) Lawful Permanent Residents of the United States. Documentation required for lawful permanent residents (formerly, permanent resident aliens) includes permanent resident card (Green Card or USCIS Form I-551) and Government-issued identification documentation which includes a photograph, such as a passport or driver's license.

(2) Nonimmigrant Visitors and Assignees. Data required includes documents supporting valid nonimmigrant status, and a valid passport with an expiration date which matches or exceeds the expiration date of the nonimmigrant status.

(a) The Visa Waiver Program (VWP). Foreign nationals entering the United States under the VWP do not require a nonimmigrant visa. Materials required for nonimmigrant visitors and assignees admitted to the United States under the VWP include a valid passport and documentation of USCIS status (I-94W Nonimmigrant Visa Waiver Arrival/Departure Form). A list of countries participating in the Visa Waiver Program is maintained by the U.S. Department of State

(b) Citizens of Canada. With the exception of Treaty Traders, Treaty Investors, or fiancés, Canadian citizens entering the United States do not require visas. For visitors and assignees who are Canadian citizens, required information includes documentation establishing Canadian citizenship (birth certificate, citizenship certificate, or passport) and a Government-issued identification document that includes a photograph, such as a passport or driver's license.

(c) Citizens of Mexico. A visitor or assignee who is a Mexican citizen must submit a valid passport and documentation of a nonimmigrant visa or Form DSP-150 (laser visa).

e. Security Plans. Each foreign national visit or assignment must be covered by an approved security plan that addresses the sensitivity factors, including area type to be visited, determination of whether information containing sensitive subjects will be shared, affiliation with sensitive countries or countries identified as state sponsors of terrorism, and the results of SME reviews consistent with the specific requirements of this CRD.

(1) Specific Security Plan is required to address site security concerns relating to foreign national visits or assignments. These plans must address—

(a) access to areas other than laboratories or facilities which perform no classified work or at which no classified materials are stored or property protection areas (PPAs);

(b) access to information on the Sensitive Subjects List; or

(c) foreign national affiliation with a sensitive country (with the exception of laboratories or facilities that perform no classified work and at which no classified materials are stored) or a country identified as a state sponsor of terrorism.

A specific security plan is also required if the site safeguards and security plan (SSSP) or site security plan (SSP) does not provide sufficient protection of DOE facilities, programs, and information for the conduct of the foreign national visit or assignment.

The specific security plan must be approved by the site security representative and by the site approval authority and will be used in conjunction with the SSSP or SSP.

(2) Generic Security Plan. If SME review determines that none of the requirements for a specific security plan exist and that the SSSP or the SSP provides sufficient protection of DOE facilities, programs, and information for the conduct of the foreign national visit or assignment, no further documentation of security measures for that visit or assignment is required.

f. Subject Matter Expert Reviews.

(1) SMEs will review requests for foreign national visits and assignments, when required, as detailed in paragraph 3i below. These reviews include—

(a) security, including cyber security, technical security, and OPSEC for the specific visit or assignment;

(b) export control including export license requirements;

(c) technology transfer;

(d) counterintelligence; and

(e) intelligence (when there is a field intelligence element onsite).

(2) SME reviewers will consider factors associated with the requested access to DOE sites, programs, information and technologies including building access and surrounding activities, and determinations of whether legal and policy-related terms and conditions associated with the proposed visit or assignment have been met.

(3) SME reviews will ensure that any identified risk to the Government associated with access approval for each visit or assignment has been appropriately evaluated and mitigated.

(4) SMEs will provide advice to the approval authority regarding access requests and will document and present to the approval authority any concerns before access approval determination. For requests involving nationals of state sponsors of terrorism, SMEs will provide advice to the site approval authority.

(5) SME reviews will be documented in FACTS and will include the date the review was completed and the name of the reviewer.

g. Indices Checks. All UFVAs involving nationals of state sponsors of terrorism, sensitive country nationals, sensitive subjects, or security areas other than laboratories or facilities that perform no classified work and at which no classified materials are stored or PPAs require indices checks coordinated by the Office of Counterintelligence. (See paragraph 3i below for requirements.)

Indices checks are requested electronically when documenting visit and assignment access requests in FACTS. In cases where indices checks must be completed before access approval, the request must be documented 30 days before the first day of access. When there is insufficient time to complete an indices check before the first day of access, the approval authority may request a counterintelligence consultation for sensitive country and nonsensitive country nationals. Counterintelligence consultations may not be employed as a standard alternative to indices checks.

Counterintelligence consultations may not be used in lieu of indices checks for nationals of state sponsors of terrorism.

h. Access Approval. All foreign national access to DOE sites, programs, information, and technologies for unclassified purposes must be approved by the Secretary of Energy or by an assigned approval authority, which may be a contractor employee. Access approvals are subject to validation and verification

of the information submitted for the access request when the visit or assignment begins.

(1) Access Approval Determinations. For all foreign national access approval requests, the following apply.

(a) The approval authority must consider all information from the review process and SME reviews and must evaluate potential impacts onsite operations.

(b) Legal and policy-related terms and conditions associated with the proposed visit or assignment must be met before approval is granted. Those terms and conditions include, but are not limited to, consideration for other activities at the site, visa sponsorship requirements, visa status conditions and requirements, right-to-work requirements, and international agreements.

(c) Approval determinations will be documented in FACTS including the date of the determination, whether approved or denied, and the name of the approval authority.

(2) Assignment of Approval Authority. Approvals for foreign national access must be consistent with line management accountability requirements.

(a) Approval Authorities. Approval authorities must be U.S. citizens.

(b) Field Sites. Line management accountability flows from the Secretary, through the Under Secretaries, to program Secretarial Officers (PSOs), to DOE field elements,[1] to the contractor site management official or laboratory director, who has been assigned specific authority and responsibility to approve access. When the site management official or laboratory director is not a U.S. citizen, the head of the cognizant DOE field element will assign approval authority to another management official. Final approval authority can be assigned to hosting site management officials or laboratory directors for access requests for sensitive country nationals and nonsensitive country nationals.

For a contractor official or laboratory director to further re-assign approval authority, he or she must first develop a plan and related procedures for that reassignment. The plan must be approved by the head of the cognizant DOE field element. Once the plan is approved, approval authority may be reassigned only to another U.S. citizen employee. Reassignment of approval authority must be in writing and be promulgated by the approval authority, and

[1]Operations offices, service centers, site offices, area offices, and regional offices of federally staffed laboratories.

copies must be provided to the cognizant DOE field element, the cognizant LPSO, the local foreign visits and assignments office, and the Office of Security. Site management officials and laboratory directors will be held accountable for all of their own approval decisions or decisions made by those to whom they have re-assigned approval authority. Employees to whom approval authority has been re-assigned may not further re-assign this authority.

(c) Nationals of State Sponsors of Terrorism. Access requests for nationals of state sponsors of terrorism require approval by both the site approval authority and the sponsoring Headquarters program office before final approval determination. Final approval authority is held by the Secretary of Energy and can only be assigned to the Under Secretary for Nuclear Security / Administrator for the National Nuclear Security Administration or the Under Secretary for Energy, Science and Environment.

i. Graded Approach. DOE, to include NNSA, contractors will follow a graded approach for reviewing and approving access by foreign nationals to DOE sites, programs, information, and technologies based on location, country, subject, and length of time.

(1) Public Areas and Open Information.

(a) Public areas are those locations which are accessible by the general public, and for which there are no requirements for security clearances, security escorts, or security logs, as documented in the site security plan. Open information is that which is not protected by statute and would be considered releasable to the general public. Events or activities that are determined to be open to the general public (such as public lectures, community meetings, cultural or entertainment events, or open house events), and that are held in public areas, may occur without documentation in FACTS. However, counterintelligence reporting may be required.

(b) Before an event or activity can occur, the hosting site approval authority must consult with SMEs in security (including cyber, technical and OPSEC), export control, technology transfer, counterintelligence, and intelligence (when there is a field intelligence element onsite), and then provide written determination that the subject matter is releasable to the public. Event or activity submissions must include an agenda and brief discussion of technical areas being discussed.

(2) Laboratories or Facilities That Perform No Classified Work and at Which No Classified Materials Are Stored. For these sites, the following requirements apply. (Note: If at any time classified work is performed or classified materials are stored at one of these laboratories or facilities, the laboratory or facility must meet all requirements of the appropriate section of paragraph 3i.)

(a) Passport, visa, and USCIS information for all foreign visitors and assignees must be validated before access is granted.

(b) SME reviews for requests involving nationals of state sponsors of terrorism must be completed before site approval determination.

(c) Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access, and must be approved in accordance with paragraph 3h(2)(d) of this CRD.

(d) All sensitive country national assignees, and all visitors whose visits involve sensitive subjects, must be documented in FACTS.

(e) Indices checks for nationals of state sponsors of terrorism must be completed before site approval determination.

(f) Indices checks for sensitive country assignments, and for assignments involving sensitive subjects, are required but do not have to be completed before access is granted. Indices checks for all visits involving sensitive subjects are required and must be completed before access is granted.

(g) For visits and assignments involving access to sensitive subjects, a specific security plan must be developed and approved by the site approval authority.

(3) Property Protection Areas.

(a) Property Protection Areas Without Access to Sensitive Information. These areas must be documented in the site security plan.

1 Passport, visa and USCIS information for all visitors and assignees must be validated before access.

2 SME reviews for access requests for nationals of state sponsors of terrorism are required, and must be completed before site approval determination.

3 Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access, and must be approved in accordance with paragraph 4h(2)(c) of this CRD.

4 Indices checks for requests involving nationals of state sponsors of terrorism are required and must be completed before site approval determination.

5 Sensitive country national and nonsensitive country national access requests must be documented in FACTS no later than the first day of access.

6 Closeout information must be documented in FACTS at the end of the visit or assignment.

(b) Property Protection Areas With Access to Sensitive Information.

1 Passport, visa, and USCIS information for all foreign visitors and assignees must be validated before access is granted.

2 SME reviews in security (including cyber, technical, and OPSEC), export control, and technology transfer are required for nonsensitive country nationals. SME reviews in security (including cyber, technical, and OPSEC), export control, technology transfer, counterintelligence, and intelligence (when there is a field intelligence element onsite) are required for nationals of state sponsors of terrorism, sensitive country nationals, and requests involving access to sensitive subjects. If an export license is required, it must be granted before the first day of access.

3 Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access and must be approved in accordance with paragraph 3h(2)(b) of this CRD.

4 Access requests for sensitive country national assignees, and for requests involving access to sensitive subjects, must be entered into FACTS 30 days before access. Access requests for nonsensitive country nationals must be documented in FACTS prior to access.

5 Indices checks for all nationals of state sponsors of terrorism must be completed prior to site approval determination. Indices checks for sensitive country

national assignees and visitors, and for requests involving access to sensitive subjects, must be completed before final access approval determination.

6 Closeout information must be documented in FACTS within 15 days of the last day of access by the visitor or assignee.

(4) Offsite Locations. These include meetings and other offsite activities that have not been determined to be public events by the site approval authority.

(a) Passport, visa, and USCIS information for all foreign visitors and assignees must be validated before access is granted.

(b) SME reviews in security (including cyber, technical, and OPSEC), export control, and technology transfer are required for nonsensitive country nationals. SME reviews in security (including cyber, technical, and OPSEC), export control, technology transfer, counterintelligence, and intelligence (when there is a field intelligence element onsite), are required for nationals of state sponsors of terrorism, sensitive country nationals, and requests involving access to sensitive subjects. If an export license is required, it must be granted before the first day of access.

(c) Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access and must be approved in accordance with paragraph 3h(2)(c) of this CRD.

(d) Access requests for sensitive country national assignees, and for requests involving access to sensitive subjects, must be entered into FACTS 30 days before access. Access requests for nonsensitive country nationals must be documented in FACTS prior to access.

(e) Indices checks for all nationals of state sponsors of terrorism, sensitive country national assignees and visitors, and for requests involving access to sensitive subjects must be completed before final access approval determination.

(f) Closeout information must be documented in FACTS within 15 days of last day of access.

(5) All Other Security Areas. These include all physical spaces, except for those areas described above, designated as containing safeguards and

security interests that require physical protection measures. Before foreign national access can be approved the following requirements must be met.

(a) Passport, visa, and USCIS information for all foreign visitors and assignees must be validated before access is granted.

(b) SME reviews must be completed in security (including cyber, technical, and OPSEC), export control, technology transfer, counterintelligence, and intelligence (when there is a field intelligence element onsite).

(c) Access requests for nationals of state sponsors of terrorism must be entered in FACTS at least 30 days before the first day of access and must be approved in accordance with paragraph 3h(2)(b) of this CRD.

(d) Requests for visits and assignments must be entered into FACTS 30 days before the first day of access.

(e) Indices checks are required for all nationals of state sponsors of terrorism and must be completed before site approval determination. Indices checks are required for all sensitive country nationals and nonsensitive country nationals and must be completed before final approval determination.

(f) Closeout information must be documented in FACTS within 15 days of the last day of access.

(6) Special Situations.

(a) Foreign national emergency responders and medical personnel who require access to medical facilities or services for medical emergencies are excluded from the preaccess approval requirements of this Order. This exclusion is expressly conditioned upon a facility's compliance with site-specific security measures.

(b) Policy for remote cyber access by foreign nationals will be drafted by the Office of the Chief Information Officer and issued by the Secretary of Energy.

(c) International Atomic Energy Agency (IAEA) visits that are not inspection activities, as defined in the agreement between the United States and the IAEA, or that otherwise do not involve classified information or technologies are unclassified and will be documented in accordance with this CRD. IAEA inspection

activities and other classified visits involving foreign nationals are governed by the requirements for classified visits.

(d) Visits by foreign national delivery, service, and vendor personnel must be covered by site security plans and policies. If fully escorted, these foreign nationals do not require documentation in FACTS. If not escorted, the visits must be in compliance with the requirements for the location of access, as described above.

(e) Foreign National participation in Work for Others projects which involves access to DOE sites, facilities, or Laboratories, or to DOE information that is not releasable to the public, are considered visits and assignments and will be in accordance with all requirements of this CRD.

4. RESPONSIBILITIES.

a. Head of the Hosting Site/Facility. Hosting sites may include contractor operated field sites, national laboratories, and other DOE operating entities.

(1) Consistent with the assignment of authority through the line management chain, serves as approval authority for UFVA activities and programs within his/her organization.

(2) Develops plans and procedures, for approval by the cognizant Federal field element, for reassignment of approval authority to other U.S. citizen contractor employees.

(3) Provides written reassignment of approval authority after approving related plans and procedures and provides copies of reassignment documents to the cognizant DOE field element, the cognizant LPSO, the local foreign visits and assignments office, and the Office of Security.

(4) Ensures that all persons who are re-assigned approval authority are fully aware of their roles and responsibilities.

(5) Implements the UFVA program consistent with guidance and direction from the head of the DOE field element with direct responsibility for program performance.

(6) Incorporates all program-specific guidance into local program management processes and procedures, and ensures that all technical and management control requirements of this CRD are incorporated into the local management process established to approve access by foreign nationals, including full documentation in FACTS.

(7) Designates a point of contact (POC) for UFVA program management, and provides contact information to the Office of Security, the head of the

DOE field element, and the LPSO. Ensures that the POC is fully knowledgeable of program issues and activities.

(8) Ensures program-specific guidance is issued and being followed, corrective actions are being implemented as appropriate, and program responsibilities associated with the presence of foreign nationals are being met.

(9) Ensures a systematic, effective process to provide managers, planners, and hosts with appropriate guidance and insight regarding all technologies and information that could lead into sensitive or export controlled areas before approving access to these activities by foreign nationals. The process will include reviews to ensure the appropriate identification of sensitive or expert controlled technologies and/or information. The process should be conducted at least annually and more often if changes in circumstances indicate the need for a subject matter review.

(10) Ensures that the requirements of this CRD are applied to Work for Others projects that require foreign national access to DOE sites, facilities or laboratories, or to DOE information that is not releasable to the public.

(11) Ensures that the UFVA program is included in organizational self-assessments.

(12) Ensures that security incident reports are filed for violations or for deviations in the status of a foreign national.

b. Hosting Unclassified Foreign Visitors and Assignees. The contractor hosting a UFVA is directly responsible for the activities associated with the successful accomplishment of the visit or assignment. The contractor must ensure that foreign nationals hosting other foreign nationals are DOE contractor employees. For laboratories or facilities that perform no classified work, and at which no classified materials are stored, the contractor may allow sensitive country nationals (to exclude nationals of state sponsors of terrorism, who may not host other foreign nationals) to host only nonsensitive country nationals for visits and assignments that do not involve access to sensitive information. For all other sites, facilities and laboratories, the contractor must ensure that sensitive country foreign nationals (to include nationals of state sponsors of terrorism) do not host other foreign nationals.

The contractor must ensure that the host for a UFVA is identified to the visitor or assignee as his/her POC, and that the following requirements are met.

(1) Ensure compliance with all requirements for access approval and conduct, including timely, complete, and accurate information for FACTS; security plans; SME reviews; environment, safety, and health reviews and requirements; program sponsorship (such as exchange visitor programs); and notification to workers regarding requirements as appropriate.

(2) The contractor is responsible for the conduct and activities of the foreign nationals for whom it is identified as the host.

(3) Ensure that hosts for UFVA complete annual security briefings/certifications.

(4) Ensure that suspicious activities are reported in accordance with local reporting requirements to include the local counterintelligence office and the local incidents and infractions reporting office.

(5) Provide the following information to the foreign nationals the contractor is responsible for hosting.

(a) The terms and conditions of access approval, including restrictions and requirements to notify the host of changes in name or status (e.g., passport, visa or other USCIS information), and other pertinent information, as required.

(b) The requirement to notify the responsible host of any civil or criminal problems that could affect their status and association with DOE.

(c) That the failure to provide appropriate documentation when required or providing fraudulent documentation will result in suspension of access approval, removal from the site/facility, and possible cancellation of future access.

c. Escorting Foreign National Visitors and Assignees. The contractor is responsible for ensuring that, when required, foreign nationals working or traveling within a site/facility are escorted to ensure there is no unauthorized access. The contractor must also ensure that, with the exception of authorized hosts at laboratories or facilities that perform no classified work and at which no classified materials are stored, sensitive country foreign nationals may not serve as escorts. The contractor is responsible for the following.

(1) Ensuring that escorts are familiar with the site/facility, including security areas.

(2) Ensuring that escorts have full understanding and knowledge of security plan requirements.

(3) Ensuring that escorts have knowledge of specific information or technologies to which the foreign national has been authorized to ensure that there is no unauthorized access.

(4) Ensuring that escorts have appropriate clearance required for escort duties as required by hosting site security.

**UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS PROGRAM DEFINITIONS**

Approval Authority—The individual who has been assigned the responsibility and accountability to approve requests for access by foreign nationals to one or more DOE sites, programs, information, and technologies. Officials who assign approval authority are responsible and accountable for ensuring that the authority assigned is implemented consistent with the requirements of DOE O 142.3 or its associated Contractor Requirements Document, program Secretarial Officer (PSO) program guidance, and lead PSO management requirements.

Assignee—A foreign national who has been approved to access a DOE site, information, or technology for a period of more than 30 consecutive calendar days, but less than 2 full, consecutive years (24 consecutive months).

Assignment—Foreign national access for more than 30 consecutive calendar days, but less than 2 full, consecutive years (24 consecutive months). An assignment may be extended for additional periods of up to 2 years each after required reviews and approvals are completed for each extension. Approval for assignments will be suspended any time a foreign national assignee is unable to prove he/she is legally present in the United States.

Cancelled After Approval—A Foreign Access Central Tracking System (FACTS) closeout term for visits or assignments which are cancelled after access approval has been granted.

Cancelled Before Approval—A Foreign Access Central Tracking System (FACTS) closeout term for visits or assignments which are cancelled before final access approval determination.

Closeout Information—The final action data in the Foreign Access Central Tracking System (FACTS) for a visit or assignment. Closeout information includes the documentation of the completion of an approved visit or assignment as cancelled, no show, or complete.

Completed—A Foreign Access Central Tracking System (FACTS) closeout term for visits or assignments which have taken place and ended.

Dual Citizenship—Recognition as a citizen by more than one country.

Escort—An authorized DOE or DOE contractor employee who has been assigned the responsibility to accompany foreign nationals who lack need-to-know or access authorization within a security area to ensure adherence to security measures.

Export Controlled Information—Certain unclassified Government information for which DOE is accountable and responsible and which requires a specific license or authorization to export and must be protected consistent with U.S. laws and regulations. Unrestricted dissemination of this information could reasonably be expected to adversely affect the U.S. national security and nonproliferation objectives.

Facility—An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on a site that is operated and protected as one unit by the Department or its contractor.

Foreign National—An alien. For the purposes of DOE O 142.3 or its associated Contractor Requirements Document, an alien is a person who was born outside the jurisdiction of the United States, is a citizen of a foreign government, and has not been naturalized under U.S. law.

Foreign National Status—The period of time a foreign national is authorized to be in the United States and what type, if any, work he/she can participate in while in the United States as determined by his or her valid passport, visa, and other Immigration and Naturalization Service documentation.

Host—The DOE or DOE contractor employee responsible for the day-to-day activities associated with the successful accomplishment of a visit or assignment. A foreign national who is a DOE or DOE contractor employee may be a host. A sensitive country national cannot host another foreign national from any sensitive country.

Indices Checks—A procedure whereby a request is made to appropriate U.S. Government agencies to determine whether information exists on a particular foreign national.

Legal Permanent Resident (LPR)—One who has the right to reside permanently and work in the United States. Unlike a U.S. citizen, however, an LPR does not have the right to vote and can be deported if, for example, convicted of certain crimes. An LPR may also be known as a permanent resident alien or Green Card holder.

National of a State Sponsor of Terrorism—A foreign national who was born in, is a citizen of, is employed by, or represents a government, company, institution, or other organization based in a country on the Department of State's List of State Sponsors of Terrorism.

National Security—The national defense and foreign relations of the United States.

National Security Assets—Department and Departmental contractor assets that require significant protection. These assets are nuclear weapons and their design, Category I and II quantities of special nuclear material, classified information, sensitive information, critical facilities, and valuable Government property.

No Show—A Foreign Access Central Tracking System (FACTS) closeout term for those visits or assignments for which a foreign national has been approved but fails to report.

Nonsensitive Country National—A foreign national who was born in, is a citizen of, is employed by, or represents a government, company, organization, or institution that is located in a county not on the Sensitive Countries List or the Terrorist Countries List.

Open Information—Information which is not protected by statute and which would be considered releasable to the general public.

Out of Status—A foreign national in the United States contrary to the terms and conditions established by the U.S. Citizenship and Immigration Service (USCIS) at the port of entry or approved by the USCIS after a request for extension, waiver, or change of status. A foreign national who is out of status may not be granted access to DOE sites, programs, or information. Status is documented on the USCIS Form I-94 (the Arrival/Departure Record) or I-95 (Crewman's Landing Permit) issued to the foreign national at the point of entry; an USCIS receipt for request for extension, waiver, or change of status; or the I-94 or I-95 card attached to the bottom on an USCIS Approval Notice (I-797). All out of status foreign nationals are unlawfully present in the United States. Unlawful presence most commonly occurs when the foreign national enters the United States without USCIS approval and/or stays past the expiration date on their I-94 or I-95 card.

Passport—A travel document issued by one's country of citizenship. It can be used for identification purposes and visa applications or entry to other countries.

Program-Specific Policy Or Guidance—Policy or guidance which is promulgated by the cognizant lead program Secretarial Office for a given site, facility, or laboratory.

Property Protection Area—A type of security area having boundaries identified with barriers and access controls for the protection of DOE property.

Public Area—an area accessible by the general public, and for which there are no requirements for security clearances, security escorts, or security logs, as documented in the site security plan.

Security Area—A physical space which has been designated as an area containing safeguards and security interests, which dictate the need for the imposition of physical protection measures to control access to and from the area. The types of security areas used within DOE include property protection areas, limited areas, exclusion areas, protected areas, material access areas, vital areas, and functionally specialized security areas, such as sensitive compartmented information facilities, classified computer facilities and secure communications centers.

Sensitive Countries List—A list of countries to which particular consideration is given for policy reasons during the DOE internal review and approval process for visits and assignments by foreign nationals. Countries may appear on the list for national security, nuclear nonproliferation, or terrorism support reasons. The list is maintained by the Office of Defense Nuclear Nonproliferation.

Sensitive Country National—A foreign national who was born in, is a citizen of, or is employed by a government, employer, institution or organization, of a sensitive country.

Sensitive Subjects List—Unclassified subjects/topics identified in existing Federal regulations governing export control and by DOE as unique to its work; information, activities, and/or technologies relevant to national security. Disclosure of sensitive subjects has the potential for enhancing weapons of mass destruction capability and proliferation, divulging militarily critical technologies, or revealing other advanced technologies which may adversely affect U.S. national and economic security. These subjects require special management oversight before release to

foreign nationals. The list of sensitive subjects is maintained by the Office of Defense Nuclear Nonproliferation.

Site—A geographical area where one or more facilities are located or a DOE-controlled land area including DOE-owned facilities (e.g., the Oak Ridge Reservation, the Nevada Test Site, the Hanford Site, Idaho National Engineering Laboratory, Rocky Flats Plant, Feed Materials Production Center).

State Sponsors of Terrorism—Countries that have been identified by the Department of State as sponsors of groups and/or activities which support terrorism or terrorist activities and are on the List of State Sponsors of Terrorism.

Subject Matter Expert—An employee who is knowledgeable about the professional standards, requirements, and practices used within the discipline he/she represents (i.e., security, export control, technology transfer, counterintelligence, or intelligence).

System of Records—A document published in the Federal Register that describes the type of information being maintained on U.S. persons by a U.S. Government agency whenever the information can be retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual as identified in the Privacy Act. The document details who will have access to the information, for what purposes, and how the information will be stored and destroyed.

Technology—Technical data, skills, know-how, or scientific information. Technology is derived from basic or applied research, development, engineering, technological demonstration, economic and social research, or scientific inquiry into phenomena or technology applications. It may exist as machinery or equipment; may be recorded, spoken, or represented in a medium for storage of communication; and may be contained in computer software with scientific and technical applications.

U.S. Citizen—As provided for in the U.S. Constitution, a person entitled to all Constitutional rights and privileges of citizenship.

Visa—A permit to enter the United States that establishes a particular status (immigrant/nonimmigrant, student, exchange visitor, diplomat, etc.) evidenced by a stamp in the passport or the status described on U.S. Citizenship and Immigration Service (USCIS) Form I-94 or I-95. A visa is not a guarantee that the foreign national will be permitted to enter the United States. Admission is the responsibility of the USCIS at the port of entry.

Visa Requirement Waivers—A foreign national request to the USCIS that the requirements of his or her visa be waived (for example, a request to waive the 2-year return home requirement for Government J-1 visa holders). A waiver request is submitted to the USCIS for approval, and a receipt for that request is obtained to verify that the request was made. Whether the foreign national is permitted to work during the period after his or her visa has expired until the USCIS makes a determination on the visa waiver request is determined by the requirements of the visa involved.

Visa Waiver Program—A State Department-managed program that enables travelers from certain countries to visit the United States for business or pleasure (but not employment) for up to 90 days without a visa document. Generally, this includes the Western European countries and others with whom the United States has established reciprocal visa waiver agreements. A traveler who entered the United States under the Visa Waiver Program may not extend his or her stay or change status while in the United States.

Visit—Access by a foreign national for 30 calendar days or less. Approval for visits will be suspended any time a foreign national assignee is unable to prove he/she is legally present in the United States.

Visitor—A foreign national who has been approved to access a site, information, or technology for 30 calendar days or less.

Work for Others—Research, development, testing, manufacturing, or experimentation conducted at a DOE facility for an Agency other than DOE.

Work Permit—An informal term for what is more properly known as an Employment Authorization Document issued to foreign nationals for specific circumstances such as student authorization for practical training, family members of J-1 visa holders, and other specific situations.