

Classified Information & Security Requirements

1. General

The contract between Brookhaven Science Associates, LLC (BSA) and the U.S. Department of Energy (DOE) for the operation of Brookhaven National Laboratory (BNL) provides that the Laboratory must conform to all classification and security orders and requirements of DOE. DOE is empowered by Congress to issue such rules and orders as are necessary to promote the National Defense and Security. These rules and orders originate from the Atomic Energy Act and other Federal statutes, which make it unlawful to divulge information affecting the National Defense and Security except to authorized personnel.

The Atomic Energy Act of 1954, as amended, and Executive Order 12958, require that all persons be granted an Access Authorization (formerly known as Security Clearance) prior to having access to classified information or materials. Access Authorizations are granted by DOE after investigation by the Office of Personnel Management or the Federal Bureau of Investigation (FBI), determination by DOE that the granting of the Access Authorization will not endanger the common defense and security, and will be clearly consistent with the national interest.

DOE and Federal security policies further require that classified and sensitive information be protected against unauthorized access, disclosure or interception. The Laboratory is obligated to implement adequate protective security programs, which involve elements of physical security, information security, personnel security, and safeguards at facilities handling classified and /or sensitive information.

Classified visits involving foreign nationals are guided by DOE Order 142.1, Unclassified Foreign Visits and Assignments.

Information concerning BNL security protection programs is provided in the BNL Security Manual, SPIs 5-01 and 5-09.

2. Organization

The Safeguards and Security Division (SSD) is located in Police Headquarters, Building 50. The Manager of SSD is the BNL Security Manager and is responsible for establishing and administering a security program to assist employees in properly safeguarding all classified information and in complying with all security orders of DOE as required by the contract between BSA and DOE. The Security Manager normally reports to the Assistant Laboratory Director for Facilities & Operations. However, the Security Manager has access to the Director when necessary, relative to implementation of Laboratory security programs. The Classified Automated Information Security Site Manager is responsible for establishing and administering a security program involving physical, technical and emissions security considerations for classified automated data processing and word processing installations. The Laboratory Classification Officer provides classification guidance to Laboratory staff members, reviews classified document holdings and reviews new programs that may involve classified information to insure compliance with appropriate DOE Orders.

An Operations Security (OPSEC) Working Committee has been appointed to review Laboratory activities to determine if classified or unclassified sensitive programs require operational security consideration. Members of the committee are appointed by the Assistant Laboratory Director for Facilities & Operations and include knowledgeable persons from the Laboratory's departments/divisions. An OPSEC Coordinator is designated from SSD. The committee makes their recommendations to the Directorate.

3. Responsibilities of Employees with Authorized Access to Classified Information

Each person who has access to classified information is responsible for the security of that information. They are also responsible for properly limiting its dissemination.

An employee or affiliate to whom an Access Authorization has been granted has a continuing personal responsibility to notify the Personnel Security Officer at Building 30 when:

1. *Suspect illegal or unauthorized access is being sought to classified or sensitive information, technology, or special nuclear material.

2. *Believe that you may be the target of attempted exploitation.
3. *Have a close or continuing contact with foreign nationals (any contacts which are more than casual in nature - whether in a business or social setting).
4. *Are aware of actual or imminent security incidents, such as the compromise of classified information, acts of sabotage or terrorism, or approaches or contacts by hostile intelligence organizations.
5. Marry or change your name, subsequent to being granted AA.
6. Are arrested or criminally charged (including dismissals), or detained by Federal, state, or other law enforcement authorities, for any violations of the law, including traffic violations for which a fine of \$250.00 or more was imposed.
7. File personal or business-related bankruptcy.
8. Have your wages garnished.
9. Change citizenship.
10. *Are employed by, represent, or have other business-related associations with a foreign or foreign-owned interest.
11. Are under treatment for mental illness.
12. Are on a leave of absence or on extended leave and will not require access for 90 consecutive calendar days.
13. *Contemplate travel to a sensitive country.
14. Are terminated from employment.
15. No longer require access authorization.
16. Leave for foreign travel, employment, assignment, education, or residence of more than 3 months (90 consecutive calendar days) not involving official United States government business.
17. Are aware of a potential security infraction and/or violation at Brookhaven National Laboratory.

*Also report the items marked with an asterisk to the Counterintelligence Program Manager at Brookhaven National Laboratory.

Travel to a Sensitive country

Travelers who hold, or have held within the last 5 years, a DOE Access Authorization are required to complete "Request for Approval of Foreign Travel," DOE Form 1512.1, when proposing travel to a sensitive country. This form must be submitted to the Budget Office at least 45 days in advance of the departure date.

Travelers planning unofficial travel to a sensitive country who hold, or have held, a DOE Access Authorization are also required to submit form DOE F 1512.1 to the Counterintelligence Program Manager (CPM), Building 801, extension 2234, 30 days prior to departure. DOE will not dissuade unofficial travel to sensitive countries unless such travel is judged to endanger the security of sensitive programs or the personal safety of the traveler.

The responsibility to notify SSD of travel to a sensitive country continues for 5 years after a person's Access Authorization is terminated.

For a current list of countries that are designated as sensitive for reasons of national security, terrorism, or nuclear nonproliferation support, contact the [BNL Counterintelligence Office](#).

NOTE: Due to the dynamic nature of world events, other countries may, at any time, become sensitive. Therefore, caution should be exercised in dealing with citizens of countries not listed to assure that sensitive information, although unclassified in nature, is not inadvertently disclosed. This would include nuclear and other U.S. technology and economic information.

4. Responsibility of Employees Not Possessing Access Authorization to Classified Information

Any employee who does not possess Access Authorization and who receives or finds classified matter must safeguard it and immediately notify the Security Manager. Classified matter may be identified by the official classification marking "Top Secret," "Secret" or "Confidential," which is located on the top and bottom of each page of a document containing classified information.

5. Principles Governing Communication of Classified Information

Classified information, whether in oral or documentary form, will be communicated only in appropriate security areas, and only to those persons with the required level of Access Authorization and who have a "need to know" in the course of their duties.

No person is entitled to receive classified information solely by virtue of his or her official position or solely by virtue of having been granted Access Authorization.

No discussion of classified information shall occur in a non-security area or within the hearing of persons who are not authorized to have such knowledge.

Classified information must not be discussed on unsecured telephones. Secure Telephone Units (STU-III) are available. Contact the Security Manager if use is required.

6. Storage of Classified Matter

Secured facilities for the storage and use of classified matter are maintained in Buildings 50 (Police Headquarters), 801 (CI), and 197C (2nd Floor) (Global Security Division). Access to these facilities (security areas) can be arranged through the Personnel and Information Security Office, Building 30.

7. Receipt of Classified Matter

The Laboratory Classified Document Control Officer (CDCO) shall control all classified matter transmitted to and from the Laboratory, and matter transmitted between security areas within the Laboratory.

Any person who expects to receive or use classified matter should have it mailed or delivered to the BNL classified mailing address:

Brookhaven Science Associates
Brookhaven National Laboratory
ATTENTION: Document Custodian
Post Office Box 155
Upton, NY 11973-0155

Upon receipt of classified matter, the SSD Document Custodian will notify the addressee. Any person who receives classified matter through the U.S. mail, by courier or otherwise, shall immediately deliver it to the SSD Document Custodian without opening. In the event it is received after normal working hours, take it to Police Headquarters, Building 50, where it will be locked in a safe until it can be delivered to the SSD Document Custodian.

8. Receipt of Classified Materials

Any person who expects to receive or use classified material (Hardware) should have it mailed or delivered to the BNL classified shipping address for classified material:

Brookhaven Science Associates
Brookhaven National Laboratory
Attention: Document Custodian
Police Headquarters, Building 50
24 Upton Road
Upton, L.I., New York 11973

BNL is not authorized to receive or produce Top Secret matter. For all accountable and all Secret matter, DOE F 5635.3, "Classified Document Receipt," or a receipt comparable in content, should accompany all classified matter transmitted outside of the Laboratory.

9. Use of Classified Documents

The handling of all classified documents shall be confined to an approved security area. This includes reading, transmittal, preparation, writing and typing of classified documents. Security areas are only those areas designated by the Security Manager and approved by the DOE-Chicago Operations Office. Unescorted access to a security area is limited to those individuals with proper Access Authorization and need-to-know.

10. Transmittal of Classified Documents

The CDCO is responsible for the transmittal of all classified documents to any other facility within and outside the Laboratory. Upon request, the CDCO will arrange to have classified documents

sent to the appropriate and approved classified repository. In the exceptional case that it may require being hand-carried, special arrangements must be made with the Security Office. Handling and wrapping requirements for hand-carried classified documents are clearly stated in the BNL Security Manual.

The CDCO shall be notified when a classified document is no longer needed with a request that it be returned to its original source. Every effort should be taken to minimize the number of classified documents in storage at the Laboratory. Those not required should be returned to their original source, or destroyed.

11. Classification of Documents

Anyone who determines that a document may be classified should consult with the Laboratory Classification Officer before distributing the document. The Laboratory Classification Officer will arrange to have an Authorized Derivative Classifier (ADC) review the document.

12. Classified Meetings

All discussions and meetings involving classified information must be held in a security area. The Laboratory maintains security areas, which are suitable for such meetings and discussions. These security areas are available upon request. All participants are required to have the appropriate Access Authorizations. Verification of Access Authorization Level is made by the Personnel Security Officer in Building 30.

13. Types of Access Authorization

"Q" Access Authorization permits the person to whom it is granted to have access to DOE Top Secret, Secret, and Confidential Restricted Data and National Security Information as may be required in the performance of assigned duties.

"L" Access Authorization permits an individual to whom it is granted access to DOE Secret and Confidential National Security Information and confidential Restricted Data as may be required in the performance of assigned duties.

14. Requests for Access Authorization

Requests for Access Authorization are made by Department Chairs or Division Managers to the Security Office, using BNL Form E3 "Request for Access Authorization" and DOE F5634.2 "Contract Security Classification." The Security Office will furnish the individual, for whom an Access Authorization has been requested, with the required forms for completion and return. These individuals must report to the Security Office, Building 30, to complete fingerprint cards and to be briefed on procedures for correctly completing required forms. The Security Office will notify the Department Chairs or Division Managers and the individuals concerned when the Access Authorization has been granted.

15. Responsibility of Department Chairs or Division Managers

The appropriate Department Chair or Division Manager shall notify the Security Manager when:

- It is anticipated that an employee will require an Access Authorization in the performance of his or her assigned duties. The justification for the Access Authorization must be in accordance with DOE Order 472.1B Attachment (1) Personnel Security Activities.
- The duties of an employee with an Access Authorization change negating the need for an Access Authorization, or the employee is transferred to another department.
- An employee possessing an Access Authorization is absent from the Laboratory for a period in excess of 90 days, hospitalized 90 days or more or otherwise treated for a mental illness, which may cause a defect in judgment or reliability.

16. Safeguards and Security Awareness Program

The Safeguards and Security Awareness Program includes all personnel authorized or expected to be authorized access to classified matter or special nuclear materials and personnel routinely exposed to sensitive information, activities or facilities. The DOE Safeguards and Security Awareness Program, which is conducted by SSD personnel, requires the following briefings:

- **INITIAL SECURITY BRIEFING** - To acquaint all new employees with local security procedures and to familiarize these individuals with their responsibilities to protect government property from theft, loss or damage.
- **COMPREHENSIVE BRIEFING** - The comprehensive briefing is designed to acquaint individuals who are granted DOE access Authorizations with their responsibilities concerning the classification, protection, and control of classified information and materials, security regulations and reporting requirements.
- **REFRESHER SECURITY BRIEFING** - The refresher security briefing provides individuals who possess DOE Access Authorizations current information on security regulations and information relating to their security responsibilities. Refresher briefings are mandatory for individuals possessing an active DOE Access Authorization. This briefing must be received no later than 12 months after the comprehensive briefing.
- **TERMINATION BRIEFING** - This briefing is given to an individual whose DOE access Authorization is terminated for any reason. The briefing is designed to ensure termination of all classified activities by the individual, outline penalties for unauthorized disclosure of classified information and assure return of any and all identification badges or credentials issued for official use.

17. Counterintelligence Program - See SPI 5-14

The Laboratory's Counterintelligence Program Manager (CPM) works for the Director's Office and normally reports to the Deputy Laboratory's Director of Operations. The CPM is responsible for the management, administration, and implementation of the Laboratory's Counterintelligence Program, which includes awareness training, pre- and post-foreign travel briefings to sensitive and non-sensitive countries; and conducts liaison activities with Federal and local counterintelligence law enforcement agencies.

Counterintelligence as defined by DOE is the information gathered and activities conducted to protect against espionage; other intelligence activities; sabotage or assassinations conducted for or on the behalf of foreign powers, organizations, or persons, or international terrorist activities.

The program's purpose is to deter and neutralize foreign industrial or intelligence activities directed at or involving DOE programs, facilities, technology, personnel, unclassified sensitive information, and classified matter. A significant aspect of the program is the required briefing of Laboratory employees who will be performing official foreign travel. Travelers going to sensitive countries are required to contact the CPM upon return to schedule a debriefing.

It is the responsibility of the BNL traveler to inform the CPM, ext. 2234, of any travel plans that will involve going to those sensitive countries listed in Section 3 of this SPI. The traveler will receive a Foreign Travel Briefing. This briefing provides the traveler with information they need to be aware of, including intelligence-gathering methods they may be exposed to, and defensive measures and precautions they should consider. Travelers going to sensitive countries are required to contact the CPM upon return to schedule a debriefing.

18. Visits or Temporary Assignments to Other Classified Areas

All visits or temporary assignments by BNL personnel to another classified site must be approved by the administration of the site to be visited. At least ten working days prior to the visit (assignment), the dates of the proposed visit, person to be visited, and the purpose of the visit should be submitted to the site to be visited.

19. Annual Reviews

Annually the Security Manager will furnish Access Authorization listings of assigned employees and affiliates to Department Chairs and Division Managers for determination of the continued need for such Access Authorizations. These lists are to be returned to the Security Manager, Building 50, with appropriate notations and /or comments.

20. Reinvestigation Programs

Each person to whom a "Q" or "L" Access Authorization has been granted is required to complete a "Questionnaire for Sensitive Positions," Form SF86, every five years for "Q" and every ten years for "L", in accordance with the DOE responsibility to confirm the continued eligibility of the person to have access to classified information.

21. Termination of Access Authorizations

The Personnel and Information Security Officer, Building 30, shall be notified when any person's Access Authorization is terminated or when:

- Laboratory employment or affiliation is terminated.
- The individual will be outside the United States for three months or more on nonofficial business.
- The individual is absent from work for three months or more.

Upon termination of access Authorization, the employee or affiliate will be debriefed and sign a "Security Termination Statement," DOE Form 5631.29.

22. Reinstatement of Access Authorization

Department Chairs or Division Managers may request reinstatement of Access Authorization in appropriate cases by forwarding a memorandum to the Security Office. If more than six months have elapsed since termination of an Access Authorization and more than a year has elapsed since the date of the last Questionnaire for Sensitive Positions (SF86), or any significant changes are known to have occurred since that date, a person for whom reinstatement is desired must complete a new SF86. In all cases a new Security Acknowledgment statement (DOE Form 5631.18) must be completed.