

[Search SBMS »](#)
[\[Add to Favorites\]](#)
[\[Introduction\]](#) [\[Contents\]](#) [\[Forms/Exhibits\]](#) [\[References\]](#) [\[Definitions\]](#) [\[Keywords\]](#) [\[Changes\]](#)
Management System: [Security](#)
Subject Area: Foreign National Visits and Assignments (Unclassified)
 [VIEW/PRINT ALL \(No Exhibits and Forms\)](#)

 Effective Date: **Aug 25, 2016** ([Rev 7.1](#))
 Periodic Review Due: **Apr 29, 2021**

 Subject Matter Expert:
[Leonard Butera](#)

 Management System Executive:
[John Carney Jr](#)

 Management System Steward:
[Amy Nunziata](#)

Introduction

Applicability

This subject area applies to all BNL and non-BNL staff, which includes employees, guests, visitors, and sub-contractors.

Scope

This subject area provides procedures for processing unclassified visits (30 days or less) and assignments (more than 30 days, less than 2 years) of foreign nationals who require access to the BNL site, BNL/DOE information, or BNL-sponsored off-site events. Additionally, it describes the process for qualifying both on-site and off-site events as Public Events. Unclassified events and activities that occur outside the United States or its territories are not required to be processed in accordance with this subject area, but may require documentation in the Foreign Travel Management System, or reporting to the Brookhaven Counterintelligence Field Office. This subject area applies only to unclassified activities. For information on classified foreign visits contact the [Personnel and Information Security Group](#).

General

For the purposes of Foreign Visits and Assignments (FV&A) requirements, a foreign national is defined as a person who was born outside the jurisdiction of the United States, is a citizen of a foreign country, and has not become a naturalized U.S. citizen under U.S. law. This includes Legal Permanent Residents (also known as Permanent Resident Aliens). The FV&A requirements do not apply to foreign nationals that have become naturalized U.S. citizens.

Additionally, information that is disseminated, by any means, to a foreign national may be subject to export-control regulations, proprietary agreements, or other Federal regulations governing the dissemination of sensitive information and technologies; therefore all Laboratory personnel must be aware that providing, purposely or inadvertently, controlled commodities or information to foreign nationals without the appropriate clearances or licenses not only violates DOE and applicable Federal Directives, but may incur severe fines on the Laboratory for violation of Export Administration Regulations or Proprietary contracts. For further information on export-controlled and sensitive technologies contact the [Export Control Office](#).

The Department of Energy (DOE) and the Laboratory support an active program of unclassified visits and assignments by foreign nationals that includes the exchange of scientific and technical information and personnel. Such activities are viewed as part of a program for international cooperation in science, as long as they are consistent with or related to DOE and Laboratory missions in basic science, energy, national security, the environment, or the protection of public health and safety. The Laboratory also recognizes the need for foreign nationals to access the site in order to participate in non-work-related activities, such as family member visits and attendance at recreational or cultural activities sponsored by the Laboratory.

The Laboratory is firmly committed to fulfilling DOE Directives and requirements regarding foreign visits and assignments. Unclassified foreign visits and assignments are to be used to advance Laboratory program objectives consistent with U.S. foreign policy, nonproliferation policy, international energy policy and agreements, and national security policy and objectives. All employees are responsible for protecting counterintelligence interests, security interests, and sensitive subject information and technologies in a manner consistent with program requirements, including compliance with export laws and regulations. By maintaining a comprehensive review and approval process before permitting foreign nationals access to property or information

under the purview of the Laboratory, the FV&A program helps to ensure the protection of DOE/BNL assets while supporting the Laboratory's scientific mission.

Approval for visits and assignments will be suspended any time a foreign national is unable to prove he/she is legally present in the United States. See [ID Requirements for Guests & Visitors](#), [The Guide to Brookhaven National Laboratory \(BNL\)](#). Foreign national visitors and assignees that fail to comply with BNL policies are subject to suspension of access approval, removal from the site, and possible cancellation of future access.

All staff are responsible for reporting incidents involving foreign nationals in accordance with local reporting requirements. See [Reporting Incidents of Security Concern](#), [Laboratory Protection Division](#) for more detailed information.

Contents

Section	Overview of Content (see section for full process)
1.Planning a Foreign National Visit/Assignment	<ul style="list-style-type: none"> • Complete form. • Assign host. • Determine the visitor's type of visit and country status. • Identify facilities the foreign national will access. • Determine computer access. • Review visit/assignment parameters and determine processing time and approval requirements. • Ensure visitor registers in the Guest Information System.
2. Processing a Visit/Assignment Request	<ul style="list-style-type: none"> • Register in the Guest Information System. • Assign host, who initiates a Security Plan, if necessary. • Complete all reviews for general approval. • Process package for approvals for visitors from State Sponsor of Terrorism countries. • Obtain approvals.
3. Special Categories	<ul style="list-style-type: none"> • Submit forms and obtain approvals for accompanying family members and casual visitors of foreign nationals. • Complete forms for delivery/service/vendor staff who are foreign nationals. • Escort such staff on-site and ensure they exit the Main Gate.
4. Qualifying Events as Public Event Requests (PERs)	<ul style="list-style-type: none"> • Assign host for event. • Register in the Public Event Request System. • Complete form. • Review, approve, and process request. • Submit Main Gate Access Form for approved event.
5. Hosting/Escorting Foreign Nationals	<ul style="list-style-type: none"> • Complete training. • Review BNL 473 Form. • Advise visitor of responsibilities, monitor accomplishments, ensure compliance with requirements, coordinate access for BNL computer systems. • Ensure compliance with close-out procedures.
6. Indices Check	<ul style="list-style-type: none"> • Obtain approvals. • Monitor indices for completion. • For short-term circumstances, request a counterintelligence consultation.
7. Computer Access: Foreign Nationals	<ul style="list-style-type: none"> • Confirm type of access being requested. • Obtain approvals.

[Definitions](#)

Exhibits

[DOE Accompanying Family Member Designations](#)
[Field Parameters for Foreign National Casual Visits to BNL](#)
[Flowchart for State Sponsor of Terrorism \(SST\) Requests](#)

[Foreign Visits and Assignments Information Brochure](#)
[Foreign Visits and Assignments Requirements Matrix](#)
[Host Reference for Protecting Unclassified Controlled Information \(UCI\)](#)
[Property Protection Areas \(PPAs\)/Controlled Access Areas \(CAAs\)](#)
[Unclassified Foreign Visits and Assignment Program Reviewer/Approval Authority Guide](#)

Forms

[Accompanying Family Member Form](#)
[Cyber Security Plan for Foreign National Visitor Access to Unclassified Computer Resources](#)
[DOE Request Memo](#)
[OPSEC Security Plan for Unclassified Foreign National Visit/Assignment](#)
[Record of Escorted Visit](#)
[Request for Foreign National Access Before Indices Completion](#)
[Specific Security Plan](#)
[State Sponsor of Terrorism Processing Checklist](#)

Training Requirements and Reporting Obligations

This subject area contains training requirements. See the [BNL Training and Qualifications](#) Web site.

This subject area does not contain reporting obligations.

External/Internal Requirements

Requirement Number	Requirement Title
15 CFR 730-774 [2015]	TITLE 15--Commerce and Foreign Trade, Parts 730-774, Bureau of Industry and Security, Dept of Commerce; [2015]
22 CFR 120-130 [2015]	Title 22--Foreign Relations, Department of State, Parts 120-130, International Traffic in Arms Regulation
BSA Contract No. DE-SC0012704 - Clause H.31	Intellectual And Scientific Freedom
BSA Contract No. DE-SC0012704 - Clause I.121	Counterintelligence (dec 2010)
N 205.2	CRD - Foreign National Access to DOE Cyber Systems
O 142.3A (OCT 14 2010)	CRD - Unclassified Foreign Visits and Assignments Program (OCT 14 2010)
O 470.5 (June 2, 2014)	Insider Threat Program

References

[Badges, Passes, and Vehicle Identification](#) Subject Area

[BNL Training and Qualifications](#) Web site

[Cyber Security, Unclassified](#) Subject Area

[Guests and Visitors](#) Subject Area

[Guest Information System \(GIS\)](#)

[ID Requirements for Guests & Visitors, The Guide to Brookhaven National Laboratory \(BNL\)](#)

[Main Gate Access Form](#)

[Operations Security \(OPSEC\)](#) Subject Area

[Public Event Request \(PER\) Form](#)

[Reporting Incidents of Security Concern, Laboratory Protection Division](#)

Standard Practice Instruction (SPI) 5-14, Counterintelligence Program**Standards of Performance**

All staff and guests shall assure that only appropriately authorized individuals have access to facilities, information, resources, and assets.

All staff and guests shall comply with applicable Laboratory policies, standards, and procedures, unless a formal variance is obtained.

All staff and guests shall appropriately protect accountable materials, classified matter, sensitive information, resources, and assets.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

| [SBMS Home Page](#) | [Subject Areas](#) | [Changes](#) |

Questions/Comments

Disclaimer

Search...

Search SBMS »

Management System: [Security](#)Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)**1. Planning a Foreign National Visit/Assignment**Effective Date: **Aug 16, 2016**Subject Matter Expert: [Leonard Butera](#)Management System Executive: [John Carney Jr](#)**Applicability**

This information applies to organizations who sponsor foreign visits and assignments and their hosts.

Required Procedure

Foreign nationals sponsored for visits or assignments may include the following:

- Officials or other persons employed by foreign governments or other foreign institutions, which may or may not be involved in cooperation under international agreements;
- Foreign students at U.S. institutions;
- Employees of DOE or other U.S. Government agencies or their contractors, of universities, of companies (professional or service staff), or of other institutions; and
- Prospective employees of DOE or DOE contractors.

Processing requirements and lead-time are determined by assessing the following factors:

- Country status (Sensitive, Non-Sensitive, State Sponsor of Terrorism);
- Area type to be accessed (Property Protection Area [PPA] w/o sensitive, PPA w/sensitive, Non-Security, and Controlled Access Areas [CAA]);
- Information/technology type to be accessed (Open Research, Sensitive/Controlled);
- Duration of request (Visit, Assignment).

To avoid delay or denial of site access, all requests for visits and assignments by foreign nationals must be submitted as soon as possible.

After obtaining approval, visitors should be advised to arrive during normal business hours whenever possible and to arrive with their "Boarding Pass" issued upon approval to avoid any delays at the Main Gate.

Step 1	<p>The sponsoring organization determines if a BNL 473 Form, "Request for Foreign National Unclassified Visit or Assignment" is required. The BNL 473 Form is generated electronically during registration in the Guest Information System (GIS). Paper copies may be used by sponsoring department staff to collect the necessary information from the visitor before data entry in the GIS system; however, paper copies will not be accepted by the Foreign Visits & Assignments (FVA) Office.</p> <p>Any foreign national attendees to Public Events (PE) events using on-site housing must process a BNL 473 Form, which is required for all foreign national access to the BNL site or BNL/DOE information except for the following:</p> <ul style="list-style-type: none"> • Attendees to events or activities officially determined to be PE (e.g., public lectures, community meetings, cultural or entertainment events, open house events) in accordance with the section Qualifying Events as Public Event Requests (PERs). • Access by foreign nationals 17 years of age or younger, who are involved in non-work-related activities (school tours, family days, etc); • Unclassified events and activities that occur outside the United States or its territories; • Delivery, service, vendor and emergency response/medical staff as handled in accordance with the section Special Categories.
Step 2	<p>The sponsoring organization identifies a host(s) for each visit and assignment. The assigned host must meet all requirements and responsibilities as stated in the section Hosting/Escorting Foreign Nationals. The responsible host(s) will be familiar with the Specific Security plan, if any, and coordinate with the appropriate GIS department administrator for assistance with the request process.</p>
Step 3	<p>For all requests requiring a BNL 473 Form, the host determines if the request is defined as a visit or an assignment.</p> <ul style="list-style-type: none"> • A visit is defined as foreign national access for 30 calendar days or less. • An assignment is defined as foreign national access for more than 30 calendar days, but less than 2 years. <p>Note: An assignment may be extended for additional 2-year periods by generating an extension to the BNL 473 Form and obtaining the required reviews and approvals for each extension.</p>
Step 4	

	The host determines the visitor's country status (non-sensitive, sensitive, State Sponsor of Terrorism) by contacting the Brookhaven Counterintelligence Field Office . Country status is based on the following: <ul style="list-style-type: none"> • Country of Birth; • Country of Citizenship; and • Country of Employer/Affiliation.
Step 5	The host evaluates all controlled information access requirements in accordance with the Hosts Reference for Protecting Unclassified Controlled Information (UCI) . Requests involving access to sensitive or controlled information must be submitted to the FVA Office a minimum of 45 days before the start date.
Step 6	The host identifies facilities to be accessed as open areas, Controlled Access Areas (CAA), or Property Protection Areas (PPA). If the visitor/assignee will be accessing a CAA or PPA, contact the Information Security Office or Laboratory Protection Manager to determine if the PPA is designated as sensitive or non-sensitive. Access to a PPA designated as sensitive must be submitted to the FVA Office a minimum of 45 days before the start date.
Step 7	The host coordinates with the applicable system administrator(s) to determine computer access. Access by foreign nationals to certain computer systems, programs, and electronically stored data are strictly controlled or prohibited. See the section Computer Access: Foreign Nationals and the Cyber Security, Unclassified Subject Area for further information.
Step 8	Escorts may need to be assigned for safety or security purposes. The building manager or supervisors of areas to be accessed can assist in determining escort requirements. All assigned escorts must meet the requirements in the section Hosting/Escorting Foreign Nationals .
Step 9	The host reviews visit/assignment parameters in accordance with the Foreign Visits and Assignments Requirements Matrix to determine processing time and approval requirements.
Step 10	The host or sponsoring department administrator must identify the host to the visitor/assignee as his/her BNL point of contact and ensure registration in the Guest Information System (GIS) .
Step 11	The host advises all foreign national visitors not to come to BNL until they are officially notified that final approval has been granted. Upon approval, the visitor will be issued an access approval form called a "Boarding Pass", which should be brought to the Lab and shown at the Main Gate entrance to facilitate site access.

References

[Cyber Security, Unclassified](#) Subject Area

[Guest Information System \(GIS\)](#)

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

| [SBMS Home Page](#) | [Top of Subject Area](#) | [Instructions](#) | [Changes](#) |

Questions/Comments

Disclaimer

Search...

Search SBMS »

Management System: [Security](#)Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)**2. Processing a Visit/Assignment Request**Effective Date: **Aug 16, 2016**Subject Matter Expert: [Leonard Butera](#)Management System Executive: [John Carney Jr](#)**Applicability**

This information applies to sponsoring organizations of foreign national and foreign nationals who wish to access the BNL site, BNL internal network computer resources, or attend BNL sponsored off-site events that have not been approved as PublicEvents in accordance with the section [Qualifying Events as Public Event Requests \(PERs\)](#). Additional information is also available in the section [Special Categories](#), which addresses special situations such as visits by accompanying family members and delivery staff.

Required Procedure

Processing a Visit/Assignment Request contains two subsections:

[2.1. General Requirements for Visit/Assignment Requests](#)**[2.2. Additional Requirements for a State Sponsor of Terrorism \(SST\) Country Foreign National](#)**

Requests involving access by individuals associated with a State Sponsor of Terrorism (SST) country must meet the requirements specified in both subsections.

DOE recognizes three distinct categories of countries:

Non-sensitive;

Sensitive;

State Sponsor of Terrorism (SST).

Processing requirements and lead-time are determined by assessing the following factors:

- Country status (Non-Sensitive, Sensitive, State Sponsor of Terrorism);
- Area type to be accessed (General Access Areas, Property Protection Areas with or without sensitive, Non-Security Areas, and Off-site Visits/Assignments);
- Information/technology type to be accessed (CRADA [Cooperative Research and Development Agreement], Open and Open Data Research, Proprietary, Sensitive/Controlled, and WFO [Work for Others]);
- Duration of request (Visit - less than 30 days; Assignment - more than 30 days and up to 2 years).

Country status (Non-Sensitive, Sensitive, State Sponsor of Terrorism) is based on the Country of Birth, Country of Citizenship, and/or Country of Employer/Affiliation. In addition to the country status for State Sponsor of Terrorism (SST) Nationals, processing includes separate approvals for 1) Legal Permanent Residents and Subsequent Site Visits (or Extensions), and 2) Initial site visits/assignments. For assistance in determining the visitor's SST status, contact the [Brookhaven Counterintelligence Field Office](#).

UFVAs may require indices checks based on the involvement of nationals of state sponsors of terrorism or sensitive country nationals, sensitive subjects, or access to security areas other than general access areas (GAAs) or certain property protection areas (PPAs). Indices checks are requested through the process of documenting access requests in FACTS.

In cases where indices checks must be completed before access approval determination: The request must be documented in FACTS with sufficient time to complete the indices checks. It is recommended that the request be entered into FACTS 30 days prior to the start date of the request to ensure adequate time for completion of indices checks.

Indices checks are not required to be completed prior to site access unless access is requested by a Non-Sensitive or Sensitive Country or SST National to Sensitive Subjects. In those cases where the indices are not completed prior to the start date, the approval authority may request a Counterintelligence Consultation in lieu of completion of the indices checks. Requests involving nationals of

State Sponsors of Terrorism require the indices check to be **completed** before granting access. Counterintelligence Consultations for SST Nationals may not be utilized until **30 days after requests are documented in FACTS**. Counterintelligence Consultations may not be employed as a standard alternative to indices checks.

Visit/assignment requests are routed electronically using the Guest Information System. Requests should always be submitted to the FVA Office as soon as possible to allow for unanticipated processing delays. Under most circumstances, **at a minimum**, all requests must be submitted to the FVA Office as follows:

- Non-sensitive country - 7 working days before the anticipated arrival date;
- Sensitive country - 30 calendar days before the anticipated arrival date;
- Sensitive subject or sensitive security area - 45 calendar days before the anticipated arrival date;
- State Sponsor of Terrorism (SST) country - 90 calendar days before the anticipated arrival date. (Extensions and LPR's are approved on-site 30 days for indices).

Submittal of incorrect or missing information to the FVA Office will result in processing delays and affect the aforementioned approval time frame. Additionally, changing world events may result in approval delays.

See the section [Planning a Foreign Visit/Assignment](#) for further information on determining visit/assignment parameters.

2.1 General Requirements for Visit/Assignment Requests

Step 1	In coordination with the sponsoring Department/Division staff, the guest registers using the Guest Information System (GIS) . At the time of the initial registration, any known requested information and accompanying family members should be entered into the GIS.
Step 2	The completed registration is electronically submitted to the sponsoring department. This process generates a BNL 473 Form, Request for Foreign National Unclassified Visit or Assignment. Note: If the organization is not identified, the system directs the request to Human Resources (HR) Records where the record is reviewed to determine the appropriate sponsoring organization.
Step 3	If not previously arranged, the sponsoring Department/Division being visited assigns a host for the foreign national. The assigned host must meet the requirements specified in the section Hosting/ Escorting Foreign Nationals , and complete the required training (Hosting and Escorting Foreign Nationals [TQ-SEC-FN]).
Step 4	If applicable, sponsoring Department/Division staff will provide additional Department/Division-specific information, such as the need for administrative support (insurance, housing, phone, email).
Step 5	If required (see the exhibit Foreign Visits and Assignments Requirements Matrix), a specific security plan is automatically generated in the BNL 473 Form. The Host reviews the data in the security plan and makes any necessary modifications or additions.
Step 6	The sponsoring Department GIS Administrator reviews the request for accuracy and completeness.
Step 7	Upon receiving Department/Division approvals, and if required, the Immigration Group (Human Resources) reviews, Human Resources or the Guest User Visitor Center (GUV) routes the request to the FVA Office . Note: If you are processing a request for a State Sponsor of Terrorism National, refer to subsection Additional Requirements for a State Sponsor of Terrorism (SST) Country Foreign National for information on preparing the SST package.
Step 8	The GUV Office reviews the data for accuracy and completeness, and coordinates with the host/sponsoring Department/Division staff to resolve any discrepancies before continuing with the approval process. Once all issues regarding discrepancies and missing/inaccurate data have been resolved, the FVA Office continues processing the request.
Step 9	An automated Upload/Download process enters the request into the DOE Foreign Access Central Tracking System (FACTS), which initiates an Indices check if the request involves a sensitive country, sensitive subject and/or access to a sensitive security area, or State Sponsor of Terrorism. See the section Indices Checks for further information.
Step 10	In those cases where a Subject Matter Expert (SME) Review is required, the FVA Office submits the request to the following SMEs for internal review: <ul style="list-style-type: none"> • Local Counterintelligence (CI); • Export Control (EC); • Operations Security (OPSEC); • Security (SE); • Technology Transfer (TT); • Cyber Security. The SMEs review the request in accordance with the Unclassified Foreign Visits and Assignment Program Reviewer/Approval Authority Guide , and document any concerns in the comments section of the BNL 473 Form.
Step 11	The Local Site Approval Authority uses the SMEs' input to determine approval or denial of the request, and returns the BNL 473 documenting the final determination to the FVA Office .
Step 12	After receiving approval authorization from the site approval authority, the FVA Office forwards the request to the GUV.
Step 13	If you are processing a request for a State Sponsor of Terrorism country, see additional requirements specified in the subsection Additional Requirements for a State Sponsor of Terrorism (SST) Country Foreign National .
Step 14	Once a final determination has been obtained, the GUV Office returns the request to the sponsoring department GIS Administrator.

Step 15	If approved, the visitor receives a system-generated email notification that final approval has been granted. If disapproved, the Site Approval Authority notifies the visitor.
Step 16	The sponsoring Department/Division does not need to submit a Main Gate Access Form for the primary foreign national listed on an approved BNL 473 Form; however, a Main Gate Access Form must be completed for visits by any accompanying family members listed on the BNL 473 Form who do not already possess a valid Family Member identification badge.
Step 17	All visitors/assignees, including accompanying family members, must present proper identification and applicable United States Citizenship & Immigration Services (USCIS) documentation upon arrival. For additional information see the Guests and Visitors Subject Area and the ID Requirements for Guests & Visitors .

2.2 Additional Requirements for a State Sponsor of Terrorism (SST) Country Foreign National

This information pertains to visits by foreign nationals who are born in, a citizen of, or affiliated with a State Sponsor of Terrorism country. For a list of State Sponsors of Terrorism (SST) countries, contact the [Brookhaven Counterintelligence Field Office](#).

In addition to the requirements set forth in the subsection [General Requirements for Visit/Assignment Requests](#), initial requests to the BNL site for visits/assignments by citizens of countries of State Sponsor of Terrorism (SST) will not take place, regardless of BNL approvals, until approved by the Deputy Secretary or cognizant Under Secretary. If the Deputy Secretary or cognizant Under Secretary does not approve the request, the BNL 473 Form is rejected via the Guest Information System. SSTs with status as Legal Permanent Residents or subsequent (extension) requests for those SST nationals previously at BNL, require completed indices and in accordance with the DOE Headquarters Office, approval at the Site Approval Authority level.

The [Flowchart for State Sponsor of Terrorism \(SST\) Requests](#) shows an overview of the review and approval process. All SST requests must be submitted to the FVA Office a minimum of 180 days before the anticipated arrival date.

Note: All forms are submitted in electronic format for review before obtaining internal signatures. Original hard copies must be signed and sent to DOE.

Step 1	Follow steps 1-13 in subsection General Requirements for Visit/Assignment Requests .
Step 2	If the Site Approval Authority approves the request, the FVA Office coordinates the submission and processing of the SST package, in coordination with the Counterintelligence Office, to the Deputy Secretary or appropriate Under Secretary. Guests who are from SST countries do not have approval to come on-site even when the BNL 473 Form has been locally approved. The final approval for access is not obtained until the DOE Review and Approval process is completed and the Deputy Secretary of Energy approves the request.
Step 3	The applicable Department/Division Administrator completes the DOE Request Memo , obtaining the FACTS Visitor and Request numbers and the Indices Check information from the FVA Office.
Step 4	The Host reviews the Operational Security Plan for Unclassified Foreign National Visit/Assignment , and in coordination with the Department/Division Administrator, completes the information in Question 8.
Step 5	The Department/Division Administrator, Host, the Department/Division Systems Administrator, and the Cyber Security Officer coordinate the preparation of a Cyber Security Plan for Foreign National Visitor Access to Unclassified Computer Resources for the guest. After approval by the Cyber Security Officer and Counterintelligence (CI), the Department/Division Administrator obtains signatures from their Department/Division representatives.
Step 6	The Department/Division Administrator coordinates with the Host and guest to obtain electronic copies of the USCIS and applicable Department of Justice (DOJ) documentation, including Passport and Visa, and any additional United States Citizenship & Immigration Services (USCIS) forms (i.e., I-94, I-20 A-B), driver's license (if any), and student or company ID (if any).
Step 7	The Department/Division Administrator obtains two justification letters, a resume, and a list of publications for the guest. At least one justification letter must be from a BNL employee, addressing the importance of the individual coming to BNL and how the benefits of the visit would be greater than the risk.
Step 8	The Department/Division Administrator submits the documentation to the FVA Office . Use the State Sponsor of Terrorism (SST) Processing Checklist to ensure you have completed all required documentation before submitting the package.
Step 9	The FVA Office reviews the registration, applicable Security Plans, and additional documentation to ascertain if there are any concerns with the paperwork. If there are no overriding concerns, the FVA Office forwards the "Package" to the Laboratory Subject Matter Experts for review and approval before obtaining signature approvals on the originals.
Step 10	The Senior Counterintelligence Officer conducts a quality assurance review on the package and provides it to the Laboratory Approving Authority, who is the final-site-approving authority for packages of SST nationals with LPR status or extension requests.
Step 11	Once final-site approval is obtained, the FVA Office makes copies and mails the original completed package for initial SST national requests to the DOE Office of Science and provides a copy of the request letter to the DOE Area office.
Step 12	The Office of Science forwards submitted the requests to the Counterintelligence Office.
Step 13	When the FVA Office receives the determination from either the Site Approving Authority or DOE, the BNL 473 Form, reflecting the final determination is sent to the SMEs, Department/Division Administrator, host, DOE Site Office, and the DOE Chicago Office.
Step 14	If approved, the guest receives a system-generated e-mail notification that site access is granted.
Step 15	If disapproved, the Local Site Approval Authority notifies the visitor.
Step 16	The sponsoring Department/Division does not need to submit a Main Gate Access Form for the primary foreign national listed on an approved BNL 473 Form; however, a Main Gate Access Form must be completed for visits by any accompanying family members listed on the BNL 473 Form who do not possess a valid Family Member identification badge.
Step 17	All visitors/assignees, including accompanying family members must present proper identification and applicable United States Citizenship & Immigration Services (USCIS) documentation upon arrival. For additional information, see the Guests and Visitors Subject Area and the ID Requirements for Guests & Visitors .

Note: During regular Lab hours and when the GUV center is open, it is permissible to allow foreign nationals access to the GUV Center for additional processing after being initially screened at the visitor trailer or main gate (depending on the time) and determining the visitor is going to be sponsored for a visit/assignment. The GUV Center will be responsible for providing full escort from the trailer/gate to B-400, during the entire time of processing, and then off-site if site access approval cannot be obtained that same day. The GUV center understands its responsibilities as outlined. Additionally, the GUV understands they are not authorized to unilaterally grant site access. They can advise if the person should be sponsored and sent down for processing and will provide additional information not available to LPD personnel in making access determinations. Off-hours screening/processing procedures remain the same. See ADM-217 Procedure updated March 2008.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

| [SBMS Home Page](#) | [Top of Subject Area](#) | [Instructions](#) | [Changes](#) |

Questions/Comments

Disclaimer

PROCEDURE: SPECIAL CATEGORIES

Management System: Security		
Subject Area: Foreign National Visits and Assignments (Unclassified)		
3. Special Categories		
Effective Date: Jan 15, 2015	Subject Matter Expert: Leonard Butera	Management System Executive: John Carney Jr

Applicability

This information applies to BNL staff and non-BNL staff who sponsor the following types of foreign national visitors or activities: accompanying family members; casual visitors; delivery/service/vendor staff; and off-site activities.

Sub-contractors are not permitted to invite family members or casual visitors to the BNL site except for events officially approved as Public Events in accordance with the section [Qualifying Events as Public Event Requests \(PERs\)](#).

Special Categories contains four subsections:

[3.1 Accompanying Family Members](#)

[3.2 Casual Visitors](#)

[3.3 Delivery/Service/Vendor Staff](#)

[3.4 Off-site Events Sponsored by BNL](#)

Required Procedure

3.1 Accompanying Family Members

An accompanying family member (AFM) refers only to relationships identified in the exhibit [DOE Accompanying Family Member Designations](#). Accompanying family members may tour the sponsor's work area, but are not permitted unescorted access to areas where actual work is being conducted, and are not permitted any access to areas where sensitive or classified information is stored or processed. Computer access must be limited to systems and connections that preclude access beyond the Visitor's Network (bnl.org). Additionally, the family member may not partake in any work-related activities. The host and sponsoring family member are responsible for ensuring that AFMs are apprised of, and adhere to, all Laboratory requirements applicable to the areas visited.

Step 1	Ensure the foreign national's relationship to the sponsoring family member appears in the exhibit DOE Accompanying Family Member Designations .
Step 2	Foreign national family members of a guest/employee that are U.S. Citizens must register in the Guest Information System (GIS) and be processed in accordance with the section Processing a Visit/Assignment Request .
Step 3	Foreign national family members of the guest/employee that are themselves foreign nationals may be added on to the guest/employee BNL 473 Form. All accompanying family member

	information should be entered into the record when the guest/employee initially registers in the GIS.
Step 4	If the guest/employee wants to have a family member visit whose information was not entered into the original registration, the sponsoring guest/employee must complete Section II of the Accompanying Family Member Form and submit it to the sponsoring department's GIS Administrator.
Step 5	The GIS Administrator completes Section I and II and submits the Accompanying Family Member Form (AFM) forms for guests, users, and visitors by fax to the GUV Center to fax number 8686. Forms for employees, contractors, or non-construction contractors, should be faxed over to Records at 3195. Forms for the Office of Education Programs (OEP) should be faxed to 5832.
Step 6	When the information is forwarded to the appropriate processing center, the data is entered into PeopleSoft. In addition, an automated upload enters the information into the DOE Foreign Access Central Tracking System (FACTS), and the sponsoring Department/Division GIS Administrator is notified that the information has been entered in the DOE and local systems. This process is usually completed in the same day.
Step 7	Upon completion of this process, the sponsoring department must submit a Main Gate Access Form before the arrival of the family member.
Step 8	All foreign national family members must present proper identification and applicable United States Citizenship & Immigration Services (USCIS) documentation upon arrival. For additional information see the Guests and Visitors Subject Area and the ID Requirements for Guests & Visitors .
Step 9	For information on obtaining family member badges at the completion of the approval process see the Badges, Passes, and Vehicle Identification Subject Area.

3.2 Casual Visitors

Due to the existence of on-site housing and BNL-sponsored educational/recreational events, Laboratory policy allows for guests and employees to be visited by persons that do not qualify as family members, but whose activities will not involve any official Laboratory or work-related purpose. These types of visits are defined as casual visits.

Casual visitors may tour the sponsor's work area, but are not permitted unescorted access to areas where actual work is being conducted, and are not permitted any access to areas where sensitive or classified information is stored or processed. Computer access must be limited to systems and connections that preclude access beyond the Visitor's Network (bnl.org). Additionally, the visitor may not partake in any work-related activities. The host is responsible for ensuring that casual visitors are apprised of and adhere to all Laboratory requirements applicable to the areas visited. All casual visit requests are subject to FV&A processing requirements. See the [Foreign Visits and Assignments Requirements Matrix](#) for further details.

Casual visits are only approved for site access of 30 days or less.

Step 1	The sponsoring Department/Division assigns a host(s) who meets all requirements and responsibilities as stated in the section Hosting/Escorting Foreign Nationals for all casual visitors. The responsible host(s) will coordinate with the appropriate GIS Administrator for assistance with the request process.
Step 2	All casual visitors must register via the Guest Information System (GIS) .
Step 3	When processing the request, the sponsoring Department/Division GIS Administrator enters field data in accordance with the exhibit Field Parameters for Foreign National Casual Visits to BNL .

Step 4	Upon receiving department approvals, the sponsoring Department/Division routes the request to the GUV Center. The request is processed in accordance with the section Processing a Visit/Assignment Request .
Step 5	All family members who will be accompanying the casual visitor are processed in accordance with the subsection Accompanying Family Members .
Step 6	The sponsoring department does not need to submit a Main Gate Access Form for the primary foreign national listed on an approved BNL 473 Form; however, a Main Gate Access Form must be completed for any family members accompanying the casual visitor.
Step 7	All foreign national casual visitors must present proper identification and applicable United States Citizenship & Immigration Services (USCIS) documentation upon arrival. For additional information see the Guests and Visitors Subject Area and the ID Requirements for Guests & Visitors .

3.3 Delivery/Service/Vendor Staff

Typically such persons are expected to only be on-site for short periods. If fully escorted by the sponsoring Department/Division, they do not need to register through the Guest Information System. If not fully escorted, the foreign national must be processed in accordance with the section [Processing a Visit/Assignment Request](#).

Foreign nationals making deliveries will be escorted to the delivery site and then escorted off-site by a Protective Force Officer. Foreign National vendors will be escorted by the hosting organization. The appointed escort must keep the foreign national under observation at all times while on-site. Escorts must be a DOE or BNL employee and adhere to escort requirements as specified in the section [Hosting/Escorting Foreign Nationals](#). Nationals of sensitive or State Sponsor of Terrorism (SST) countries cannot act as escorts.

Step 1	When a protective force officer is assigned to escort foreign national delivery staff, the officer will only escort the foreign national from the Main Gate to the delivery location and back off-site.
Step 2	All Department/Division staff who escort delivery, service, or vendor staff complete and sign a Record of Escorted Visit .
Step 3	For vendors and service staff, the assigned escort will meet the vendor at the Main Gate or protective force personnel will escort the vendor to the host facility and effect transfer to the Department/Division escort.
Step 4	The assigned escort takes responsibility for the vendor/service staff and stays with them the entire time they are on-site.
Step 5	The escort ensures the foreign national is only taken to areas essential to complete the job, and is not provided access to any sensitive or classified security areas.
Step 6	When vendor/service staff have completed the job, the escort must accompany the foreign national back to the Main Gate and confirm the foreign national exits the site.
Step 7	The escort reports any suspicious activities immediately in accordance with local reporting requirements. See Reporting Incidents of Security Concern for more detailed information.

3.4 Off-site Events Sponsored by BNL

Off-site events and activities are processed in the same manner as on-site events and activities. All off-site events that are sponsored by BNL, either solely or jointly, must adhere to the DOE Foreign Visits and Assignments requirements. Depending on the event parameters, an off-site event may be processed as a Public Event (PE) as long as it meets the following criteria:

- **Widespread notification.** Public Events (PE) are advertised in such a way as to provide invitation to a wide range of recipients, thereby preventing the sponsor from obtaining knowledge of all attendees before the event.
- **The general public, or general scientific community, is welcome to attend.** Anyone who shows up is to be permitted to attend the event. If unexpected attendees are going to be denied access to the event, the event is not considered PE.
- **Foreign Nationals are expected to attend.** If you are sure no foreign nationals will be attending the event, approval as PE is not required.
- **The event may not be held in a security area.** For example, a Property Protection Area (PPA) or a Limited Area.
- **Only Open Research, or information available to the general public, will be discussed.**

Step 1	If the event qualifies as a Public Event (PE), process in accordance with the section Qualifying Events as Public Event Requests (PERs) .
Step 2	If the event does not qualify as a PE, contact the Brookhaven Counterintelligence Field Office for assistance in determining the country status of all attendees.
Step 3	For off-site events that do not qualify as a PE, all foreign national attendees register via the Guest Information System (GIS) and are processed in accordance with the section Processing a Visit/Assignment Request .
Step 4	For off-site events that do not qualify as PE, foreign national employees provide passport, Visa, and USCIS information to BNL. The sponsoring Department/Division validates the information in accordance with the event location procedures before access is granted to the event.

References

[Badges, Passes, and Vehicle Identification](#) Subject Area

[Guests and Visitors](#) Subject Area

[Guest Information System \(GIS\)](#)

[Main Gate Access Form](#)

[Reporting Incidents of Security Concern, Laboratory Protection Division](#)

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

| [SBMS Home Page](#) | [Top of Subject Area](#) | [Instructions](#) | [Changes](#) |

Questions/Comments

Disclaimer

https://sbms.bnl.gov/sbmsearch/subjarea/185/185_pro3.cfm

Search...

Search SBMS »

Management System: [Security](#)**Subject Area:** [Foreign National Visits and Assignments \(Unclassified\)](#)**4. Qualifying Events as Public Event Requests (PERs)**Effective Date: **Aug 16, 2016**Subject Matter Expert: [Leonard Butera](#)Management System Executive: [John Carney Jr](#)**Applicability**

This information applies to sponsoring organizations and hosts of foreign nationals accessing the site for events or activities open to the general public.

Required Procedure

Events or activities that qualify as open to the general public are exempt from DOE Order 142.3A, Unclassified Foreign Visits and Assignments Program. Approval for such events may be submitted to FV&A on the Public Event Request (PER) form located on the BNL home page. Once approval is obtained, these events, social/recreational, or scientific, may be posted on the Main Gate Access. Frequently recurring events may be approved for a period of up to one year. For an event to qualify as a Public Event (PE), the following criteria must be met:

- **Widespread notification.** PE are advertised in such a way as to provide invitation to a wide range of recipients, thereby preventing the sponsor from obtaining knowledge of all attendees before the event.
- **The general public, or general scientific community, is welcome to attend.** Anyone who shows up is to be permitted to attend the event. If unexpected attendees are going to be denied access to the event, the event is not considered Open-to-the-Public.
- **Foreign Nationals are expected to attend.** If you are sure no foreign nationals will be attending the event, approval as a public event is not required.
- **The Event may not be held in a security area.** For example a Property Protection Area (PPA), Controlled Access Area (CAA), or a Limited Area.
- **Only Open Research, or information available to the general public, will be discussed.**

Foreign nationals accessing the site for a PE are only authorized to partake in the activities specified in the approval. Visitors cannot access the site for a PE and conduct any discussion, work, or activity that goes beyond the scope of the Public Event Request approval unless they have an individual BNL 473 Form approved for the additional activity in accordance with the section [Processing a Visit/Assignment Request](#).

PERs must be submitted to the FVA Office a minimum of 15 days before the requested start date. Submittal of incorrect or missing information to the FVA Office will result in processing delays and affect the approval timeframe.

Sponsors of recurring events are responsible for advising the FVA Office of any date or time changes that occur outside the date/time parameters originally submitted in the request.

News releases or other public advertisements for an event must not be posted before obtaining PER approval. Doing so may result in attendees being delayed or denied access to the site.

Step 1	The sponsoring organization identifies a host(s) for the Public Event. All hosts must meet the requirements as specified in the section Hosting/Escorting Foreign Nationals .
Step 2	The BNL sponsor of the event, or the sponsoring Department/Division administrator, completes the Public Event Request (PER) Form which is also on the BNL Homepage under BNL Site Access.
Step 3	Include a brief summary and agenda if available for requests for social or recreational events.
Step 4	For all scientific events, whether recurring or not, the host prepares a detailed summary of the topics to be discussed.
Step 5	For recurring scientific events, the host contacts the OPSEC Chair to ensure all activities i.e., seminars, lectures, to be held during the approved period, fall under the scope of Open Research.
Step 6	The host and sponsoring Department Chair/Division Manager or higher review and approve the request.
Step 7	After required Department/Division approvals have been obtained, the BNL sponsor of the event submits the PER Form to the FVA Office along with an agenda and event summary as applicable.
Step 8	The FVA Office reviews the data for accuracy and completeness, and coordinates with the host/sponsoring Department/Division staff to resolve any discrepancies before continuing with the approval process. Once all issues regarding discrepancies and suitability for PER approval have been resolved, the FVA Office continues processing the request.

Step 9	<p>The FVA Office submits the request to the following Laboratory Subject Matter Experts (SMEs) for internal review:</p> <ul style="list-style-type: none"> • Local Counterintelligence (CI); • Export Control (EC); • Operations Security (OPSEC); • Security (SE); • Technology Transfer (TT); • Cyber Security. <p>SMEs document any concerns in the comments section of the PER Form.</p>
Step 10	<p>After review by all of the SMEs, the FVA Office forwards the request to the Associate Laboratory Director (ALD) for Facilities and Operations for final approval.</p>
Step 11	<p>The ALD for Facilities and Operations (Local Final Approval Authority) uses the SMEs' input to determine approval or denial of the visit, and returns the request documenting the final determination to the FVA Office.</p>
Step 12	<p>Once a final determination has been obtained, sponsoring department's GIS administrator, the host and the Department Chair/Division Manager receive electronic notification of the determination.</p>
Step 13	<p>If the request has been approved, the FVA Office enters the event in the Main Gate PER Event calendar in the Public Folders under Laboratory Protection Division.</p>
Step 14	<p>The sponsoring department submits a Main Gate Access Form for each approved PER event. Main Gate notification forms must be submitted for each individual event in a recurring series. Enter the PE tracking number in the Comments field of the form.</p> <p>Note: Refer to the PE tracking number on all correspondence regarding the request.</p>

References

[Guest Information System \(GIS\)](#)

[Main Gate Access Form](#)

[Public Event Request \(PER\) Form](#)

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

| [SBMS Home Page](#) | [Top of Subject Area](#) | [Instructions](#) | [Changes](#) |

Questions/Comments

Disclaimer

Search...

Search SBMS »

Management System: [Security](#)**Subject Area:** [Foreign National Visits and Assignments \(Unclassified\)](#)**5. Hosting/Escorting Foreign Nationals**Effective Date: **Aug 16, 2016**Subject Matter Expert: [Leonard Butera](#)Management System Executive: [John Carney Jr](#)**Applicability**

This information applies to BNL staff and non-employees from non-sensitive countries, such as those holding Joint Appointments or researchers at user facilities and BNL administrative staff who assist a host in meeting these responsibilities.

The Host of Record, the individual listed in PeopleSoft as the host, is responsible for ensuring the following requirements are met. Sponsoring Department/Division administrative staff, as well as staff in the Guest, User, Visitor (GUV) Center and the Foreign Visits and Assignments Office (FVA Office) may assist the host in meeting these responsibilities. Vendor and service staff may also require assigned escorts. See the section [Special Categories](#) for additional information on escort of Delivery and Service staff. All hosts of foreign nationals must ensure they are familiar with the escort requirements for all areas to be accessed. Facility managers and supervisors can assist with providing this information.

Required Procedure

Hosts and escorts must be a DOE or DOE contractor employee. Non-employees from non-sensitive countries, such as those holding Joint Appointments and researchers at user facilities, may also act as hosts. All non-employee hosts fall under the same requirements and limitations as BNL employees. Foreign nationals who are affiliated with a sensitive or State Sponsor of Terrorism (SST) country may not act as hosts or escorts. For a current list of sensitive and SST countries, contact the [Brookhaven Counterintelligence Field Office](#). Co-hosts may be assigned to meet requirements during periods when the primary host may be unavailable due to official travel, authorized leave, etc.; however, the FVA Office must be notified of all assigned co-hosts before the co-hosts take on hosting responsibilities. All co-hosts must adhere to the same requirements, e.g., training, as primary hosts.

Hosts will be held accountable, to the extent that the situation warrants, if they do not report unusual or suspicious activities, whether observed directly or brought to their attention by other staff, that fall outside the scope of the approved visit/assignment, violate BNL security procedures, or are otherwise in contradiction to the purpose of the visit/assignment. Individuals hosting foreign nationals at BNL may be selected for a counterintelligence debriefing.

Step 1	All hosts, co-hosts, and escorts must complete Hosting and Escorting Foreign Nationals (TQ-SEC-FN) .
Step 2	For all foreign national visitors/assignees that you will be hosting, review the BNL 473 Form for accuracy and completeness.
Step 3	Review the Host Reference for Protecting Sensitive Information and ensure all potential access to sensitive information is accurately reflected in the BNL 473 Form.
Step 4	If the request involves a State Sponsor of Terrorism or sensitive country, sensitive subject, or access to a security area, select the "Security Plan" button on the BNL 473 Form to populate a Specific Security Plan. Note: A template is pre-populated with the visitor's/assignee's specific information and additional criteria may be added to the visit/assignment as necessary. Host-developed Specific Security Plans must be at least as restrictive as requirements specified in any existing facility security plans associated with the areas to be accessed.
Step 5	Ensure that all requests requiring Subject Matter Expert (SME) reviews are submitted to the FVA Office within the lead-time parameters specified in the Foreign Visits and Assignments Requirements Matrix .
Step 6	Identify yourself to the visitor/assignee as his/her BNL point of contact.
Step 7	Advise the visitor/assignee that he/she must maintain legal immigration status at all times when accessing the site, and must notify the host or administrative staff of all changes in personal or visit/assignment-related information or immigration status.
Step 8	Ensure the visitor/assignee understands his/her responsibilities and any limitations on the visit/assignment. Inform visitor/assignee of all BNL/ Department requirements applicable to the visit, such as safety, security, and operational procedures. Be sure to brief visitor/assignee on approved and precluded facility and information areas of access.
Step 9	Provide the visitor with pertinent information about, and ensure understanding and compliance with, requirements on cyber security and physical access, conduct while on-site, extension requirements, gate notifications, badging, security plan restrictions, training, use of equipment, invited guests and family members, and escort restrictions if applicable. Use the Foreign Visits and Assignments Information Brochure .
Step 10	Coordinate access and termination of access/permissions to BNL computer systems, i.e., databases and web sites, when applicable.

Step 11	<p>When required, foreign nationals working or traveling within a site/facility are escorted to ensure there is no unauthorized access. In situations where the host assigns another individual to act as escort, the host ensures the escort:</p> <ul style="list-style-type: none"> • Is a DOE or DOE contractor employee or a non-employee from a non-sensitive country who holds a Joint Appointment, or is a researcher at a user facility; • Is not a sensitive or SST country national. Contact the Brookhaven Counterintelligence Field Office for country designations; • Has been granted unescorted access to the areas of escort responsibility; • Is an individual who has a full understanding of the Facility Security Plan and activities that regularly occur in the security area; • Has knowledge of specific information and technologies to which visitor access has been authorized to ensure that no unauthorized access occurs; • Is responsible for no more than four visitors at any given time. <p>Brief all escorts on visit/assignment parameters, such as approved access for building areas and information. Escorts must stay in visual proximity to the foreign national at all times, and ensure no unauthorized access takes place. If acting as escort in a Property Protection Area (PPA) or Controlled Access Area (CAA), see the exhibit Property Protection Areas (PPAs)/Controlled Access Areas (CAAs) for further information.</p>
Step 12	<p>All staff who escort visitors who have not undergone the review and approval process, such as vendor and service personnel, complete and sign a Record of Escorted Visit.</p>
Step 13	<p>Adhere to applicable security plans to include specific facility plans when accessing PPAs/CAAs during visit/assignment. Contact the building manager or area supervisor for information on specific facility security plans. See the exhibit Property Protection Areas (PPAs)/Controlled Access Areas (CAAs) for further information.</p>
Step 14	<p>Notify the sponsoring department's GIS Administrator, GUV, or FVA Office when:</p> <ul style="list-style-type: none"> • Visit/assignment parameters may change; • Visitor no longer requires site access; • There are anticipated extended host absences during periods when the foreign national will be accessing the site. <p>Note: Reporting such situations assists with records maintenance and proper assigning of co-hosts.</p>
Step 15	<p>Regularly monitor the activities associated with the successful accomplishment of the visit or assignment, e.g., the progress and scope of an experiment, or equipment repairs and modifications.</p>
Step 16	<p>Identify and protect areas of work that are classified or sensitive. Be vigilant about not disseminating classified or sensitive information/technologies, e.g., Export Controlled Information, proprietary details concerning Cooperative Research and Development Agreements (CRADA), or providing access to controlled facilities/areas that have not been specified and approved under the visit/assignment request. See the Host Reference for Protecting Sensitive Information for further guidance.</p>
Step 17	<p>Ensure suspicious activities are reported immediately and in accordance with local reporting requirements, to include the local Counterintelligence Office and the local Safeguards and Security Division. See Reporting Incidents of Security Concern for more detailed information.</p>
Step 18	<p>Deflect inquiries that attempt to seek information outside the scope of the visit/assignment, to include personal information about the host, other personnel, or government programs.</p>
Step 19	<p>Report to Counterintelligence:</p> <ul style="list-style-type: none"> • Close and continuing contact with foreign nationals; • Anomalies; • Solicitation of sensitive information; • Questionable activities or motives; • Persistent requests for information despite deflection attempts. <p>See Standard Practice Instruction (SPI) 5-14, Counterintelligence Program for further information.</p>
Step 20	<p>At the conclusion of a visit/assignment, ensure compliance with close-out procedures to include the return of all identification/facility access badges, keys, and equipment to the appropriate office.</p>
Step 21	<p>Reply to system-generated e-mails at conclusion of the visit/assignment to provide the FVA Office with information required by DOE (occurrences, dates on-site). The system prompts the host to reply that to the best of his/her knowledge there were no unusual occurrences regarding the visit/assignment, or that details regarding all reportable occurrences have been disseminated to the proper authority. The system will automatically provide additional information, such as on-site dates.</p>

References

[Hosting and Escorting Foreign Nationals \(TQ-SEC-FN\), BNL Training and Qualifications](#) Web site

[Reporting Incidents of Security Concern, Laboratory Protection Division](#)

[Standard Practice Instruction \(SPI\) 5-14, Counterintelligence Program](#)

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

PROCEDURE: INDICES CHECK

Management System: Security		
Subject Area: Foreign National Visits and Assignments (Unclassified)		
6. Indices Check		
Effective Date: Sep 13, 2013	Subject Matter Expert: Leonard Butera	Management System Executive: John Carney Jr

Applicability

This information applies to BNL staff that process Indices checks for foreign nationals who are born in, citizens of, or an affiliate of a sensitive or State Sponsor of Terrorism (SST) country.

Required Procedure

Indices Check contains three subsections:

[6.1 Indices Process Requirements](#)

[6.2 Requesting Site Access before Indices Completion - Visits Only \(Access for less than 30 days\)](#)

[6.3 Requesting Site Access before Indices Completion - Assignments](#)

Indices checks are required for foreign nationals who are born in, citizens of, or an affiliate of a sensitive or State Sponsor of Terrorism (SST) country. For a current list of sensitive and SST countries, contact the [Brookhaven Counterintelligence Field Office](#). Additionally, Indices are required for all foreign nationals, regardless of country status, who are conducting work that permits access to sensitive information or technologies, or security areas that store sensitive or classified matter. Under normal conditions Indices checks are completed 30 days after initiation; however, world events may result in extensive delays. Requests requiring Indices completion before access (see the [Foreign Visits and Assignments Requirements Matrix](#)) must be submitted to the GUV Office (automated upload) a minimum of 30 days before the start date of the visit/assignment. Indices are valid for 2 years from date of completion unless derogatory information comes to light during that time. If a visitor has a current Indices that was initiated for a previous visit/assignment, and no derogatory information exists, the Brookhaven Counterintelligence Field Office may apply that Indices to the current request. Requests for Sensitive Country Nationals to Non Sensitive/Non Security areas do not require Indices completion prior to site access and the Counterintelligence Office will monitor the Indices to completion. State Sponsor of Terrorism foreign nationals, regardless of access request, require completed Indices prior to access.

6.1 Indices Process Requirements

Step 1	A new Indices is initiated when a request is entered into the DOE FACTS (Foreign Access Central Tracking System) by GUV Office staff. Note: The investigation portion of the Indices check is conducted by various U.S. Government agencies.
Step 2	The local Counterintelligence (CI) Office monitors the Indices for completion.
Step 3	The DOE Headquarters, Office of Counterintelligence, notifies the Brookhaven Counterintelligence Field Office of Indices completion and any derogatory results.

Step 4	<p>The Senior Counterintelligence Officer</p> <ul style="list-style-type: none"> • Reviews the data gathered during the Indices and determines local counterintelligence approval or rejection for each request; • Recommends approval or denial of a request to the Final Approval Authority.
Step 5	If a request is denied, the CI Officer rejects the request via the GIS so that the requestor is advised. The designated Local Approval Authority notifies the requestor.
Step 6	Requests requiring a Subject Matter Expert (SME) Review will be reviewed and approved by all of the Subject Matter Experts. The GUV then receives the request for the Guest User Visitor Center designated Final Approval Authority, and the process, as described in the subsection General Requirements for Visit/Assignment Requests , Steps 12-17, continues.

6.2 Requesting Site Access before Indices Completion – Visits Only (Access for less than 30 days)

Under certain circumstances, visits (this process is only applicable within the parameters identified below) involving foreign nationals accessing sensitive subjects or areas may be approved before Indices completion. This option is **not** to be used as an alternative to visitors registering on time and may not be used instead of Indices checks for nationals of State Sponsor of Terrorism (SST) countries. Access to sensitive subjects or access to sensitive security areas without Indices completion requires the Senior Counterintelligence Officer, or designee, to make the final determination on these requests. If at any time information arises that indicates the visit activities should not continue, the visit will be immediately terminated, the approval revoked, and the visitor escorted off-site.

To request access before Indices completion for a visit, the following parameters apply:

- For interviews, the requested visit is not to exceed 7 days.
- For activities other than interviews the visit is not to exceed 14 days.

It is always preferable to have the Indices complete before access; therefore, the [Request for Foreign National Access Before Indices Completion Form](#) is **not** to be submitted to the FVA Office more than two weeks before the requested start date.

Step 1	<p>If necessary, contact the Brookhaven Counterintelligence Field Office to confirm the visitor's country status.</p> <p>Note: Facility access is limited to Open Areas and PPAs that have been designated as non-sensitive only. Information Access is limited to Open Research only.</p>
Step 2	<p>Submit the Guest Information System (GIS) request to the FVA Office as a visit with a requested date span not exceeding 7 days for an interview or 14 days for other activities.</p> <p>Note: The GIS registration request must be received by the FVA Office with enough lead time to ensure initial reviews can be completed by all of the Subject Matter Experts (SMEs) before the first day of access.</p>
Step 3	The host submits a Request for Foreign National Access before Indices Completion Form to the FVA Office a minimum of 7 working days before the first day of access.
Step 4	The local Counterintelligence Office will conduct an initial check on the visitor and advise the FVA Office of approval/denial for access before Indices completion.
Step 5	The FVA Office, as appropriate, either submits the request for final approval or notifies the

	sponsoring department that access before Indices completion has been denied.
Step 6	Upon receiving final approval, the FVA Office routes the approved request to the sponsoring department GIS Administrator. If disapproved, the Assistant Laboratory Director for Facilities and Operations notifies the visitor.
Step 7	The Counterintelligence Office monitors the Indices for completion.

6.3 Requesting Site Access before Indices Completion – Assignments (Access for more than 30 days)

Under certain short notice circumstances, foreign national assignees may be granted access to the site before Indices completion via a Counterintelligence (CI) Consultation. CI Consultations are conducted at the discretion of the Senior CI Officer. CI Consultations are only conducted when the visitor has had a prior Indices check completed in the past. Counterintelligence Consultations may not be used as a standard alternative to Indices checks and may not be used instead of Indices checks for nationals of State Sponsor of Terrorism countries.

Step 1	If short notice circumstances do not allow for the Indices to be completed before the start date of an assignment request and it is imperative that the foreign national be permitted to conduct activities immediately, the Host may request a Counterintelligence (CI) Consultation be conducted.
Step 2	To request a CI Consultation be conducted, the host contacts the Brookhaven Counterintelligence Field Office and provides justification for permitting access before Indices completion.
Step 3	During a CI Consultation the Senior Counterintelligence Officer and the Laboratory Deputy Director for Operations (Final Approval Authority) review the data gathered during the prior Indices. They either approve or deny the visitor site access before Indices completion.
Step 4	If the request is denied, the CI Officer will reject the request via the GIS so that the host is notified.
Step 5	If approved, the FVA Office is notified and continues processing the request.
Step 6	Upon receiving final approval, the FVA Office routes the approved request to the sponsoring department GIS Administrator. If disapproved, the Assistant Laboratory Director for Facilities and Operations notifies the visitor.
Step 7	The Counterintelligence Office monitors the Indices for completion.

References

[Guest Information System \(GIS\)](#)

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

| [SBMS Home Page](#) | [Top of Subject Area](#) | [Instructions](#) | [Changes](#) |

Questions/Comments

Disclaimer

PROCEDURE: COMPUTER ACCESS: FOREIGN NATIONALS

Management System: Security		
Subject Area: Foreign National Visits and Assignments (Unclassified)		
7. Computer Access: Foreign Nationals		
Effective Date: Sep 13, 2013	Subject Matter Expert: Leonard Butera	Management System Executive: John Carney Jr

Applicability

This information applies to BNL staff who process requests for computer access for foreign nationals, including access to computer systems beyond the BNL network and BNL internal computer networks from an off-site location.

Required Procedure

Computer Access: Foreign Nationals contains three subsections:

[7.1 General Access](#)

[7.2 Remote Users](#)

[7.3 Computer Access for State Sponsor of Terrorism Nationals](#)

All requests for foreign national access to computer systems beyond the BNL Visitor Network (bnl.org) must undergo the review and approval process specified in the section [Processing a Visit/Assignment Request](#). Access to systems that store sensitive information, or access to any system by a State Sponsor of Terrorism National requires a Cyber Security Plan (SST) before approval.

7.1 General Access

Step 1	The host confirms that the general type (bnl.gov – Internal Network; bnl.org – Visitor Network; or None) of computer access being requested on the Guest Information System (GIS) is appropriate for the foreign national's work responsibilities. Note: Computer access granted must not exceed that which is required to conduct the activities specified in the GIS request.
Step 2	The host and applicable system administrator coordinate on the specific computer access required by the foreign national, and if applicable, develop a specific Cyber Security Plan. Contact the ITD Cyber Security Group for further information and assistance in developing the plan.
Step 3	After the visit/assignment request and if applicable, the Cyber Security Plan receive final approval, the host coordinates obtaining the necessary access accounts for the visitor. Note: All new requests for internal network computer access by State Sponsor of Terrorism (SST) nationals require approval by the Secretary of Energy. Extensions and Legal Permanent Resident SST National requests are approved by the Final Local Approval Authority. See the subsection Computer Access for State Sponsor of Terrorism Nationals for further information.

Step 4	Immediately report any detected or suspicious incidents involving Laboratory computers or networks in accordance with the Cyber Security, Unclassified Subject Area.
Step 5	Once the foreign national no longer needs access to a particular system or systems, the host ensures that the access accounts are terminated. See the Cyber Security, Unclassified Subject Area for further information on obtaining accounts, use of BNL systems, incident reporting, and terminating accounts.

7.2 Remote Users

The designation Remote User applies to individuals who will be accessing BNL internal computer networks (e.g., bnl.gov) from an off-site location, and will not physically be accessing the site at all or only on rare occasions.

All Remote Users must present proper identification and applicable United States Citizenship & Immigration Services (USCIS) documentation anytime they will physically access the site. For additional information see the [Guests and Visitors](#) Subject Area and the [ID Requirements for Guests & Visitors](#).

Step 1	Use the Guest Information System (GIS) to process requests for remote access to internal BNL networks by foreign nationals as specified in the section Processing a Visit/Assignment Request .
Step 2	Select "Remote User" as the Guest Title, and "Remote Computer Access" for the Type of Access Requested. If the remote user may come on-site, then enter the buildings that the remote user will probably access into the GIS.
Step 3	The host and applicable system administrator coordinate on the specific computer access required by the foreign national, and if applicable, develop a specific Cyber Security Plan. Contact the ITD Cyber Security Group for further information and assistance in developing the plan. Note: Computer access granted must not exceed that which is required to conduct the activities specified in the GIS request.
Step 4	After the visit/assignment request, and if applicable, Cyber Security Plan, receive final approval, the host coordinates obtaining the necessary access accounts remote access security for the individual. Note: All new requests for internal network computer access by State Sponsor of Terrorism nationals require approval by the Secretary of Energy. Extensions and Legal Permanent Resident SST National's requests are approved by the Final Local Approval Authority. See the subsection Computer Access for State Sponsor of Terrorism Nationals for further information.
Step 5	Immediately report any detected or suspicious incidents involving Laboratory computers or networks in accordance with the Cyber Security, Unclassified Subject Area.
Step 6	Once the foreign national no longer needs remote computer access, the host ensures the access accounts and paths into the network are terminated. See the Cyber Security, Unclassified Subject Area for further information on obtaining accounts, use of BNL systems, incident reporting, and terminating accounts.

7.3 Computer Access for State Sponsor of Terrorism (SST) Nationals

This subsection only applies to processes related to computer access for State Sponsor of Terrorism nationals. See the subsection [Processing a Visit/Assignment Request](#) for additional requirements on State Sponsor of Terrorism requests.

Step 1	<p>The host confirms that the general type (bnl.gov – Internal Network; bnl.org – Visitor Network; None) of computer access being requested on the BNL 473 Form, “Request for Foreign National Unclassified Visit or Assignment” is appropriate for the foreign national's work responsibilities.</p> <p>Note: Computer access granted must not exceed that which is required to conduct the activities specified in the BNL 473 Form.</p>
Step 2	<p>All requests for computer access to internal BNL networks by a State Sponsor of Terrorism national require a specific Cyber Security Plan for Foreign National Visitor Access to Unclassified Computer Resources. To avoid approval delays, the host contacts the ITD Cyber Security Group for coordination in developing the plan.</p>
Step 3	<p>The Department/Division user administrator provides</p> <ul style="list-style-type: none"> • Visitor/Assignee Identification and Information (found in Part 1 of the plan: User Facilities, buildings, rooms); • Departmental/Divisional staff who will be signing the plan (Part 6).
Step 4	<p>The host provides</p> <ul style="list-style-type: none"> • Identification of the information system(s) to be accessed by the SST Visitor (Part 2); • Detailed justification for the level of access requested and host contact information (Part 1).
Step 5	<p>The Systems Administrator provides Information about the systems not provided by the host (Part 2):</p> <ul style="list-style-type: none"> • Location (building, room); • DNS (Internet) Name; • IP/MAC address; • The security measures to be executed: <ul style="list-style-type: none"> ◦ Which of the above listed systems and components are involved, what action(s) will be taken and how? State device(s) to be used. ◦ Who will be performing each of the actions that will affect the security of the system(s)? ◦ When all this will be done (if the actions must be taken more than once, include specifics). ◦ Where this will be done (i.e., switch, data line jack, control room). ◦ Why each of the actions is necessary and the effect they will have on isolating the named system(s). ◦ Will all the listed systems be effectively isolated by the same actions, or must additional actions be taken to isolate them from the BNL Campus network as well (and details)? ◦ Notify ITD Cyber Security Office each time the above actions are taken by e-mailing the SST Plan distribution group (SSTPlan@bnl.gov, or in the GAL, the “SST Plan” alias).

Step 6	<p>The Cyber Security staff provide</p> <ul style="list-style-type: none"> • Technical guidance and where appropriate, implementation of the security measures in the plan; • Approval of the technical and administrative controls proposed by the host Department.
Step 7	<p>After final approval by the Local Final Approval Authority and/or the Secretary of Energy (see the section Processing a Visit/Assignment Request, for further information on the approval process), the host coordinates obtaining the system accounts for the individual.</p>
Step 8	<p>Immediately report any detected or suspicious incidents involving Laboratory computers or networks in accordance with the Cyber Security, Unclassified Subject Area.</p>
Step 9	<p>Once the foreign national no longer needs remote computer access, the host ensures the access accounts and paths into the network are terminated.</p> <p>See the Cyber Security, Unclassified Subject Area for further information on obtaining accounts, use of BNL systems, incident reporting, and terminating accounts.</p>

References

[Cyber Security, Unclassified](#) Subject Area

[Guest Information System \(GIS\)](#)

[Guests and Visitors](#) Subject Area

[ID Requirements for Guests & Visitors](#), [The Guide to Brookhaven National Laboratory \(BNL\)](#)

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

| [SBMS Home Page](#) | [Top of Subject Area](#) | [Instructions](#) | [Changes](#) |

Questions/Comments

Disclaimer

https://sbms.bnl.gov/sbmsearch/subjarea/185/185_pro7.cfm

DEFINITIONS

Definition: Foreign National Visits and Assignments (Unclassified)

Term	Definition
close and continuing contact	A relationship that (a) involves bonds of affection and/or personal obligation, and/or (b) where the employee and foreign national share private time together in a public or private setting where sensitive professional and personal information is discussed or is the target of discussion. This includes contact (including e-mail) regardless of location (on-site or off-site), but does not include incidental contact. Questions concerning this term and the required reporting obligations should be directed to the appropriate counterintelligence officials.
economic security	Concerns protection of U.S. proprietary economic or trade secret information from theft by any foreign power (see Economic Espionage Act of 1996).
export controlled information (ECI)	Certain unclassified government information under DOE's cognizance, which is controlled under U.S. export laws or export regulations, and which unrestricted dissemination could reasonably be expected to adversely affect U.S. national security and nonproliferation objectives.
foreign national	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. This includes Legal Permanent Residents (a.k.a. Permanent Resident Aliens).
generic security plan	A plan that ensures security interests and sensitive information and technologies are not placed at risk during visits and assignments of foreign nationals.
guest	Any non-employee who visits the Laboratory for whom the Laboratory establishes and maintains a permanent record. A permanent record may be required if the visitor meets one or more of the following conditions: 1) Visits a facility for which training is required; 2) Visits a facility requiring the use of a radiation monitoring device; 3) Visitor or accompanying family member is a foreign national; 4) Visitor is expected to spend more than three days at the Laboratory. A guest is assigned a BNL guest number.
guest administrator	One or more employees, appointed by each Laboratory organization, authorized to capture, input, and update information on guests and terminate their active status. This person may also be the sponsor.
Guest Information System (GIS)	A module of the Human Resources Information System (HRIS), which tracks demographical and historical information on guests.
host	A DOE or DOE contractor employee responsible for the activities associated with the successful accomplishment of a visit or assignment. A sensitive or State Sponsor of Terrorism (SST) country national cannot act as host.
Indices check	A procedure whereby a request is made to appropriate U.S. Government agencies to determine whether information exists on a particular foreign national.

international agreement	An agreement between the United States or an entity thereof, and a foreign country or an entity thereof, or an international organization or an entity thereof, to cooperate in an endeavor of common interest. Included are agreements of specific types, such as umbrella agreements, project agreements, implementing agreements, cooperative agreements, protocols, memoranda of understanding, and contracts providing for cooperative endeavors.
legal permanent resident (LPR)	An individual 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.
open research	Basic or applied research that is intended to be published and/or presented at open meetings, or that has already been released to the public.
Property Protection Area (PPA)	A type of security area having boundaries identified with barriers and access controls for the protection of DOE property.
proprietary information	Information that contains trade secrets or commercial or financial information, which is privileged or confidential, and may only include such information that <ul style="list-style-type: none"> • Has been held in confidence by its owner; • Is of a type which is customarily held in confidence by its owner; • Has not been transmitted by the transmitting party to other entities (including the receiving party) except on the basis that it be held in confidence; and • Is not otherwise available to the receiving party from another source without restriction on its further dissemination.
Public Event	Events or activities that are officially determined to be open to the general public (such as public lectures, community meetings, cultural or entertainment events, or open house events), by the BNL approval authority in coordination with subject matter experts (SMEs), are held in open areas, and involve only information releasable to the general public.
security areas	A specific physically bounded area, individually certified by the cognizant security officer, which has been approved by the Department/Division for generating, receiving, using, processing, storing, reproducing, transmitting, destroying, or handling special nuclear material or classified matter. A security facility temporarily sanitized to protect a security interest during a visit or assignment continues to be a security facility. Security areas at BNL are located in Buildings 50, 197C, and 801.
sensitive country	A country to which particular consideration is given for policy reasons during the DOE internal review and approval process of visits and assignments by foreign nationals. Countries may appear on this list for reasons of national security, nuclear nonproliferation, regional instability, threat to national economic security, or terrorism support. A foreign national is considered to be from a sensitive country if he or she is a citizen of, or employed by, a government or institution of a sensitive country. For a current list of sensitive countries, contact the Brookhaven Counterintelligence Field Office.
sensitive subject	Unclassified subject/topics identified in existing Federal regulations governing export control as well as those identified by DOE as unique to

	its work, which involves information, activities, and/or technologies that are relevant to national security. Disclosure of sensitive subjects has the potential for enhancing weapons of mass destruction capability, leading to weapons of mass destruction proliferation, divulging militarily critical technologies, or revealing other advanced technologies, which may adversely affect U.S. national economic security. Therefore, they require special management oversight, especially before release to foreign nationals. A list of sensitive technologies and information that reside at BNL is maintained by the OPSEC Working Group.
specific security plan	A plan developed and implemented to protect DOE and DOE contractor assets and to prevent the compromise of a DOE security interest or sensitive subject to a foreign visitor or assignee. The specific security plan imposes specific access restrictions and security countermeasures to ensure effective protection of DOE assets. The security plan will be included in the approval process by the authority for the unclassified foreign visit or assignment. The effectiveness of the security plan will serve as a critical decision element regarding approval actions. The security plan must provide sufficient detail to support the approval authority in the decision-making process.
technology	Also referred to as technical data, technical skills or know-how, or as scientific and technical 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; it 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	A citizen of the United States, including naturalized citizens.
visit	Access by a foreign national for 30 calendar days or less.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

Search...

Search SBMS »

Management System: [Security](#)Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

DOE Accompanying Family Member Designations

Effective Date: **Sep 06, 2011**

Designation
Aunt
Brother
Brother-in-law
Cousin
Daughter
Daughter-in-law
Father
Father-in-law
Godchild
Godparent
Grandchild
Grandparent
Mother
Mother-in-law
Nephew
Niece
Sister
Sister-in-law
Son
Son-in-law
Spouse
Uncle

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)
[Disclaimer](#)

[Search SBMS »](#)

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Field Parameters for Foreign National Casual Visits to BNL

Effective Date: Jan 15, 2015

Purpose: "Personal – not work-related" or "Car-pool" as applicable

Subject: General & Miscellaneous

Justification: Visit with (**relationship** [see the exhibit [DOE Accompanying Family Member Designations](#)] & **name of person being visited**) who is a (**status** [Guest, Employee, etc.]) with the (_____**Dept.**)

HDE Code: N/A

Assoc. HDE Code: N/A

DOE POC:

BHSO

Frank Crescenzo

(631) 344-3433

DOE Mission: N/A

DOE Benefits: N/A

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)[Disclaimer](#)

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Flowchart for State Sponsor of Terrorism (SST) Requests

Effective Date: **Sep 06, 2011**

Flowchart for State Sponsor of Terrorism (SST) Requests is provided as a [PDF](#) file.

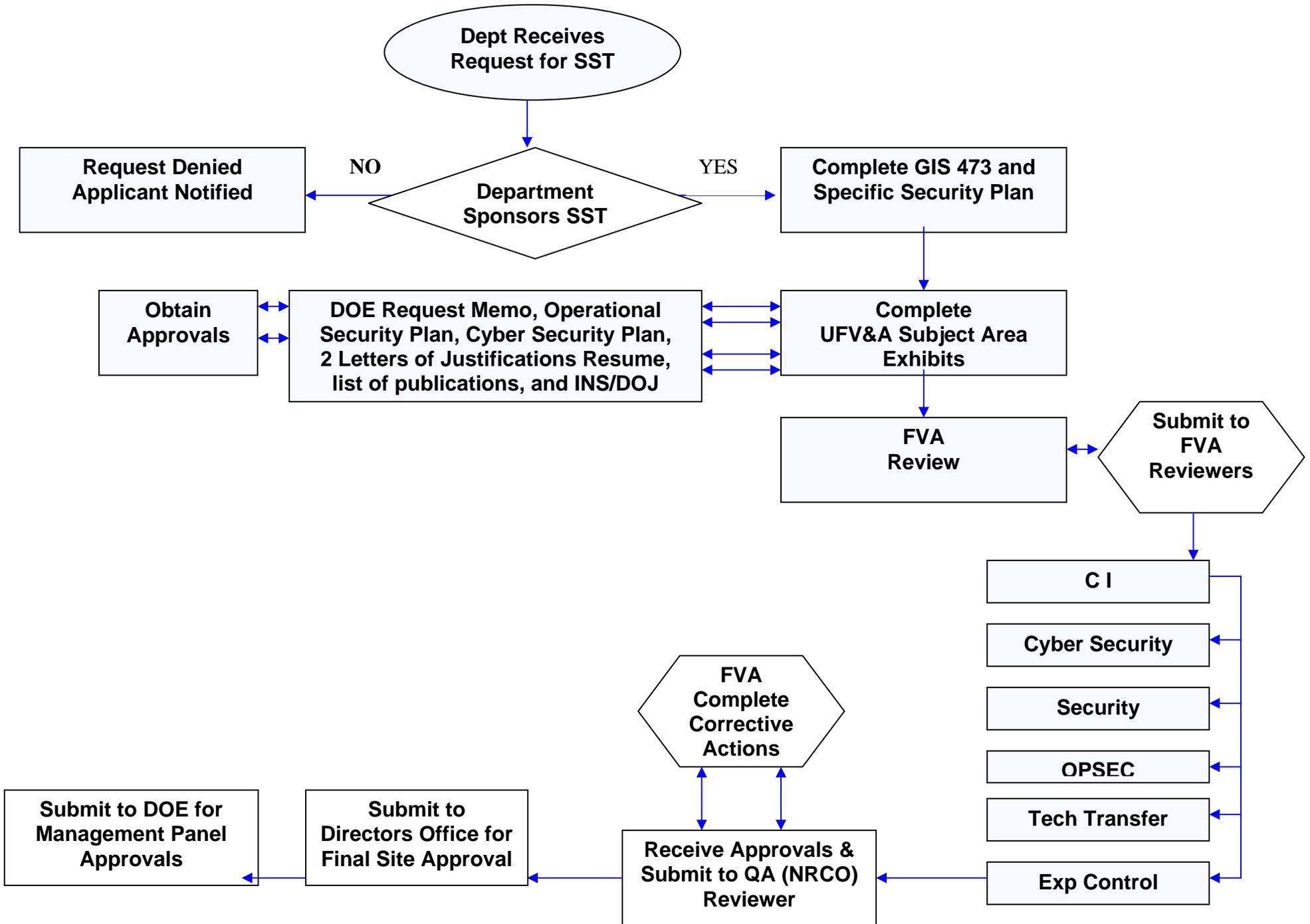
The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

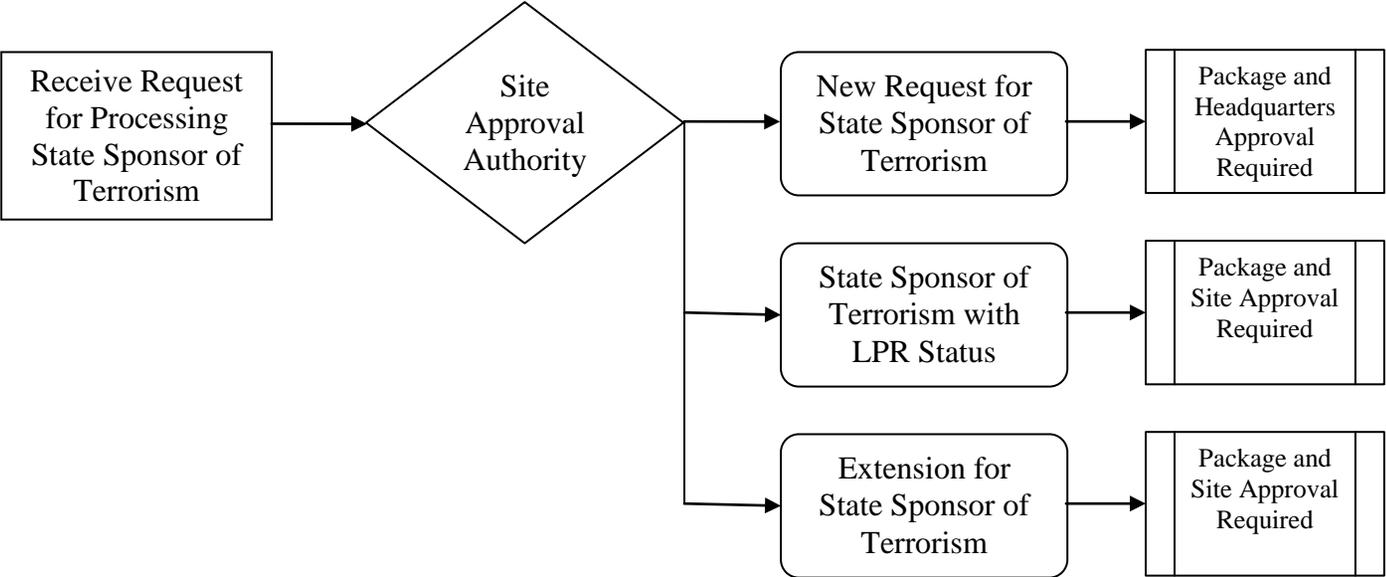
[Questions/Comments](#)

[Disclaimer](#)

Flowchart for State Sponsors of Terrorism (SST) Requests



Flowchart for State Sponsors of Terrorism (SST) Requests



Search...

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Foreign Visits and Assignments Information Brochure

Effective Date: Aug 16, 2016

[Foreign Visits and Assignment Information Brochure](#) is provided as a Word file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)

DOE RELATIONSHIP CODES

Aunt
Brother
Brother-in-law
Cousin
Daughter
Daughter-In-Law
Father
Father-In-Law
Godchild
Godparent
Grandchild
Grandparent
Mother
Mother-In-Law
Nephew
Niece
Sister
Sister-In-Law
Son
Son-In-Law
Spouse
Uncle

5. USEFUL TELEPHONE NUMBERS

Guest Users, Visitor Center X3333
Brookhaven Employee Recreation Association (BERA) X2873
Courtesy Van X2714
Emergency 911 or X2222
Housing X2541
Human Resources X2882
NSLS II User Group X8737
Office of Educational Programs (OEP) X4000
Police Group Help X2238
RHIC & AGS User Center X3333
Foreign Visits Office X7105

BADGES - While on the BNL site, you must wear your ID badge. The badge must be worn between the shoulder and the waist, with the picture showing.



BNL Foreign Visits and Assignments
Research Support Center, Building 400
20 Brookhaven Avenue
Upton, New York 11973
Phone (631) 344-7105

BNL FOREIGN VISITS AND ASSIGNMENTS PROGRAM

REQUIREMENTS FOR GUESTS AND VISITORS

What You Need to Know



GUIDELINES FOR FOREIGN NATIONAL VISITORS AND GUESTS

Welcome to Brookhaven National Laboratory (BNL). By the time you receive this brochure, you should have been issued an identification badge for site access. This brochure contains some additional information that may be useful to you during your stay. If you have additional questions, or need assistance, please call the GUV Center at X3333 or email GUVCenter@bnl.gov. This brochure covers the following topics:

1. What it means when your badge is scanned at the Main Gate.
2. Requirements for reporting updates in your USCIS documentation.
3. How to get permission for another guest or family member to access the site.
4. When and how to get an extension for your visit.
5. Some useful telephone numbers.

1. HAVING YOUR BADGE SCANNED

The bar code on the back of your badge has information about your USCIS documentation, your identity, and your ap-

pointment here. The Officer at the Main Gate will scan your badge when you enter the site. If both vehicle lanes are open, you should use the right lane to speed up the process. The scan information is maintained in a database so that we have a record of the dates and times our guests have been on the BNL site.

**Call Guest Registration at
X3333 or e-mail**

GUV@bnl.gov

2. REPORTING UPDATES IN USCIS DOCUMENTATION AND OTHER REPORTING OBLIGATIONS

You are required to notify the GUV Center if any information affecting your legal status changes: name change, visa change, interactions with law enforcement. If your visa or passport changes during your visit/assignment dates, you must go to the GUV Center with the updated information. If you try to enter the BNL site and your badge scans with a warning, you will be directed to the GUV Center to update your information. If you do not rectify a warning reading, the next scan will alert the officer to collect your badge. **If you do not update your USCIS Documentation, you will not be allowed on-site.**

All foreign nationals accessing the site must have their Passports and Visas

3. INVITING GUESTS AND FAMILY MEMBERS ON-SITE

If accompanying family members were not on the original guest registration, you must contact the GUV Center. Using the Relationship Codes list published by DOE (see back cover), guests are allowed to bring “Accompanying Family Members” on-site, providing the family member is only going to areas that are open to the public. If you want family members to tour your work area or enter other buildings where work is being done, they must complete and be approved on their own Guest Registration. Any guest you wish to invite that is not on the DOE Relationship list must complete a Guest Registration.

Guest Registration and more information is available at

<https://www.bnl.gov/guv/>

4. EXTENDING YOUR STAY AT BROOKHAVEN LAB

If you need to extend your appointment for BNL site access, please contact your host and/or department administrator to discuss. They will provide you with information and directions if there is a need for an extension. You should not return to the BNL site once your badge is expired. Doing so will result in denial of access to BNL.

You should have all updated passport and visa information available and make any other necessary changes to the registration information before the extension is submitted for processing.

[Search SBMS »](#)

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Foreign Visits and Assignments Requirements Matrix

Effective Date: **Sep 13, 2013**

The Foreign Visits and Assignments Requirements Matrix is provided as a [Word](#) file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)[Disclaimer](#)

Foreign Visits & Assignments Requirements Matrix

****NOTE: submittal times reflect average processing times and are subject to change based on world events and available resources.**

Request Parameters	Requirements							
START HERE	Submittal Time to FV&A Office	Request Form	Passport / Visa Validation	Specific Security Plan	Agenda / Event Summary	Indices Check		Additional
						Completion Prior to Start	Access prior to completion permitted	
Open to the Public Event-OTP	15 calendar days	OTP			X	N/A	N/A	Add to Gate Access
Non-Sensitive Country National								
Visit or Assignment	Submittal Time to FV&A Office	Request Form	Passport / Visa Validation	Specific Security Plan	Agenda / Event Summary	Indices Check		Additional
Public Areas	7 working days	GIS	X	N/A	N/A	N/A	N/A	
PPAs/No Sensitive Access	7 working days	GIS	X	N/A	N/A	N/A	N/A	
PPAs/Sensitive Access	30 calendar days	GIS	X	X	N/A	X		Cyber Plan if accessing sensitive systems
Offsite Locations - no sensitive	7 working days	GIS	Information must be provided to BNL - Adhere to remote location requirements regarding verification		N/A	N/A	N/A	
Sensitive Subject	30 calendar days	GIS	X	X	N/A		X	Cyber Plan if accessing sensitive systems

Sensitive Country National

Visit (< 30 days)	Submittal Time to FV&A Office	Request Form	Passport / Visa Validation	Specific Security Plan	Agenda / Event Summary	Indices Check		Additional
Public Area	30 calendar days	GIS	X	X	N/A		X	
PPAs/No Sensitive Access	30 calendar days	GIS	X	X	N/A		X	
PPAs/Sensitive Access	30 calendar days	GIS	X	X	N/A	X		Cyber Plan if accessing sensitive systems
Offsite Locations - no sensitive	30 calendar days	GIS	Information must be provided to BNL - Adhere to remote location requirements regarding verification	X	N/A		X	
Sensitive Subject	30 calendar days	GIS	X	X	N/A	X		Cyber Plan if accessing sensitive systems
Assignment (= > 30 days)								
Public Area	30 calendar days	GIS	X	X	N/A	X		
PPAs/No Sensitive Access	30 calendar days	GIS	X	X	N/A	X		
PPAs/Sensitive Access	30 calendar days	GIS	X	X	N/A	X		Cyber Plan if accessing sensitive systems
Offsite Locations - no sensitive	30 calendar days	GIS	Information must be provided to BNL - Adhere to remote location requirements regarding verification	X	N/A	X		
Sensitive Subject	30 calendar days	GIS	X	X	N/A	X		Cyber Plan if accessing sensitive systems

State Sponsor of Terrorism Country National

Visit or Assignment	Submittal Time to FV&A Office	Request Form	Passport / Visa Validation	Specific Security Plan	Agenda / Event Summary	Indices Check	Additional	Submittal Time to FV&A Office
Local Approval for LPR or Extensions/Headquarters Approval for new assignments								
Public Area	90 calendar days	GIS	X	X		X		SST Package
PPAs/No Sensitive Access	90 calendar days	GIS	X	X		X		SST Package
Offsite Locations - no sensitive	90 calendar days	GIS	X	X		X		SST Package

NOTE: SST Nationals are not permitted access to sensitive PPAs or sensitive subjects

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Host Reference for Protecting Unclassified Controlled Information (UCI)

Effective Date: **Sep 06, 2011**

General

Information that is disseminated, by any means, to a foreign national may be subject to export-control regulations, proprietary agreements, or other Federal regulations governing the dissemination of sensitive information and technologies. Exports may include commodities, software/computer coding, and/or technical data from the United States that is transferred by mail, verbally, email, facsimile, through shipment, via hand-carried materials, over the web and/or by any other means.

In general, only "open research" should be disclosed to a foreign national. Open research or information includes only information/technology that is not protected by statute (classified or sensitive), holds no vested BNL or DOE interest in licensing or patent rights, would be considered releasable to the general public, and is intended for publication or presentation in an open forum. Generally, information in the public domain, or intended to be published or presented in open scientific meetings, would qualify as open research.

While much of the work in which BNL and its employees engage in qualifies as open research, there are facilities and programs that involve unclassified controlled information (UCI). For economic, privacy and national security reasons, it is imperative that UCI be protected from inadvertent disclosure. All access to sensitive information by a foreign national must be reflected in the BNL form 473 "Request for Foreign National Unclassified Visit or Assignment" and formally approved before dissemination.

All personnel with access to such information must be especially knowledgeable of sensitive topical areas, because sensitive information can be inadvertently transferred to foreign nationals through a variety of means, including oral communications, written documentation, U.S. computer software, and visual inspection of U.S. facilities and equipment. Additionally, individuals granted access to Other Agency (OA) or Foreign Government Information (FGI) must adhere to the protection and dissemination requirements of the originating Agency or Government. All forms of Unclassified Controlled Information have dissemination restrictions and are never disseminated to individuals who do not have a "need-to-know" the information in furtherance of their official duties.

The major categories of controlled information at the Laboratory are listed below; however, hosts of foreign nationals should take the following steps before the start of a foreign national visit or assignment that requires access to a BNL facility or technology that is not generally accessible to the public:

1. Review the technologies to be discussed with the foreign national for compliance with information control requirements and verify with the Export Control Office that the technologies do not appear on the DOE or BNL Sensitive Subjects list. Remember, technical data may consist of specific information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of the technologies in question, and may take the form of blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals, and instructions written or recorded on other media or on such devices as disk, tape, and read-only memories.
2. Review any existing agreements or contracts related to the exchange of information or technologies during the project. Only approved technical data, software, and/or commodities can be disclosed, and only to the specific foreign nationals who have been approved for access.
3. If your job responsibilities include access to UCI, review documents and material to be accessed by the foreign national for markings that would indicate the information is sensitive i.e., ECI, UCNI or OUO.
4. Confirm with your GIS Administrator or the Foreign Visits and Assignments Office that access to sensitive information has been documented and approved by all the Subject Matter Experts and the local Approval Authority as indicated in the BNL form 473.

Common Categories of Unclassified Controlled Information at BNL

Export Controlled Information (ECI)

Export Control is required to prevent regulated technology, information and software from being illegally released within or outside the United States to a foreign national who has not been granted U.S. citizenship or does not have legal permanent residence in the United States. A deemed export can occur through transfer of technology to a foreign national when such a transfer would convey an understanding of: the design, construction or functioning of the export-controlled equipment or process, or to advance significantly the development of similar equipment or processes. Contact the Export Control Office for assistance in identifying Export Controlled technologies.

Official Use Only (OUO)

Official Use Only is the DOE term for identifying information that may be exempt from public release under the Freedom Of Information Act (FOIA), such as Personal/Privacy information. Identification and protection requirements are available in the SBMS [Operations Security \(OPSEC\)](#) Subject Area.

Unclassified Controlled Nuclear Information (UCNI)

UCNI is certain unclassified but sensitive government information concerning Nuclear Material, weapons & components whose dissemination is controlled under section 148 of the Atomic Energy Act. Generally, Foreign Nationals are not granted access to UCNI at BNL without special DOE approval.

Confidential Foreign Government Information-Modified Handling (C/FGI-MOD)

Note: Although C/FGI-MOD is actually classified information, the protection requirements applied are in accordance with protection requirements for U.S. Unclassified Controlled Information.

C/FGI-MOD is classified information provided to the United States by a foreign government. The United States and originating entity agree that the protection requirements are less than those afforded to U.S. classified information; therefore, the information is approved for modified handling. Although not classified by U.S. standards, protection guidelines provided by the originating country must be adhered to.

Other Agency (OA) Information

Quite often documents containing Unclassified Controlled Information are received from other agencies. Some of the most common are

- "For Official Use Only" (FOUO), a designation used by the Department of Defense (DOD) and Department of Homeland Security (DHS);
- "Sensitive But Unclassified" (SBU), a designation used by the Department of State (DOS);
- Law Enforcement Sensitive (LES), a designation used by the FBI, and some local law enforcement agencies;
- "Limited Official Use" (LOU), a designation used by the Department of Justice (DOJ);
- Safeguards - information controlled by the Nuclear Regulatory Commission (NRC) primarily concerning the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material;
- Critical Infrastructure Information (CII) is used by various agencies when referring to information regarding the nation's critical infrastructure.

When granted access to OA information, adhere to the protection and dissemination guidance provided by the originating agency.

Contact the Information Security Office or Export Control Office for further information on the protection and control of Unclassified Controlled Information.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)

Search...

Search SBMS »

Management System: [Security](#)Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)**Property Protection Areas (PPAs)/Controlled Access Areas (CAAs)**Effective Date: **Aug 25, 2016**

A **Property Protection Area (PPA)** is a type of security area having defined boundaries and access controls for the protection of Departmental/Divisional property. It is a designation used for facilities where a special standard of protection must be applied. For example, such a facility may have property of significant monetary value; nuclear materials requiring safeguards controls or special accounting procedures; property of significance to Departmental program continuity or national security considerations; or property that, if mishandled, could have adverse impacts upon the public health and safety.

PPAs are established to protect Government-owned property/information against damage, destruction, or theft. Only appropriately cleared and authorized personnel are permitted unescorted access. Visitors will be escorted at all times while in the PPA. Personnel, vehicles, hand-carried items, and packages entering or exiting the PPA are subject to inspection to deter and/or detect unauthorized introduction of prohibited articles and removal of Government assets.

Controlled Access Areas (CAAs) are management-defined security areas that include an entry point requiring controlled access. These areas require a level of security protection below that of a PPA.

Open Areas - for the purpose of processing foreign visits and assignments, once access to the site has been granted, all areas of the site are considered open areas except for those otherwise specified in this section.

The following is a list of PPAs and CAAs at BNL:

Property Protection Areas (PPAs)/Controlled Access Areas (CAAs)			
Number	Building/Facility	Security Area	Designation
1	50 - Police Headquarters	PPA	S
2	B-98 Warehouse	CAA	NS
3	129 - Computers	CAA	NS
4	244- Locksmith Shop	PPA	S
5	348- Radiation Calibration Facility	PPA	NS
6	356- Solid State Gamma Irradiation Facility	PPA	NS
7	400- Personnel Security Badging and FV&A Office	PPA	S
8	449- Telephone & Data Equipment Nodes 1&2	PPA	NS
9	459- ITD Computing Data Center	CAA	S
10	463- Biology - Rooms B101, B012 and B014	PPA	NS
11	490- Rooms 5-11A	PPA	NS
12	490- Medical Research Center Gamma Irradiation Facility - Room 9B-134B	PPA	NS
13	510 - Clean Room	CAA	NS
14	515- ITD Brookhaven Computing Facility	PPA	NS
15	515- ITD Cyber Security Laboratory M1-58	PPA	S
16	515 - Net Work Lab	PPA	NS
17	703 - Labs E-2 and E-4	CAA	NS
18	734 - Multiple Laboratories	CAA	NS
19	735 - Room 1G05	PPA	NS
20	735-CFN	CAA	NS
21	740-NSLS II	CAA	NS
22	750 RAP Team - 750 Receiving/Storage Room in 750 Annex	PPA	S
23	750 Annex - Radiological Protection Program	PPA	S

24	801- Room 19	PPA	S
25	801- Isotope Research & Processing Laboratory -Rooms 2-46, 2-66, 2-66C and 2-51	PPA	NS
26	801 - Room 46	PPA	NS
27	830 - Lab 6, Lab 8, Lab 8a and East hot cell	PPA	NS
28	830 - GST Rig	CAA	NS
29	T834 - Meteorology Tower & Communication Trailer	PPA	NS
30	835 - Electrical Operations	CAA	NS
31	860/865 - Waste Management Operations & Reclamation	PPA	NS
32	911- Collider Accelerator Department Operations Control - Rooms 219-223	CAA	NS
33	924 Wire Yard	CAA	NS
34	926 CAD Warehouse	CAA	NS
35	931- BLIP	PPA	NS
36	939 - LP Emergency Operations Center	CAA	S
37	958 - NASA Space Radiation Laboratory	CAA	NS
38	1005A - Collider Accelerator Department RHIC Cryogenic Control Room	CAA (during Ops)	NS

NS - Denotes facilities without sensitive information

S - Denotes facilities with sensitive information

Limited Areas – Unclassified foreign visits are not permitted to occur in Limited Areas.

Foreign National Access to Property Protection Areas (PPA) and Controlled Access Areas (CAA)

For the purpose of foreign national access to PPAs and CAAs, the areas are designated as "sensitive" or "non-sensitive" based on what is stored or processed within the facility. Access by a foreign national to a PAA/CAA designated as sensitive will extend the approval processing time. Contact the Information Security Office at x5524 or Deputy Manager, Laboratory Protection Division at x4691 to determine the designation of the facility to be visited. When processing Foreign Visit & Assignment requests for access to the aforementioned areas, please use Property Protection Area/Controlled Access Area for the "Facility Type" field. Refer to the exhibit [FV&A Requirements Matrix](#) for approval time frames for foreign nationals' access to these areas. **Note:** Certain PPAs/CAAs designated as sensitive do not permit any access by foreign nationals.

Escort Procedures for Property Protection Areas (PPA) and Controlled Access Areas (CAA)

Escort Criteria

- The escort must be an individual who has a full understanding of the Facility Security Plan and activities that regularly occur in the security area.
- Personnel escorting foreign nationals must be DOE or DOE contractor employees.
- Sensitive or State Sponsor of Terrorism (SST) country nationals may not serve as escorts.
- Escorts must have knowledge of specific information and technologies to which visitor access has been authorized to ensure that no unauthorized access occurs.
- One cleared escort may escort no more than four visitors.

Escort Responsibilities

- Verify the identity of the visitor(s), using a form of photo identification.
- Ensure that site and facility Security Plan requirements regarding prohibited and controlled items (i.e., explosives, controlled substances, receiving, transmitting and recording devices) are enforced.
- Ensure the visitor(s) signs in and out on the visitor register each time they enter and leave the area.
- Ensure the visitor(s) displays the visitor badge at all times. The badge must be worn on the upper front portion of the body, on the outer garment.
- Keep the visitor(s) under observation at all times.
- Preclude any exposure or access to sensitive information or technologies that have not been formally approved.
- Ensure the visitor(s) returns the visitor badge at the end of the visit.
- Report any unusual or suspicious occurrences in accordance with local procedures.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)

Search...

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Unclassified Foreign Visits and Assignment Program Reviewer/Approval Authority Guide

Effective Date: Aug 16, 2016

The [Unclassified Foreign Visits and Assignment Program Reviewer/Approval Authority Guide](#) is provided as a Word file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)



**UNCLASSIFIED FOREIGN
VISITS AND
ASSIGNMENTS PROGRAM**

REVIEWER/APPROVAL

AUTHORITY GUIDE

1. PURPOSE:

This guide will serve to aid local subject matter expert (SME) reviewers and local approval officials, as charged by DOE Order 142.3A for processing visit/assignment requests by foreign nationals under the Unclassified Foreign Visits and Assignments Program. The guide is intended to assist with standardized implementation and to provide knowledge of the individual review responsibilities and overall approval process. It will also provide program continuity when alternate reviewers and approving officials are performing the duties and responsibilities. The guide identifies how requests are handled for visits/assignments by foreign nationals from state sponsors of terrorism and for processing requests for open-to-the-public events. Although a condensed list of host responsibilities is included, it is only to demonstrate the relationship between the host and the reviewers. It does not provide a substitute for the detailed host responsibilities identified in the Foreign National Visits and Assignments (Unclassified) Subject Area. This guide is distributed to each of the SMEs, approval authority, and alternates. It is not intended for distribution to hosts.

2. REFERENCES:

- A. DOE Order 142.3A, Unclassified Foreign Visits and Assignments Program, dated October 14, 2010.
- B. Foreign National Visits and Assignments (Unclassified) Subject Area.

3. SUBJECT MATTER EXPERT REVIEWS:

- A. SME reviewers will consider factors associated with the requested access to BNL/DOE facilities, programs, information, and technologies, including area building type requesting 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.
- B. 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.

C. 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.

D. SME reviews will be documented and uploaded to FACTS by the Guest, User, Visitor Center (GUV Center). Documentation will include all elements required of the "Package", the date the reviews were completed, and the name of the reviewer. All required documentation will also be uploaded to FACTS prior to the final Local Approval or DOE access approval.

E. Subject Matter Expert Reviews are required when: the Host has a clearance, a Security Area or Sensitive Subject/Information is accessed; or Proprietary work is to be performed; and, for visits/assignments involving State Sponsor of Terrorism Nationals.

4. RESPONSIBILITIES:

A. HOSTS:

(1) Hosts and escorts should be a DOE or DOE contractor employee. Non-employees from non-sensitive countries, such as those holding Joint Appointments and researchers at User Facilities may also act as hosts. All Non-Employee Hosts fall under the same requirements and limitations as BNL employees. Foreign nationals (FNs) who are affiliated with a sensitive or State Sponsor of Terrorism (SST) country may not act as hosts or escorts. Co-hosts may be assigned to meet requirements during periods when the primary host may be unavailable due to official travel, authorized leave, etc., however, the GUV Center must be notified of all assigned co-hosts before the co-hosts take on hosting responsibilities. All co-hosts must adhere to the same requirements (e.g., training) as primary hosts.

- (2) Ensure the completion of the request for foreign national unclassified visit or assignment form (BNL-473) located on the Guest Registration System (GIS). Ensure the request is routed according to departmental and GUV review and approval procedures. If the foreign national is a citizen of a Department of State (DOS) defined terrorist country, the submittal to FV&A for completion of a package must be at least 90 days in advance, contact K. Walker at ext. 7105 for appropriate paperwork and coordination. The DOS has currently defined the following three (3) countries as sponsors of terrorism: Iran, Sudan, and Syria.
- (3) If the visit or assignment involves access to a security area, a sensitive subject, and/or access by a sensitive or non-sensitive country foreign national to a Property Protection Area (PPA), or Controlled Access Areas (CAA) with sensitive information, develop and submit a specific security plan.
- (4) Follow up with the GUV Center at ext. 3333 or the BNL FV&A Administrator (Kathy Walker ext. 7105) to ensure approval has been granted prior to notifying the visitor or assignee they may come to BNL.
- (5) Comply with the generic security plan (Foreign National Visits and Assignments Subject Area) and, if applicable, the approved specific security plan.
- (6) Participate in host briefings and debriefings conducted by Counterintelligence officers.

Note: Most administrative requirements are completed by the GUV; however it is the ultimate responsibility of the host to ensure approvals are with in compliance with DOE requirements.

B. GENERAL SME REVIEW ITEMS:

The BNL request for a foreign visitor assignment includes biographical information on the foreign national, department specific information, subject information, and host information. The Department submits the request for the Host review, the record is then sent to the GUV Center, and if required, for Office of Scientific Personnel (OSP) review prior to the FVA review. The review of a

request by each of the SMEs will include a check of the following generic items for each visit or assignment request and all requests for an open-to-the-public event:

- (1) Name (First, Last, Middle)
- (2) Country of Birth (sensitive or non-sensitive)
- (3) Country of Citizenship (sensitive or non-sensitive)
- (4) Country of Second Citizenship, if applicable (sensitive or non-sensitive)
- (5) Passport Country of Issue
- (6) Guest Title
- (7) Employment Information (Affiliation Entity)
- (8) Host Name (First, Last)
- (9) Host's Organization
- (10) Host Clearance (yes/no)
- (11) Type of Research or Work the Visitor/Assignee will be doing?
 - a. Open
 - b. Co-operative Research and Development Agreement (CRADA)
 - c. Strategic Partnership Projects (SPP) (formerly known as Work for Others [WFO])
 - d. Guest Intellectual Property Agreement (GIPA)
 - e. Proprietary
 - f. Sensitive and/or Classified (which requires additional approvals)
 - g. Not Applicable.
- (12) Justification of visit or assignment.

C. COUNTERINTELLIGENCE:

(1) The Senior Counterintelligence Officer (SCIO) or his designee coordinates with the DOE Office of Counterintelligence for required indices checks on all visitors and assignees to security areas and/or accessing sensitive subjects, Proprietary agreements, CRADAS, or SPP, requests whose Hosts have

Clearances and State Department Designees of State Sponsor of Terrorist Nationals.

(2) For a priority short notice visit/assignment under (1) above, when the required indices check will not be completed prior to the requested start date, the Counterintelligence Office will monitor the indices to completion and may allow the visitor (escorted/unescorted) site access dependent on the indices and access requested, after the request has been entered in CARDS and coordinated with the GUV Center.

(3) The SCIO or his designee will review indices when received and advise the approval authority if there is any derogatory information and any necessary actions to be taken.

(4) For all requests for "Open/Open Data" research or "Not Applicable" designations, the review and approval by the SCIO or his designee on the request indicates the completion of the indices check and serves as the notification to the FV&A Administrator.

(5) The SCIO or his designee will process and provide derogatory indices check information to the Final Approval Authority for his determination on the appropriateness of the visit or assignment.

(6) The Counterintelligence Office will coordinate derogatory indices results with other Federal agencies as necessary and

(7) Complete the Counterintelligence review and route accordingly.

(8) SST Nationals require a completed indices check prior to site access.

D. FOREIGN VISITS AND ASSIGNMENTS ADMINISTRATOR:

(1) Will review the request for FV&A to ensure completeness, accuracy, and compliance with the program requirements.

(2) Monitor entry into the Foreign Access Central Tracking System (FACTS).

(3) Ensure the GUV routes the request, and specific security plan if required, for SME reviews with the offices of Export Control, Technology Transfer, Security, Cyber Security, OPSEC, and Counterintelligence with a return due date of 10

days from initial routing for Non-Sensitive country nationals and Sensitive Country Nationals not requiring a completed indices prior to site access.

(4) Submit a completed package coordinated with the requesting Department for initial terrorist country foreign nationals request for access to the Subject Matter Experts and the Local Final Approval Authority prior to the DOE Site Office and DOE Headquarters for review and approval. Packages submitted by Legal Permanent Residents and Extensions of guest registrations may be approved for site access by the Local Final Approval Authority. If comments are received from DOE Headquarters, make the necessary modifications to the request then return to DOE Headquarters for approval coordination with the DOE Office of Science. If approval is granted, notify the requesting department/division and the host.

(5) Conduct the SME security review for any physical security concerns.

(6) Ensure approvals are completed and entered into FACTS.

(7) Review records in FACTS weekly for close-out information within the ten day time frame and manually close employee records.

E. CYBER SECURITY OFFICE:

(1) Review the FVA request for the following:

- a. Request for Computer Access and to what systems.
- b. For requests of terrorist country FNs, ensure that the specific Cyber Security plan is completed and approved as required.

(2) Complete the cyber security review and route accordingly.

F. EXPORT CONTROL:

(1) In accordance with the references, et al, determine the need for an export control license (deemed export) based on the citizenship/visa status and employment of the visitor or assignee, the subject codes, and the subjects to be discussed or research to be conducted.

- (2) Contact the host if there are any export control issues that need to be clarified.
- (3) Complete the Export Control review and route accordingly.

G. OPSEC:

- (1) Review the FVA request for the following:
 - a. Check the subject area for the visit and compare it against the BNL Sensitive Subjects List to ensure that there is no unauthorized access to information.
 - b. Ensure that there is no access to critical or sensitive systems by unauthorized foreign nationals. Contact the host for requests to systems that are not authorized and coordinate with the Cyber Security Office to ensure that access is not granted.
 - c. For requests of terrorist country FNs, conduct an OPSEC review of the request and accompanying specific security plans.
- (2) Complete the OPSEC review and route accordingly.

H. TECHNOLOGY TRANSFER:

- (1) Determine regulatory compliance with transfer of technologies to the visitor or assignee based on the references, et al, and the citizenship/visa status and employment of the individual, the subject codes, and subjects to be discussed or research to be conducted. Ensure compliance with any contractual obligations for CRADAs, SPP, and other programs.
- (2) If a request is for CRADA work, ensure that the foreign national is authorized to work on the CRADA and is officially added to the list of participants.
- (3) Contact the host to clarify and resolve any technology transfer concerns.
- (4) Complete the Technology Transfer review and route accordingly.

I. SECURITY:

- (1) Review dates for program compliance and ensure documentation is accurate.
- (2) Determine compliance with the requirement for a specific security plan based on citizenship, access to security areas, access to PPAs, subjects to be accessed, and CAAs with sensitive information/subjects.
- (3) Review specific security plans for viability.
- (4) Ensure submittal of packages for requests of citizens identified by the DOS as Terrorist Country Nationals are routed through BNL management, and DOE channels for the proper site and/or Headquarters approvals.
- (5) Review the citizenship of the host to ensure they are not from a sensitive country and they are an employee or an approved host with valid Host training.
- (6) Complete the Security review and route accordingly.

J. APPROVAL AUTHORITY:

- (1) The Laboratory Director has delegated appointed members of the GUV Center with Final Approval Authority for all unclassified foreign visits and assignments. A. Melocoton will act in this capacity and K. Guiffreda as back up in her absence.
- (2) Upon receipt of the completed request, ensure all SME reviews have been completed and that any comments on the visit or assignment have been considered.
- (3) The Laboratory Director has designated review and approval requests and the specific security plans for terrorist country foreign nationals under the Local Final Approval Authority to the Associate Laboratory Director of Facilities and Operations, who will sign the Final Approval or transmittal letter to DOE requesting review and approval, dependent on the circumstances of the SST National approval requirements under DOE Order 142.3A.

(4) Bring to the attention of the Laboratory Director, any concerns with requests and discuss any questions on programmatic need or advisability of the visit or assignment with the applicable SME, Department Chair/Division Manager, and Laboratory Director.

(5) The Local Final Approval Authority will complete the final site approval or denial.

(6) Route requests for new T3 applicants to the DOE Area Office prior to the request to the Headquarters DOE Office of Science and return the request back to the FVA Office for processing and/or notifications.

5. **PUBLIC EVENT REQUESTS:** Qualifying Events as Open-to-the-Public

A. Requirements:

BNL events or activities are determined to be open to the general public and therefore exempt from the DOE Order 142.3A, "Unclassified Foreign Visits and Assignments Program" after meeting the listed criteria below:

(1) Events are defined as public lectures, community meetings, cultural or entertainment events, or open house events (e.g., Summer Sunday Tours, Community Advisory Committee meetings, BERA events).

(2) Events are held in locations that are determined by the local SMEs and approval authority to be open to the general public.

(3) And are reviewed by the hosting sites Local Final Approval Authority and/or their designee, in coordination with subject matter experts (SMEs), as follows:

- a. Security
- b. Cyber Security
- c. OPSEC
- d. Export Control
- e. Technology Transfer
- f. Counterintelligence

B. Obtaining an Exemption:

(1) An event must be submitted for review and approval prior to being declared a "Public Event".

(2) Submissions must be made 30 days in advance to allow for processing of the event. Timeliness of submission is important as a denial will require compliance with procedures for processing foreign nationals as directed in DOE Order 142.3A.

(3) Hosts must complete a Public Event Request (PER) Form, which is accessed from the main BNL intranet web page under the BNL Site Access Public Event Request tab in the left hand navigation area, or from the Foreign National Visits and Assignments (Unclassified) Subject Area.

(4) Event or activity submissions must include an agenda and a detailed description of scientific/technical areas being discussed. This information is necessary for the reviewers to make an informed decision. If there is not enough information submitted with the request, approvals will be delayed until the necessary information is obtained.

(5) The Local Final Approval Authority or their designee must:

- a. Consult with SMEs in security (including cyber, technical and OPSEC), export control, technology transfer, and counterintelligence.
- b. Provide written determination that the subject matter is releasable to the public and the event has been approved as open to the public.

C. Special Situations:

(1) Recurring Events - Because of the repetitive nature of certain events, a one year approval may be issued for submissions of events listed below:

- a. Sunday Summer Tours
- b. Tours from the Stakeholder Relations Office
- c. Community Relations events
- d. Weekly or monthly events that are held in designated public areas on a consistent basis, with subjects such as, BERA bus trips, Weekly BERA social or cultural workshops, well-defined seminar series, etc.

- e. Off-site Locations - meetings and other off-site activities must be approved as open to the public, or processing through the FVA program is a requirement.
- f. Unclassified events and activities that occur outside the United States or its territories do not have to be processed under the FVA program, but may require documentation in the Foreign Travel Management System, or may require reporting to Counterintelligence.

D. Implementation:

- (1) Once an SME has completed his/her review, they will indicate approval or denial as appropriate.
- (2) Once reviewed and either approved or denied, electronic notifications will be returned to the sponsoring organization of the event.
- (3) A copy will be sent to the FVA Administrator, who, if approved, will place the event on the Public Calendar in the Laboratory Protection Division Outlook folder for access by the Main Gate and Visitor Center.
- (4) The sponsoring organization must then make an entry in the Main Gate Access Event Notification form. This will enable the personnel at the Main Gate to print the badges required for all attendees.

6. CONTINUITY OF PROCESS:

- A. Each person with responsibilities listed in paragraph 5. Public Event Requests, A. (3) above will ensure another individual is capable of carrying on these duties in his/her absence.
- B. Each SME and alternate shall ensure that they are familiar with the content of this guide.
- C. Primary SMEs are responsible to notify the FVA Administrator when they will be away from the Lab so that the alternate's ability to conduct reviews can be activated in the GIS. They are also responsible to notify their alternates that they will be away from the Lab so that they can conduct the reviews.

Search...

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Accompanying Family Member Form

Effective Date: **Sep 06, 2011**

The Accompanying Family Member Form is provided as a [Word](#) file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)

ACCOMPANYING FAMILY MEMBER FORM

Please complete Sections I and II and FAX form for GUESTS to GUV CENTER: **Ext. 8686**

For Employees FAX form to HR Records: **Ext. 3195**

For OEP FAX form to HR Records: **Ext. 5832**

SECTION I - SPONSORING EMPLOYEE / GUEST INFORMATION

To be completed by Department GIS Administrator

GIS Administrator Name:
Phone Number:

BNL Guest/Employee Name:
Guest Registration Number:
FACTS Visitor Number:

SECTION II - ACCOMPANYING FAMILY MEMBER INFORMATION

To be completed by BNL Guest/Employee Sponsoring Accompanying Family Member

Family Member's Name
First:
Middle:
Last:

Gender: Female Male
Relationship to Visitor:
Date of Arrival at BNL: ,

Citizen of:

Birth Date: ,

Country of Birth:

City of Birth:

Visa Information

Type:

Exp. Date: ,
Visa Number:

Passport Information

Country of Issue:

Exp. Date: ,
Passport Number:

SECTION III - PROCESSING INFORMATION

To be completed by GUV Staff

Received: _____
Date

Entered in FACTS: _____
Date

Entered by: _____

Notification to Department to Enter in PeopleSoft

Department: _____

Name: _____

Date Notified: _____

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Cyber Security Plan for Foreign National Visitor Access to Unclassified Computer Resources

Effective Date: **Sep 06, 2011**

Cyber Security Plan for Foreign National Visitor Access to Unclassified Computer Resources is provided as a [Word](#) file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)



Cyber Security Plan: for Foreign National Visitor Access to Unclassified Computer Resources

(For Foreign Nationals who are citizens of, born in, or have an affiliation with
a country identified as a State Sponsor of Terrorism)

Date of Request:

1. Visitor/Assignee Identification & Information:*

Name:

Start Date:

End Date:

(no longer than 2 yrs from Start Date)

Employment Status on Start Date:

Life No.:

Guest No.:

Temporary Guest Registration No.:

BNL User Facility(s) to be accessed:

AGS

ATF

NSLS

NSRL

RHIC

Tandem

None

ATLAS

Department building(s) and room number(s) to
be accessed*:

Justification of visit/assignment; include specific activities, involvement, subjects to be discussed or
statement of research:

Host Name*:

Telephone:

Host Organization:

Directorate:

2. Computer System(s) Identification:

NOTE: All information here must match network registration information in the Network Jack
Registration database. See http://intranet.bnl.gov/itd/reg/reg_form.asp. Approval of the
system administrator responsible for each computer system accessed by the Visitor/Assignee
is required (see signature area).

Primary Computer System(s) to be accessed:

Location Building/Room	DNS (Internet) Name	IP/MAC Address	System Admin.

Security Implementation:

Include details:

- a. Which of the above listed systems and components are involved, what action(s) will be taken to restrict access and how?
- b. Who will be performing each of the actions that will affect the security of the system(s)?
- c. When all this will be done (if the actions must be taken more than once, include specifics).
- d. Where this will be done.
- e. Why each of the actions is necessary and the effect they will have on isolating the named system(s).
- f. Will all the listed systems be effectively isolated by the same actions, or must additional actions be taken to isolate them from the BNL Campus network as well (and details)?
- g. Notify ITD Cyber Security Office each time the above actions are taken by sending e-mail to the SST Plan distribution group (SSTPlan@bnl.gov, or in the GAL, the "SST Plan" alias).

3. Network Identification:

If any computer system to be accessed by the Visitor/Assignee is connected to a network(s), identify all network(s):

- BNL.Gov (Public, Campus, Restricted, Critical System Zone)
- BNL.Org (Open Zone, Visitor Network)
- Other Network(s):

4. Information Access:

A. During the visit/employment, will any system accessed by this Visitor/Assignee contain sensitive unclassified information or Official Use Only? Yes No

B. Sensitive Information

- Unclassified Controlled Nuclear Information (UCNI)
- Naval Nuclear Propulsion Information (NNPI)
- Confidential Foreign Government Modified Handling
- Export Controlled Information
- None

C. Official Use Only (OUO): Information identified as OUO, information must be unclassified; fall under at least one of eight Freedom of Information Act (FOIA) exemptions (exemptions 2 through 9); and be reasonably expected to cause damage to governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their official duties or other DOE-authorized activities.

- | | | |
|--------------------------------------|--|---|
| <input type="checkbox"/> CRADA | <input type="checkbox"/> Export Controlled | <input type="checkbox"/> Technical/Scientific |
| <input type="checkbox"/> Privacy Act | <input type="checkbox"/> Proprietary | <input type="checkbox"/> None |

If yes, identify machine(s). Explain and describe the mechanisms used to protect the information:

DNS (Internet) Name:
IP Address:
MAC Address:

- D. Will the Visitor/Assignee be granted privileged access to any hardware or software such that this person could impact the security features of any system (e.g., root accounts, or administrator privileges)? Yes No

If yes, explain why this is necessary and describe the protections that mitigate the risk of unauthorized disclosure of information:

- E. Will the Visitor/Assignee be accessing the computer system(s) from on-site at other than normal BNL business hours? Yes No

5. Remote Access to BNL:

Will the Visitor/Assignee be accessing the computer system(s) from off-site? Yes No

6. Approvals:

BNL Host (Sponsor): _____ Date: _____

System Administrator(s): _____ Date: _____

Department Chair: _____ Date: _____

Cyber Security Office: _____ Date: _____
Keith Lally

Cyber Security Office: _____ Date: _____
James Fung

Counterintelligence Officer _____ Date: _____
Randy Biegelman

OPSEC/Export Control: _____ Date: _____
Mark Sakitt

cc: Host
System Administrator
Department Chair
Counterintelligence
M. Sakitt

Search...

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

DOE Request Memo

Effective Date: **Aug 16, 2016**

[DOE Request Memo](#) is provided as a Word file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)

DOE Request Memo
Requests for Visits/Assignments
By Foreign Nationals from State Sponsors of Terrorism
(SST Template Processing Checklist)

The following information is provided to assist in preparing packages for visits and assignments to DOE facilities by foreign nationals from state sponsors of terrorism. This information is IAW DOE Order 142.3A, *Unclassified Foreign Visits and Assignments Program*, dated October 14, 2010.

A visit and/or assignment request for a foreign national from a state sponsor of terrorism must be fully documented and entered into Foreign Access Central Tracking System (FACTS) by the hosting site. The requests must have the concurrence of Subject Matter Experts, as well as completed indices checks, prior to being approved by the Approval Authority for the hosting site.

The DOE facility requesting an initial visit/assignment for a foreign national will assemble the package. Then they will upload this complete package into FACTS and notify Nancy Day or Mark Thornock afterwards. In turn, Nancy Day will print and review the package for accuracy and completeness. If all required documentation is there, the package will be processed for Headquarters Program Secretarial Office (PSO) approval and forwarded to the Under Secretary for their signature.

The SST packet must include the following:

- Memo to Franklin M. Orr, Jr.
Under Secretary for Science & Energy
- Subject Matter Expert Approvals
 - Laboratory Director
 - Counterintelligence (Local CI SME should not concur without prior coordination with IN-25)
 - Security
 - Export Control
 - Technology Transfer
 - OPSEC
 - Cyber Security
- FACTS Printout
- Specific Security Plan (SSP)
- Cyber Security Plan
- Current INS documentation
- Current Copies of Passport and Visa Document(s);
- Curriculum Vitae/Resume (date/place of birth, major field of study and what they specifically worked on, where they lived for each year after **high school (until present)** and if they plan on return to their T3 country after they complete their research)
- Current Employment
- Letters of Support (if readily obtainable)
- Local approval signatures

If the proposed start date is near, e-mail an advanced copy of the justification and the visitor's most current CV or resume, to Mark Thornock at Mark.Thornock@science.doe.gov and copy Nancy Day at Nancy.Day@science.doe.gov.

Note: Legal Permanent Resident T3 access approval can be approved by the Site Approval Authority as well as extensions.

FOREIGN VISITS AND ASSIGNMENTS PROGRAM
Visits/Assignments by Foreign Nationals from State Sponsors of Terrorism
(SST Template Processing Checklist continuation)

This checklist serves as a guide to ensure all the paperwork and requirements of DOE Order 142.3A, *Unclassified Foreign Visits and Assignments (FV&A)* are met. Please keep in mind the processing of citizens of State Department Designated Terrorist Sponsoring Nations (i.e., currently Iran, Syria, and Sudan) takes a considerable amount of time to process, review, and adjudicate. In addition to the basic information, a comprehensive justification is also required that clearly describes the research this individual will be conducting while at the Laboratory and particularly what contributions to your programs and to DOE you expect from this individual. **All SST requests require at least 21 calendar days for DOE approval.*

<u>Step</u>	<u>Action Description</u>	<u>Date Completed</u>
1.	Complete Site/Facility Registration: (Local Databases and FACTS). (Foreign Access Central Tracking System)	_____
2.	Requests for SST must include: <ul style="list-style-type: none"> • Justification Memo to the Office of Science, Acting Director (until an Under Secretary is appointed); • Specific Security Plan (SSP); • Cyber Security Plan; • Current Copies of Passport and Visa Document(s); • Curriculum Vitae (CV); and • Letter of Support (if readily obtainable). <p><i>Forward an advanced copy (marked appropriately and protected for PII) of the CV and Justification to SC if the proposed start date is near.</i></p>	_____
3.	Complete the DOE Request Memorandum and obtain SME signatures.	_____
4.	Check with local OPSEC Manager for most recent OPSEC assessment, if appropriate.	_____
5.	Approve locally in FACTS is needed before HQ approval (Local approval comes from the Hosting Site, HQ approval from Under Secretary).	_____
7.	SST Package must be stamped/marked (OUO/Privacy Act Information).	_____
8.	All acronyms must be spelled out the first time used in the package.	_____
9.	Host responsibilities. <ul style="list-style-type: none"> • Ensure Host is aware of his/her responsibilities. • It promotes research not readily available from a U.S. citizens or non-sensitive country nationals. • Ensure all notifications are made to the Hosting Department/Office. 	_____
10.	Ensure at least 4 lines are available between the Under Secretary's title and signature block.	_____
12.	Email notification sent to Nancy Day (nancy.day@science.doe.gov) and cc: Mark Thornock (mark.thornock@science.doe.gov) of the assignment package that is initiated in FACTS (all documentation should be scanned into FACTS for processing.)	_____

**APPROVAL OF INITIAL ASSIGNMENT FOR A FOREIGN NATIONAL
FROM A COUNTRY IDENTIFIED AS A STATE SPONSOR OF TERRORISM**

DATE:

TO: Franklin M. Orr, Jr.
Under Secretary for Science & Energy

THROUGH: Patricia M. Dehmer
Deputy Director for Science Programs, Office of Science

FROM: Joseph M. McBrearty
Deputy Director for Field Operations
Office of Science

SUBJECT: Approval of Initial Assignment for a Foreign National from a Country Identified as a
State Sponsor of Terrorism

Name of Laboratory requests **(first name) (middle name) (last name)** citizen from **(country)** be granted access to the Laboratory to conduct fundamental research. Dr./Mr. **(name)** is working on **(provide brief description)** project and is uniquely qualified by **(describe their qualifications)**. We expect to further our understanding and gain expert knowledge from this project as a part of the_____.

Justification must be concise (three to four sentences) and include the main points below:
(Draft justification here for this initial assignment)

- Is the individual essential to the SC research?
 - What are the benefits to the U. S. Government and DOE SC?
 - What specific product or tool has this person created and how will these help Lab research?
 - Other circumstances (if not covered above) that are unique to this request?
-

The Lab has contacted the host and ensures the visitor will not have physical or cyber access to sensitive or classified information during this assignment.

<p>OFFICIAL USE ONLY</p> <p><u>May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: <u>6, Personal Privacy</u></u></p> <p>Name/Org: <u>Kathleen M Walker/BNL</u> Date: <u>02/02/2015</u></p> <p>Guidance (if applicable): <u>Click here to enter text.</u></p>
--

PRIVACY ACT PROTECTED INFORMATION
~ CONTAINS PERSONALLY IDENTIFIABLE INFORMATION, WHEN COMPLETED ~

FACTS Request#: _____

Visitor#: _____

_____ Visit
_____ Assignment
_____ Recurring Visit/Assignment
_____ (Please Check one)

1. Visitor Name:
2. Date of Birth:
3. Country of Birth:
4. Country of Citizenship
5. Date of Last Visit to T3 Place of Birth (or other T3 Countries [Iran/ Sudan /Syria] for the past 5 years):
6. Tentative Start and Tentative End Dates:
7. DOE Facility to be Visited/Assigned to:
8. Purpose: (Include technologies to be accessed and whether or not sensitive subjects will be discussed)
9. Justification for Visit/Assignment:
10. Benefit and Impact to DOE
11. Site FV&A Point of Contact:
12. International Agreement Involved: Y/N, If yes, list agreement_____.
13. Country of Current Residence:
14. How Long at Current Residence:
15. Status: _____ Non-Immigrant Alien _____ Legal Permanent Resident _____ Other

a. (Documentation to include Immigration number): _____

b. Passport Number: _____

Passport Expiration Date: _____

Country of Issuance: _____

c. Visa Number: _____

Visa Expiration Date: _____

Visa Status: _____

16. Indices Check Completed*: _____ Yes _____ No

a. Date Indices Completed: _____ b. Date Indices Expire: _____

17. Current Employer: (Include Name, Address, Phone Number, and Location):

18. Length of Service with current Employer:

19. Site Host's Organization and Telephone Number:

- Per the guidance provided in Deputy Secretary Daniel Poneman's memorandum, dated March 9, 2010, and entitled, "*Unclassified Foreign National Visits and Assignments*", re-occurring visits and assignments of T3 Country nationals (or born in) can be approved locally. It is strongly recommended that a documented process be implemented and approved at your site to perform these reviews and certifications after HQ has granted initial request approval. SC HQ recommends utilizing a review and adjudication process similar to the requirements from our initial request package without HQ signatures; however, this is clearly a local determination.
- Local Counterintelligence Consultations will not be accepted in lieu of the completion of indices checks for Terrorist Supporting Country packages.

OFFICIAL USE ONLY

SITE APPROVAL AUTHORITY CERTIFICATION

I certify that I have reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #**11111**, Request #**AAA1111111111**, and considered all the sensitivity factors associated with the requested access to DOE sites, programs, information and technologies. I have reviewed the advice provided by the Subject Matters Experts in Security, Cyber Security, OPSEC, Export Control, and Counterintelligence, and have addressed any concerns to the satisfaction of the Subject Matter Expert involved. My determination is consistent with reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

Additionally, I certify that any approval certifies that, in my opinion, the benefits to the Government are greater than the risks associated with the presence of the foreign national and that the legal and policy-related terms and conditions associated with the proposed *Visit/Assignment* have been met. These terms and conditions include, but are not limited to, other activities at this site, visa sponsorship requirements, visa status conditions and requirements, right-to-work requirements, and international agreements.

Requesting Facility Approving Official:

Name: **Amy Nunziata**

Title: **Associate Laboratory Director for Facilities & Operations**

Signature: _____ Date: _____

SUBJECT MATTER EXPERT CERTIFICATION

The Subject Matter Expert (SME) has reviewed the request for access approval for *Foreign National Visitor Name*, FACTS Visitor #11111, Request #AAA1111111111, and has considered all the sensitivity factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities. I have provided advice to the approval authority regarding this request, and he has acknowledged receiving my advice, and has addressed any concerns to my satisfaction. My review was consistent with the reasonable standards and practices used to ensure risk to the Government associated with access approval is appropriately identified and evaluated.

Local Security:

Kathleen M Walker

Signature and Date

Export Control:

Mark Sakitt

Signature and Date

Technology Transfer:

Michael Furey

Signature and Date

Counterintelligence:

Randy Biegelman

Signature and Date

Cyber:

James Fung

Signature and Date

Host:

Signature and Date

OPSEC:

Mark Sakitt

Signature and Date

Concurrence/Approval Form for DOE

Requesting Facility: Brookhaven National Laboratory

Name: _____ Title: **(Requesting Department Chair)**

Signature: _____ Date: _____

Name: **Amy Nunziata** Title: **Associate Laboratory Director for Facilities & Operations**

Signature: _____ Date: _____

DOE HEADQUARTERS

Name: **C. A. Murray** Title: **Director, Office of Science**

Signature: _____ Date: _____

Name: **Franklin M. Orr, Jr.** Title: **Under Secretary for Science and Energy**

Signature: _____ Date: _____

Concurrence/Approval Form for Extension/LPR

Requesting Facility:

Name: _____ Title: **(Requesting Department Chair)**

Signature: _____ Date: _____

Name: **Amy Nunziata** Title: **Associate Laboratory Director for Facilities & Operations**

Signature: _____ Date: _____

Questions to confirm with the Host for a T3 package

Host's Name (Circle Mr./Mrs./Ms./Dr.): _____

1. Are you a U.S. citizen? Yes _____ No _____

If no, please identify Country of citizenship: _____

2. Do you understand the responsibilities of hosting this visitor?
(i.e., general work scope, in the country legally, local security requirements, etc.) Yes _____ No _____

3. Do you confirm this researcher **will not** have access to any sensitive or classified information at this Laboratory during his/her stay at this Lab? Yes _____ No _____

4. Are there approved physical and cyber security (to include clear remote access determination if needed) plans in place? Yes _____ No _____

If no, can you develop these plans or will you require assistance?

As the Host of this researcher from (or born in) a Terrorist Supporting Country, I understand to contact my local CI officer at (phone # and email) if questions/issues emerge.

Visitor's Name: _____

Visitor's Country: _____

Host Signature: _____ Date of Briefing: _____

To be filled out by Office of Science Personnel Only

SC Assessment Review: Recommend Approval

CI Headquarters Coordination: _____ Date: _____

SC Associate Director Review: _____ Date: _____

SC Safety and Security Policy

Date: _____

Search...

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

OPSEC Security Plan for Unclassified Foreign National Visit/Assignment

Effective Date: **Aug 16, 2016**

The [OPSEC Security Plan for Unclassified Foreign National Visit/Assignment](#) is provided as a Word file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)

OPSEC Security Plan

(for Foreign Nationals who are citizens of, born in, or have an affiliation with a country identified as a State Sponsor of Terrorism)

Date:

(Last) (First) (Middle)

Address of Visitor/Assignee:

Citizenship:

Place of Birth (City, Country):

Employer:

Employer's Address:

Type of Visit: Visit
 Assignment
 Extensions of Assignments

Scope of Assignment:

Duration of Assignment:

Any specific International agreement:

Facility/organization to be assigned: Brookhaven National Laboratory
Upton, NY 11973

Subject code(s):

Type of Security Area:

Name of Host:

Name of Escort:

Designation of individual(s) responsible for Security Plan:

Operational Security Plan

1. Verification

Researcher's identity is verified at time of arrival.

2. Badging

Guest will be issued a photo ID badge. Guest will be required to possess and display the badge while on the Laboratory site.

3. Transportation on-site

Guest will use vehicular and foot modes of transportation.

OPSEC Security Plan

(for Foreign Nationals who are citizens of, born in, or have an affiliation with a country identified as a State Sponsor of Terrorism)

4. Role of Host

Host will ensure assignee understands his responsibilities and limitations on the assignment. Host will ensure compliance with required training, including safety. Host will ensure assignee is issued a BNL identification badge and advises assignee that it must be worn photo side out above the waist at all times on-site. Host will maintain assignee's residence, phone number, and person to be notified in event of emergency. Host will ensure the return of the BNL ID badge upon completion of the assignment. Host will advise assignee as to any restrictions with for use of communications, telephones, computers, and facsimiles, if any exist. Pertinent Safety and Department personnel will ensure compliance with restrictions for use of equipment, if any exist. There are no areas within the guest's assigned building identified as sensitive or classified. Host will be vigilant about discussions with foreign nationals that could divulge proprietary details concerning the work to be completed. Host will inform employees in the work area about this assignment and remind them to deflect inquiries that attempt to seek information not appropriate to the assignment, to include personal information, other personnel, or government programs. Such inquiries and any close and continuing contact will be reported to the BNL Counterintelligence Officer.

5. Cyber Access

See Cyber Plan attached.

6. Role of Escort

The assignee will not require access to any areas requiring an escort. In the event that an escort becomes necessary, the host or an appropriate designee will work with the foreign national to ensure the established requirements of an escort are maintained. Assignment will not include sensitive facilities, subjects, or security areas.

7. Lab Security Officers

Lab security will be notified when the assignee arrives on-site at BNL and will be advised of his workstation and residence hall if staying on-site.

8. Designation of Specific Buildings/Facilities

(Fill in areas where SST National will be going) Other public areas that may be accessed include Berkner Hall, Cafeteria, Brookhaven Center, Post Office, the Research Support Building 400, Gymnasium, Athletic Fields, Research Library, the dormitories/apartment areas, and any other facilities generally involved in tours.

OPSEC Security Plan

(for Foreign Nationals who are citizens of, born in, or have an affiliation with a country identified as a State Sponsor of Terrorism)

9. Classified Activities

Classified activities will not be accessible to the assignee and there is no need to suspend any classified activities on-site.

10. Briefing of Visitors regarding rules of conduct

This is carried out during orientation.

11. Access to site outside normal business hours

After normal business hours the assignee may be given access to facilities such as residence halls, Cafeteria, Research Library, and the building designated as the guest's work area under the cognizance of the host.

12. Briefing of all personnel who will be involved with the visit or participation

The assignment does not involve a sensitive subject area and the assignee's building is not a security facility. Host will inform employees in the work area about this assignment and remind them to deflect inquiries that attempt to seek information not appropriate to the assignment, to include personal information, other personnel, or government programs. Such inquiries and any close and continuing contact will be reported to the BNL Counterintelligence Officer.

13. Views of Operation Security (OPSEC) Committee

The Chair of the OPSEC Working Committee has reviewed the issues of this visit and has no concerns.

OPSEC Security Plan

(for Foreign Nationals who are citizens of, born in, or have an affiliation with a country identified as a State Sponsor of Terrorism)

Host: _____
(Name) _____ Signature and Date

Local Security: _____
Kathleen M Walker _____ Signature and Date

Export Control: _____
Mark Sakitt _____ Signature and Date

Technology Transfer: _____
Michael Furey _____ Signature and Date

Counterintelligence: _____
Randy Biegelman _____ Signature and Date

Cyber: _____
James Fung _____ Signature and Date

OPSEC: _____
Mark Sakitt _____ Signature and Date

[Search SBMS »](#)

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Record of Escorted Visit

Effective Date: **Sep 06, 2011**

The Record of Escorted Visit is provided as a [Word](#) file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)[Disclaimer](#)

RECORD OF ESCORTED VISIT

Requirements:

- All Escorted Visitors must complete a Guest Registration and receive CI approval prior to site access.
- All Escorts/Hosts must have current training [Hosting and Escorting Foreign Nationals](#) (TQ-SEC-FN).
- All Escorts/Hosts must be familiar with escort responsibilities as specified on page two of this form.
- All Escorts/Hosts must be BNL employees and cannot be a citizen of a sensitive or State Sponsor of Terrorism (SST) country. For a current list of sensitive and SST countries, contact the Northeast Regional Counterintelligence Office at X2234.
- An Escort can be responsible for no more than four visitors at any given time.
- This signed form shall be returned to the Foreign Visits and Assignments Coordinator for filing.

Parameters that Apply to This Escorted Visit to Brookhaven National Laboratory:

- **Submitted by:**

Name:

Department:

Life #:

Building:

Phone:

- **Date and Time:**

- **Visitor(s):**

Name

DOB

Citizenship

- **Affiliation (Name and address of Company, University, etc.):**

- **Facilities to be Accessed (Buildings/Rooms):**

- **Purpose/Justification:**

RECORD OF ESCORTED VISIT

- **INS Verification**

Passport:	Issuing Country:	Number:	Expiration Date:
Visa:	Type Of Visa:	Number:	Expiration Date:

- **Escort/Host:**

Name:	Citizenship:	Dept:
Life #:	Building:	Phone:

- **CI Approval:**

Name:	Phone:	Approval:
Denial:	Date:	GR #:

Escort Responsibilities:

An escort is a DOE/BNL employee who is assigned responsibility for a foreign national accessing the site to ensure there is no unauthorized access to controlled information or facilities. Escorts are responsible for the following:

- Familiarity with the site security requirements for all areas to be accessed.
- Understanding the purpose of the foreign national access and ensuring all activities while on-site are within the scope of the intended purpose.
- Verifying the identity of the visitor(s).
- Staying in visual proximity of the foreign national at all times, and ensuring no unauthorized access takes place.
- Reporting any unusual or suspicious occurrences in accordance with local procedures.

Acknowledgement:

The undersigned agrees to remain with the visitors at all times, preclude unauthorized access to security areas and controlled information, and ensure site access is in accordance with the above specified parameters.

Sign: _____

Print: _____ Host Training Completion Date: _____

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Request for Foreign National Access Before Indices Completion

Effective Date: **Sep 13, 2013**

Request for Foreign National Access Before Indices Completion Form is provided as a [Word](#) file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)

BROOKHAVEN NATIONAL LABORATORY

Request for Foreign National Access Before Indices Completion

Please complete Sections I, II, and III. Send original to: **GUV Office – Building 400**
Copies may be emailed to GUVCenter@bnl.gov or Faxed to x8686 in order to expedite the process

SECTION I - GUEST INFORMATION

To be completed by Host or Department GIS Administrator

GIS Administrator Name:	Visitor Name:
Phone Number:	Citizenship:
Fax Number:	Guest Registration Number:
	Visit Dates: _____ to _____

SECTION II - HOST INFORMATION

Host Name:	Sponsoring Department:
Life Number:	Date of Request: _____
Phone Number:	

SECTION III – JUSTIFICATION FOR ACCESS PRIOR TO INDICES COMPLETION

Interview: (limited to a seven day period)

Other (provide specific details, limited to a 14-day period):

I understand approval of this request will only affect the Indices completion requirement. All other Foreign Visits & Assignments requirements, such as the need for Specific Security Plans and Host training/reporting responsibilities, will remain in effect. Additionally, if information arises during the processing period that indicates the visit activities should not continue, the visit will be immediately terminated, the approval revoked, and the visitor escorted from site.

Signature of Host _____	Department Chair Authorization Print : _____ Sign: _____
---------------------------------------	---

SECTION IV – DETERMINATION

To be completed by FVA Staff

Received: _____	FACTS Numbers	Indices Status
To CI Office: _____	Visitor #:	<input type="checkbox"/> No Prior Indices <input type="checkbox"/> Indices > 30 days
To Dept./Host: _____	Request #:	<input type="checkbox"/> Indices Expired Expiration: _____ Date

To be completed by Counterintelligence Office

<input type="checkbox"/> Approved	<input type="checkbox"/> Denied	Date of Determination: _____	CI Authorizing Signature _____
-----------------------------------	---------------------------------	-------------------------------------	--

[Search SBMS »](#)

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

Specific Security Plan

Effective Date: **Aug 16, 2016**

The [Specific Security Plan](#) is provided as a Word file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)[Disclaimer](#)

Unclassified Visits and Assignments Specific Security Plan

BNL GR# or Life No. :

Foreign National Name: Last First Middle

Foreign Nation Employer/Affiliation:

Citizenship:

Inclusive dates of V/A: From (mm/dd/yyyy) To (mm/dd/yyyy)

Sponsoring Department/Division:

Host's Name Responsible for the V/A: (Last, First)

Host's Phone Number:

Host signature: _____ Date: _____

Buildings and rooms to be accessed: are as specified in the BNL-473 submitted. In addition, the F/N may have access to on-site housing, cafeteria, open meeting rooms, and recreation facilities.

The Host identified above will ensure the following:

- I. This visit/assignment(V/A) will involve access only to unclassified, non-sensitive, government information. There will be no access by the FN to any security area, including Property Protection Area, unless specified in IV below. There will be no access to Export Control information. Export Control is required to prevent regulated technology, information and software from being illegally released within or outside the United States to a foreign national who has not been granted U.S. citizenship or does not have legal permanent residence in the United States. A deemed export can occur through transfer of technology to a foreign national when such a transfer would convey an understanding of: the design, construction or functioning of the export-controlled equipment or process, or to advance significantly the development of similar equipment or processes. Contact the Export Control Officer, Mark Sakitt at X3812 for assistance in identifying Export Controlled technologies. Developments from this V/A are intended to be published in open literature.

- II. Any deviations to the planned scope of this V/A that result in an incident of security concern involving any credible information that a foreign national or an agent of a foreign power is involved will be reported to the BNL Security Operations Manager, L. Butera at 631-344-4691, the Brookhaven Field Office Senior Counterintelligence Officer, Randy Biegelman at 631-344-2234 in accordance with current DOE requirements.

Incidents Specific to Foreign Nationals - Examples of incidents include, but are not limited to:

1. Unauthorized access by a foreign national to locations that are determined not to be open to the general public.
2. Attempts by a foreign national to gain access to areas or information outside the scope of approved work related activities.
3. Any knowledge of foreign industrial or intelligence threats against BNL personnel, information, activities, facilities, and technologies.
4. Any known, or suspected, espionage activities.
5. Failure by a foreign national to notify the host of changes in name or status (e.g., passport, visa, or other USCIS information).
6. Failure by a foreign national to notify the host of any civil or criminal problems that could affect their status.
7. Failure by a foreign national to provide appropriate documentation when required or providing fraudulent documentation.
8. Access to the site by a foreign national whose activities are not exempt from the requirements of DOE Order 142.3A, Unclassified Foreign Visits and Assignments, and who has not undergone the review and approval process.
9. Access to the site by a foreign national who is not in lawful immigration status at the time the access occurs.
10. Commencement of work-related activities by a foreign national who does not possess sufficient documentation for the authority to work (when applicable for the activities involved).

For additional information on reportable foreign national activities, counterintelligence concerns, and Brookhaven Counterintelligence points of contact, please contact the Brookhaven Field Office at 631-344-2493.

III. The FN will be instructed during the check-in process on the access and security requirements at BNL. The FN will be issued a guest badge and vehicle registration, if applicable, The badge is scanned upon entry at the Main Gate and the expiration corresponds to the legal status of the FN's INS document or end of the V/A, which ever comes first. Computer access will only be allowed to the systems identified in the Cyber Security Plan for individuals from State Sponsors of Terrorism or for other foreign nationals, the BNL Domain and/or specialized data collection computers associated with experiments as determined by the appropriate systems administrator. Upon termination, all Laboratory credentials, keys, and other issued BNL equipment will be collected by the

hosting department and ITD notified to terminate computer access.

IV. Additional provisions(if any):



Search...

Search SBMS »

Management System: [Security](#)

Subject Area: [Foreign National Visits and Assignments \(Unclassified\)](#)

State Sponsor of Terrorism Processing Checklist

Effective Date: **Aug 16, 2016**

The [State Sponsor of Terrorism Processing Checklist](#) is provided as a Word file.

The only official copy of this file is the one on-line in SBMS.

Before using a printed copy, verify that it is the most current version by checking the *effective date*.

[Questions/Comments](#)

[Disclaimer](#)

Requests for Visits/Assignments
By Foreign Nationals from State Sponsors of Terrorism
(SST Template Processing Checklist)

The following information is provided to assist in preparing packages for visits and assignments to DOE facilities by foreign nationals from state sponsors of terrorism. This information is IAW DOE Order 142.3A, *Unclassified Foreign Visits and Assignments Program*, dated October 14, 2010.

A visit and/or assignment request for a foreign national from a state sponsor of terrorism must be fully documented and entered into Foreign Access Central Tracking System (FACTS) by the hosting site. The requests must have the concurrence of Subject Matter Experts, as well as completed indices checks, prior to being approved by the Approval Authority for the hosting site.

The DOE facility requesting an initial visit/assignment for a foreign national will assemble the package. Then they will upload this complete package into FACTS and notify Nancy Day or Mark Thornock afterwards. In turn, Nancy Day will print and review the package for accuracy and completeness. If all required documentation is there, the package will be processed for Headquarters Program Secretarial Office (PSO) approval and forwarded to the Under Secretary for their signature.

The SST packet must include the following:

- Memo to Franklin M. Orr, Jr.
Under Secretary for Science & Energy
- Subject Matter Expert Approvals
 - Laboratory Director
 - Counterintelligence
 - Security
 - Export Control
 - Technology Transfer
 - OPSEC
 - Cyber Security
- FACTS Printout
- Specific Security Plan (SSP)
- Cyber Security Plan
- Current INS documentation
- Copies of All Current Passport and Visa Document(s)
- Curriculum Vitae/Resume (date/place of birth, major field of study and what they specifically worked on, where they lived for each year after high school and if they plan on return to their T4 country after they complete their research)
- Current Employment
- Letters of Support (if readily obtainable)
- Local approval signatures

If the proposed start date is near, e-mail an advanced copy of the justification and the visitor's most current CV or resume, to Mark Thornock at Mark.Thornock@science.doe.gov and copy Nancy Day at Nancy.Day@science.doe.gov.

Note: Legal Permanent Resident T3 access approval can be approved by the Site Approval Authority as well as extensions.

**OFFICE OF SCIENCE
FOREIGN VISITS AND ASSIGNMENTS PROGRAM
Visits/Assignments by Foreign Nationals from State Sponsors of Terrorism
(SST Template Processing Checklist continuation)**

This checklist serves as a guide to ensure all the paperwork and requirements of DOE Order 142.3A, *Unclassified Foreign Visits and Assignments (FV&A)* are met. Please keep in mind the processing of citizens of State Department Designated Terrorist Sponsoring Nations (i.e. currently Iran, Syria, Cuba and Sudan) takes a considerable amount of time to process, review, and adjudicate. In addition to the basic information, a comprehensive justification is also required that clearly describes the research this individual will be conducting while at the laboratory and particularly what contributions to your programs and to DOE you expect from this individual. ***All SST requests require at least 21 calendar days for DOE approval.**

<u>Step</u>	<u>Action Description</u>	<u>Date Completed</u>
1.	Complete Site/Facility Registration: (Local Databases and FACTS). (Foreign Access Central Tracking System)	_____
2.	Requests for SST must include: <ul style="list-style-type: none"> • Justification Memo to the Office of Science, Acting Director (until an Under Secretary is appointed); • Specific Security Plan (SSP); • Cyber Security Plan; • Current Copies of Passport and Visa Document(s); • Curriculum Vitae (CV); and • Letter of Support (if readily obtainable). <p><i>Forward an advanced copy (marked appropriately and protected for PII) of the CV and Justification to SC if the proposed start date is near.</i></p>	_____
3.	Complete the DOE Request Memorandum and obtain SME signatures.	_____
4.	Check with local OPSEC Manager for most recent OPSEC assessment, if appropriate.	_____
5.	Approve locally in FACTS is needed before HQ approval (Local approval comes from the Hosting Site, HQ approval from Under Secretary).	_____
7.	SST Package must be stamped/marked (OUO/Privacy Act Information).	_____
8.	All acronyms must be spelled out the first time used in the package.	_____
9.	Host responsibilities. <ul style="list-style-type: none"> • Ensure Host is aware of his/her responsibilities. • It promotes research not readily available from a U.S. citizens or non-sensitive country nationals. • Ensure all notifications are made to the Hosting Department/Office. 	_____
10.	Ensure at least 4 lines are available between the Under Secretary's title and signature block.	_____
12.	Email notification sent to Nancy Day (nancy.day@science.doe.gov) and cc: Mark Thornock (mark.thornock@science.doe.gov) of the assignment package that is initiated in FACTS (all documentation should be scanned into FACTS for processing.)	_____

**APPROVAL REQUEST FOR A VISIT/ASSIGNMENT BY A
FOREIGN NATIONAL FROM A STATE SPONSOR OF TERRORISM**

DATE:

TO: Franklin M. Orr, Jr.
Under Secretary for Science & Energy

THROUGH: C. A. Murray
Director, Office of Science

FROM: Joseph A. McBrearty
Deputy Director for Field Operations
Office of Science

SUBJECT: Approval of Initial Assignment for a Foreign National from a Country Identified as a
State Sponsor of Terrorism

Name of Laboratory requests **(first name) (middle name) (last name)** citizen from **(country)** be granted access to the laboratory to conduct fundamental research. Dr./Mr. **(name)** is working on **(provide brief description)** project and is uniquely qualified by **(describe their qualifications)**. We expect to further our understanding and gain expert knowledge from this project as a part of the _____.

Justification must be concise (three- four sentences) and include the main points below:
(Draft justification here for this initial assignment)

- Is the individual essential to the SC research?
 - What are the benefits to the U. S. Government and DOE SC?
 - What specific product or tool has this person created and how will these help lab research?
 - Other circumstances (if not covered above) that are unique to this request?
-

The Lab has contacted the host and ensures the visitor will not have physical or cyber access to sensitive or classified information during this assignment.

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act
(5 U.S.C. 552), exemption number and category: 6, Personal Privacy

Name/Org: Kathleen M Walker/BNL Date: 02/02/2015

Guidance (if applicable): **Click here to enter text.**____

PRIVACY ACT PROTECTED INFORMATION

~ CONTAINS PERSONALLY IDENTIFIABLE INFORMATION, WHEN COMPLETED ~

FACTS Request#: _____

Visitor#: _____

- _____ Visit
- _____ Assignment
- _____ Recurring Visit/Assignment
- _____ (Please Check one)

1. Visitor Name:
2. Date of Birth:
3. Country of Birth:
4. Country of Citizenship
5. Date of Last Visit to T-4 Place of Birth (or other T-4 Countries if easily obtainable):
6. Tentative Start and Tentative End Dates:
7. DOE Facility to be Visited/Assigned to:
8. Purpose: (Include technologies to be accessed and whether or not sensitive subjects will be discussed)
9. Justification for Visit/Assignment:
10. Benefit and Impact to DOE
11. Site FV&A Point of Contact:
12. International Agreement Involved: Y/N, If yes, list agreement_____.
13. Country of Current Residence:
14. How Long at Current Residence:
15. Status: _____ Immigrant Alien _____ Legal Permanent Resident _____ Other

a. (Documentation to include Immigration number): _____

b. Passport Number: _____

Passport Expiration Date: _____

Country of Issuance: _____

c. Visa Number: _____

Visa Expiration Date: _____

Visa Status: _____

16. Indices Check Completed*: _____ Yes _____ No

a. Date Indices Completed: _____ b. Date Indices Expire: _____

17. Current Employer: (Include Name, Address, Phone Number, and Location):

18. Length of Service with current Employer:

19. Site Host's Organization and Telephone Number:

- It is strongly recommended that a documented process be implemented and approved at your site to perform these reviews and certifications after HQ has granted initial request approval. SC HQ recommends utilizing a review and adjudication process similar to the requirements from our initial request package without HQ signatures; however, this is clearly a local determination.
- Local Counterintelligence Consultations will not be accepted in lieu of the completion of indices checks for Terrorist Supporting Country packages.

OFFICIAL USE ONLY

CONCURRENCE/APPROVAL FORM
(Name: First NMI Last)

Requesting Facility: *Brookhaven National Laboratory*

Name:

Title: **(Requesting Department Chair)**

Signature: _____ Date: _____

Name: **Amy Nunziata**

Title: **Associate Laboratory Director for Facilities & Operations**

Signature: _____ Date: _____

Local Federal Signature Authority (or date and POC notified at the local site office)

Name: **Gerald Granzen**

Title: **Brookhaven Site Office Reviewer**

Signature: _____ Date: _____

Name: **Frank J Crescenzo**

Title: **Brookhaven Site Office Manager**

Signature: _____ Date: _____

DOE HEADQUARTERS

Name: **C. A. Murray**

Title: **Director, Office of Science**

Signature: _____ Date: _____

Name: **Franklin M. Orr, Jr.**

Title: **Under Secretary for Science and Energy**

Signature: _____ Date: _____

Questions to confirm with the Host for a T3 package

Host's Name: _____ Date of briefing: _____

1. Are you a U.S. citizen? Yes _____ No _____

If no, please identify Country of citizenship: _____

2. Do you understand of the responsibilities of hosting this visitor?
(i.e., general work scope, in the country legally, local security requirements, etc.) Yes _____ No _____

3. Do you confirm this researcher **will not** have access to any sensitive or classified information at this laboratory during his/her stay at this lab? Yes _____ No _____

4. Are there approved physical and cyber security (to include clear remote access determination if needed) plans in place? Yes _____ No _____

If no, can you develop these plans or will you require assistance?

As the Host of this researcher from (or born in) Terrorist Supporting Country, I understand to contact my local CI officer at (phone # and email) if questions/issues emerge.

Visitor's Name: _____

Visitor's Country: _____

Host Signature: _____

To be filled out by Office of Science Personnel Only

SC Assessment Review: Recommend Approval

CI Headquarters Coordination: _____ Date: _____

SC Associate Director Review: _____ Date: _____

SC Safety and Security Policy

Date: _____