

ANL-E SPECIFIC SECURITY PLAN

The basic criterion which a security plan must meet is that its implementation will prevent the compromise of a DOE security interest or sensitive subject by a foreign national visitor or assignee. The plan must be completed for all visits/assignments by sensitive country foreign nationals and for non-sensitive country foreign nationals if classified or sensitive unclassified information will be access by the visitor/assignee. Security plans not meeting this criterion will not be approved causing delay in the approval process.

Specific security plans must include the following elements:

Name of visitor/assignee:

Citizenship:

Purpose of visit/assignment:

(Example) Exchange of procedures relating to non-technical bioassay

Duration:

June 1, 2000 through June 15, 2000

Location of visit/assignment (building(s) room number(s):

(Example) Building 200, rooms D110 & J152

Subject(s) to be discussed:

(Example) Advanced procedures for conducting non-destructive bioassays

Sensitive Subject: Yes No

Name of host:

Designation of individual(s) responsible for implementation of plan and required to ensure DOE security interests and sensitive subjects are not compromised:

John Doe, Group Leader, Bioassay Section

Initial verification of visitor or assignee:

(Example) Visitor/assignee will report to the Argonne Information Center for identification and access processing.

Designation of specific buildings/facilities to be utilized and specific protective measures to be employed:

(Example) Building 200 is the Chemistry Facility. The visitor/assignee will not have access to any areas that may contain sensitive information.

Briefing of hosts/escorts on their responsibilities:

(Example) Host will be knowledgeable of and involved in the visit/assignment. The host and escorts, as applicable, have been supplied with a briefing regarding their responsibilities.

Need to suspend classified activity as appropriate:

(Example) N/A, no classified involved or in area to be visited nor will access to security areas be allowed.

Access to site after normal working hours:

(Example) Visitor/assignee will be staying on site at the Argonne Guest house and will have access to common areas of the site. Off hours access to the work area will not be required during the off-hours.

Access to computers:

Note: The following are examples of the type of wording that can be used to describe computer access. Your description should reflect the actual results of assessing risk and the access control procedures utilized by your organization.

(Example - No Access) Access to computers is not anticipated. However should the need arise, an appropriate computer account will be established in accordance with Division and laboratory procedures.

or

(Example - Access) The computers that will be used by this visitor have been reviewed to verify that they contain no sensitive technology or information. Further we have reviewed the opportunities afforded users of these computers to verify that they do not indirectly permit access to other sensitive material.

Computer access (accounts) provided will:

- Implement file access controls to prevent users from maliciously accessing other user files or are non-shared computers;
- Provide only non-sensitive applications for general use.

These characteristics and other security measures are documented in divisional risk assessments and access control procedures, which are maintained by divisional Cyber Security Program Representatives.