

# **Argonne National Laboratory**

## **Foreign National Unclassified Visits and Assignments**

### **Host Briefing Package**

#### **Introduction**

The Foreign National Unclassified Visits and Assignments Host Briefing Package outlines the responsibilities of the host as they pertain to Department of Energy's directive for Unclassified Foreign Visits and Assignments.

Under the DOE's directive for Unclassified Foreign Visits and Assignments, the host for a foreign visit or assignment is: a DOE or DOE contractor employee who is sponsoring a visitor or assignee... The host is directly responsible for ensuring that the visit or assignment is conducted according to the plans for the visit that are reflected in the approved Form ANL-593 and the approved security plan. The host must be an Argonne employee and must be a person who is directly involved with the visit or assignment. For hosting purposes, members of APS Collaborative Access Teams who hold ANL "APS User" badges are considered to be ANL employees. DOE's directive for Unclassified Foreign Visits and Assignments also states that a sensitive country national cannot be the host of another sensitive country national.

For a particular visit or assignment, the host is designated on the ANL-593 and approved by the requesting Division Director or Department head. To serve as a host, an individual must be familiar with the material contained in this briefing document and should so signify by signing a copy of the Host Briefing Certification Form. The requesting Division/Department should retain the signed Form.

#### **Security Plans**

A security plan is required for each foreign national visit or assignment. A generic security plan is applicable if the visit or assignment does not involve any of the following conditions:

- A sensitive country national, or
- Access to a sensitive subject, or
- Access to a security area.

There is a single generic security plan for visits/assignments of the ANL-East site. The plan is maintained by the Security Department. A copy of the plan is attached to this briefing document for reference.

If all of the conditions for applicability of a generic security plan are not satisfied, a specific security plan for the visit must be developed. A template for a specific security plan is attached to this document.

#### **Host Responsibilities**

- Make the visitor/assignee feel welcome, and facilitate the visit so that both the visitor and Argonne get what they should get from the visit. Be sure that the visitor has an appropriate badge or gate pass.
- If a sensitive subject or material is involved, ensure that only that information authorized for release is made available to the foreign national.

- Provide access only to computers that are approved by host organization management for foreign national access.
- Report any suspicious or out of the ordinary behavior or questions that reach outside of the scope or intent of the visit/assignment, especially any actions or questions that may involve sensitive or classified information, to the Security or Counterintelligence Officers.
- Inform the Foreign Visits and Assignments Office of changes in the visit/assignment parameters.
  - Changes in date.
  - Changes in designated host.
  - Changes in areas of access (may require review of security plan)
  - Changes in subjects to be discussed or work to be done (may require sensitive subject or export control review)

### **Sensitive Countries**

A sensitive country is one to which particular attention is given during the review and approval process for Foreign Visits and Assignments. Countries may be designated as sensitive 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/she is a citizen of a sensitive country or is employed by the government or an institution of a sensitive country. The current list of sensitive countries is attached and also is available on the Export Control Web page.\*

A sensitive country national is also considered to be a terrorist country national if he/she is from a country on the list of State Sponsors of Terrorism of the Department of State. These countries are denoted as "embargoed" countries on the Sensitive Countries List. A visit/assignment by a terrorist country national requires specific approval by the Secretary of Energy.

### **Classified Information**

Classified information in whatever form, as well as materials, components, and other physical entities that embody classified information must always be protected from disclosure to unauthorized persons. Classified information should never be discussed, handled, generated, processed, or stored outside of specially designated security areas. If a foreign visitor is to have access to a security area where classified information may be present, special precautions detailed in a specific security plan must be in place to protect classified information. Consult the Security Department for guidance, if necessary.

---

\*The Export Control Web page is directly accessible from the ANL Home page by clicking on <Export Control> at the bottom.

## **Sensitive Subjects**

A sensitive subject is unclassified information, activity, and/or technology that is relevant to national security, nonproliferation, or economic security. The list of subjects that ANL and DOE consider to be sensitive is provided on the ANL Intranet in the Export Controls Web page. If the visit will not involve any of these subjects or relates to these subjects only to the extent of information publicly available, it is considered that the visit/assignment will not involve sensitive material. If the visit clearly will involve sensitive material as identified by someone familiar with the specific sensitivities associated with the topic area, this should be so identified on the ANL-593. This will flag the visit for Export Control and Counterintelligence review and determination.

Generally, sensitive material includes:

- Information designated as Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), Official Use Only (OUO), "Systems of Record" under the Privacy Act.
- Information or technology that requires a specific license or authorization for export. Such information or technology may be identified in regulations of the Export Administration, State Department, Nuclear Regulatory Commission, DOE, or in the Militarily Critical Technologies List.
- Technologies identified in the current ANL Sensitive Technologies List, available on the Export Control Web page.

If there is any doubt about the visit/assignment involving a sensitive subject, consult the Export Control Web page or the Export Control Coordinator. If sensitive material is involved, the host must ensure that only that information authorized for release is made available to the foreign national.

## **Exports**

An "export" is the actual shipment or transmission of items subject to the Export Administration Regulations (EAR) out of the United States or the release of information, technology or software subject to the EAR to a foreign national in the United States. In addition, information that Laboratory staff pass on to a foreign national visiting the United States -- or information that Laboratory staff pass on to a foreign national while overseas -- may also be covered by export-control regulations. Exports may include commodities, software/computer coding, and/or technical data from the United States transferred by mail, telephone, electronic mail, or facsimile; through shipment; via hand-carried materials; as a result of presentation; over the web; and/or by any other means.

By verifying that the technology, information, and/or commodities fall into one or more of the following categories, you can be relatively confident that export regulations do not apply.

- Fundamental Research and Information Resulting from Fundamental Research
- Published Information and Software (Publicly Available)
- Educational Information
- Patent Applications

Expanded definitions of these categories are contained in the Argonne Guide to Exporting available on the Export Control Web page. If you have Export Control questions you should contact the Export Control Coordinator. If material subject to export control is involved in the visit/assignment, the host is responsible for ensuring that there is no export of that material without a license.

### **Security Areas**

A security area is a specifically designated area in which work involving special nuclear material or classified matter is authorized. A security area may include limited areas or protected areas. Security areas are specifically designated as such by the ANL Security Department. If in doubt as to whether a specific area is considered a security area, consult the Security Department.

### **Computer Access**

Computer access for foreign national visitors/assignees is at the discretion of the host organization. Foreign visitors from non-sensitive countries may be granted access to computer systems that are generally accessible to users from the host organization. Foreign visitors from sensitive countries may also be authorized to have access to computer systems that are generally accessible to users from the host organization if such access is approved as part of the visit-specific security plan. Any access to computer systems beyond those generally available to members of the host organization should be reviewed by the Security, Export Control, and Cyber-security Offices on a case-by-case basis before being granted by the host organization.

If computer access is required, you must

1. As part of your account authorization process, identify the specific computer system that will be accessed and what data or applications are available to users of that computer system.
2. Provide a risk assessment identifying the vulnerabilities of your environment, the mitigations you have in place, and the impact of an exploitation of those vulnerabilities. Be cognizant of any trust relationships in your environment that accompany a computer account. For example trust relationships caused by using a common authentication service (e.g. Windows domains, UNIX's NIS, etc.) may allow an individual to log on to multiple computers and file sharing (e.g. Windows file shares or UNIX NFS mounts) may allow a user to see files on other computers.
3. Identify the access controls you have in place to manage the user's environment. In addition to the standard login process, describe default file permissions, WWW content access, ftp server access, etc.
4. Have all of the above approved by your division director and on file in your division.

It is possible that your divisional risk assessment has already addressed items 2 and 3. However, if needed, you must supplement your divisional risk assessment to address items 2 and 3.

**For Extended Assignments only:**

- Brief the visitor/assignee on his/her responsibilities and limitations while on the Argonne site.
  - Areas to which access is allowed.
  - Subject matter to be discussed.
  - Prohibited articles.
  - Safety requirements.
  - Emergency procedures, including use of the A911" system.
  - Procedures for admitting guests to the site.

**Office of Counterintelligence:**

All hosts must comply with DOE's directive for Unclassified Foreign Visits and Assignments requiring them to report any suspicious behavior or requests for information outside the stated scope or intent of the visit/assignment. Some indications of suspicious activity or inappropriate solicitation of information may include but are not limited to the following:

- A visitor who attempts to solicit information outside the stated scope or intent of the visit/assignment; specifically if the request for information may involve classified or sensitive information.
- A visitor who "wanders" away from his normal working space specifically identified in the security plan and is offended when challenged about his presence in "unauthorized" locations; or
- A visitor who does not exhibit similar levels of expertise as other members of the group, does not appear focused on the agenda of the visit, or engages in incongruous behavior for the occasion.
- A visitor who attempts to access programs, data, or applications beyond the computer access specifically approved by the host organization.

All suspicious behavior or attempts to solicit information outside the stated scope or intent of the visit/assignment should be immediately reported to the Argonne Office of Counterintelligence.

**Argonne National Laboratory-East  
Foreign National Unclassified Visits and Assignments  
Host Briefing Certification Form**

I certify that:

- I have read and understood the material in the Foreign National Unclassified Visits and Assignments Host Briefing Package
- I understand my obligations as a host to ensure that the visit or assignment is conducted according to the plans reflected in the approved Form ANL-593, the applicable security plan, and any limitations on subjects to be discussed or information or technology that may be transferred to the visitor.

Name: \_\_\_\_\_ Badge: \_\_\_\_\_ Division: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_