

# Personnel Security

## 1. General

The provisions of the Atomic Energy Act of 1954, as amended, and Executive Order 12958 of April 17, 1995, Classified National Security Information, require that all persons must be granted an Access Authorization (also known as Security Clearance) before having access to classified information or materials.

Access Authorization may be granted by the Department of Energy after an investigation by the Office of Personnel Management or the Federal Bureau of Investigation, and a determination made by DOE that the granting of the Access Authorization would be clearly consistent with the national interest.

## 2. Types of Access Authorization

### "Q" Access Authorization

"Q" Access Authorization is appropriate for and permits the person to whom it is granted access to special nuclear material or DOE classified information at the levels of Top Secret, Secret, and Confidential, and information in the classification categories of Restricted Data, Formerly Restricted Data, and National Security Information as required in the performance of assigned duties.

### "L" Access Authorization

"L" Access Authorization is appropriate for and permits the person to whom it is granted access to DOE classified information at the levels of Secret and Confidential National Security Information, Confidential Restricted Data, and Formerly Restricted Data as may be required in the performance of assigned duties.

"L" Access Authorization is appropriate for craft and manual workers, service personnel, health and safety workers, and others employed in areas of classified operations provided the work of such persons does not afford them:

- More than visual access to buildings and equipment classified not higher than Secret
- Access to information classified higher than Confidential Restricted Data or Secret National Security Information

### **3. Request for Access Authorization (Security Clearance)**

Requests for Access Authorization are made by Department or Division Managers to the Personnel Security Office, Building 30, using BNL Form E3 "Request for Access Authorization." After the Personnel Security Specialist receives this form, the person for whom Access Authorization has been requested will be given the required forms, Standard Form 86 "Questionnaire for Sensitive Positions" and BNL Request for Background Information, "CARCO." These completed forms must be returned to the Personnel Security Office. Individuals requesting Access Authorization must also report to Building 30 to be fingerprinted. The completed forms, less CARCO, are then sent to the Chicago Operations Office, U.S. Department Energy for processing.

### **4. Notification of Access Authorization Granted**

The Personnel Security Office will notify the individual when Access Authorization has been granted. A Security Briefing explaining the responsibilities of those holding an Access Authorization will be given at the Personnel Security Office when the security clearance is granted. The Department Chair or Division Manager will be notified after the individual's briefing has been completed

### **5. Responsibilities of Department Chairs or Division Managers**

The Department Chair or Division Manager shall notify the Security Office when a cleared individual in their Department or Division:

- Terminates his/her Laboratory employment or affiliation.
- Transfers to another department or division.

- Transfers to other duties within your department/division which require a different level of AA, or which does not require AA.
- Is arrested, charged criminally (including dismissals), or detained by Federal, State, or other law enforcement authorities, for any violation of the law, including traffic violations for which a fine of more than \$250.00 or more was imposed.
- Is hospitalized or treated for mental illness which may cause a defect in judgment or reliability.
- Is on leave of absence or extended leave, and will not require access for at least 90 days.
- Has his/her wages garnished.
- Files for personal or business-related bankruptcy.

Department Chairs and Division Managers are responsible for ensuring that personnel under their supervision having authorized access to classified information are properly instructed in, and are thoroughly familiar with, procedures and requirements for safeguarding such information.

## **6. Responsibilities of Employees with Access Authorization**

The responsibility for controlling the dissemination of classified information rests upon each authorized individual who may have access to such information.

An employee or affiliate to whom Access Authorization has been granted has a continuing personal responsibility to notify the Personnel Security Specialist immediately if they:

- Find classified matter unattended.
- Realize classified matter is lost or stolen.
- Change your home address, marital status, name or citizenship.
- File for personal or business-related bankruptcy.
- Intend to travel to a sensitive country for either business or personal reasons.
- Expect to be outside the U.S. for more than three months on non-official business.
- Have your wages garnished.
- Are on a leave of absence or on an extended leave and will not require access authorization for 90 consecutive calendar days.

- Are hospitalized or undergoing treatment for a mental illness; treatment for drug abuse; or treatment for alcohol abuse.
- Are arrested, charged criminally (including dismissals), or detained by Federal, State, or other law enforcement authorities, for any violation of Federal, State, county, or municipal law, regulation, or ordinance, including traffic violations for which a fine of more than \$250.00 or more was imposed, within or outside the U.S.
- Experience illegal or unauthorized access being sought to classified or sensitive information, technology, or special nuclear materials.
- Believe that you may be the target of attempted exploitation.
- Have continuing contact with foreign nationals (any contacts that are more than casual in nature, whether in a business or social setting).
- Have knowledge 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.
- Become employed by, are a representative of, or have any other business-related association with a foreign or foreign-owned interest, or foreign national.

## **7. Travel to Sensitive Countries**

The BNL Counterintelligence Officer must be notified of travel contemplated to sensitive countries as set forth in applicable DOE Orders pertaining to "Foreign Travel Authorization".

Travelers who hold, or have held within the last five years, a DOE Access Authorization are required to complete a DOE Request for Foreign Travel in the Foreign Travel Management System when proposing official travel to a sensitive country. The BNL Foreign Travel Office can be contacted on Extensions 6042 and 6043. The request must be submitted to the Foreign Travel Office at least 30 days in advance of the departure date to ensure approval. Prior to travel to a sensitive country, it is mandatory that the traveler receives a pre-foreign travel briefing conducted by the BNL Senior Counterintelligence Officer. Upon receipt of a foreign travel trip report, the BNL Counterintelligence Office will schedule a travel debriefing with the traveler.

Travelers planning unofficial travel to a sensitive country, who hold or have held, within the last five years a DOE Access Authorization are required to notify the Counterintelligence Office two

weeks in advance of the proposed travel. At the discretion of the BNL Senior Counterintelligence Officer, the traveler may be required to complete a pre-travel briefing. Upon completion of the trip, the traveler shall contact the BNL Counterintelligence Office to notify them that the trip has been completed. Then at the discretion of the BNL Senior Counterintelligence Officer, a travel debriefing may be required.

See the BNL Counterintelligence Program [Sensitive Country List](#).

**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. Such information includes nuclear and other U.S. technology and economic information.

## **8. Classified Visits to Other Sites**

All visits by cleared BNL personnel to discuss classified information at another DOE site must be approved by the administration of the site to be visited. At least ten working days before the visit, the dates of the proposed visit, the person to be visited, and the purpose of the visit shall be submitted to the site to be visited. If the visit is to a non-DOE site, or a DOE site requiring special access, a DOE form 5631.20 must be prepared and brought to the Personnel Security Office, Building 30, at least 10 working days before the visit.

## **9. Escort Responsibilities for Uncleared Visitors**

Visitors shall be escorted at all times while in a protected/secured area. The escort will:

- Verify the identity of the visitor(s), using a form of photo identification.
- Keep the visitor(s) under observation at all times.
- Ensure the visitor(s) signs in and out on the visitor register each time they enter and leave the area.
- Require that the visitor(s) display the visitor badge at all times. The badge must be worn on the upper front portion of the body, on the outer garment.
- Ensure that the visitor(s) returns the visitor badge at the end of the visit.
- Precludes any exposure or access to sensitive or classified information.

- Prohibits cameras, pagers, and cell phones in the security area.
- Ensures that no more than four visitors are escorted by one cleared escort.

Uncleared U.S. citizens may be authorized to visit security areas for official purposes. Such visitors will be under authorized escort.

Nationals of sensitive foreign countries are not allowed in security areas. They cannot be taken into those areas, even under escort. Nationals of non-sensitive countries may be allowed escorted entry into security areas, but only after Chicago Operations Office has approved a specific plan covering their visit to the area. These rules apply to all foreign nationals, including those who may be employees or subcontractors performing building maintenance or modifications, e.g., plumbers, carpenters, and electricians. These rules are explained in detail in the applicable DOE Order, and [SPI 5-09, Visits and Assignments of Foreign Nationals](#).

## **10. Annual Reviews**

The Personnel Security Office will furnish listings annually to Department Chairs and Division Managers of employees and affiliates who possess active Access Authorizations to determine the continued need of such Access Authorizations.

## **11. Reinvestigation Programs**

Each individual to whom "Q" or "L" Access Authorization has been granted will be sent a Standard Form 86, "Questionnaire for Sensitive Positions," and associated forms every five years for "Q" AA, and every 10 years for "L" AA, to be completed in connection with the DOE responsibility to confirm the continued eligibility of the individual to have access to classified information.

## **12. Termination of Access Authorizations**

The Access Authorization of an individual shall be terminated when:

- Laboratory employment or affiliation is terminated.
- The Department Chair or Division Manager determines that the duties of an employee or affiliate have changed and an Access Authorization is no longer required.

- The individual is on a leave of absence or an extended leave and will not require access for 90 consecutive calendar days.
- The individual will be outside the United States for three months or more on non-official business.
- Access to classified matter is no longer required due to transfer to a position not requiring such access.

When the Access Authorization of the employee or affiliate is terminated, he or she will sign DOE Form 5631.29, "Security Termination Statement," and will be given a security debriefing at the Personnel Security Office.

### **13. Reinstatement of Access Authorization**

Department Chairs or Division Managers may request reinstatement of Access Authorization in appropriate cases by forwarding a Form E-3 to the Personnel Security Office. Appropriate paperwork will be given to the individual for completion.

### **14. Changes in Status**

The Personnel Security Officer must notify the DOE Chicago Operations Office of name changes. When an individual with an access authorization marries, a DOE Form 5631.34, "Data Report on Spouse," must be completed and forwarded to the Personnel Security Office.

### **15. Rebriefings**

DOE Orders require that security rebriefings be given yearly to individuals holding access authorization. Individuals will receive appropriate instructions from the Personnel Security Office.

### **16. Laboratory Identification Badges/Cards**

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

### **17. Secure Area Access (Encoded Security Badge)**

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

## 18. Foreign Ownership, Control, or Influence Program (FOCI)

The FOCI Program is administered by Brookhaven's Procurement and Property Management Division. The purpose of the U.S. Department of Energy FOCI Program is to ensure that the degree and extent of FOCI does not pose an undue risk to national security.

## 19. Definitions

**Access:** The knowledge, use, or possession of classified information or other sensitive information, which is required by an individual in the performance of official duties. Access is provided on a "need-to-know" basis.

**Access Authorization:** An administrative determination that an individual who is either a DOE employee, an applicant for employment, a consultant, an assignee, other Federal departmental or agency employee (and other persons who may be designated by the Secretary of Energy), or a contractor or subcontractor employee for DOE, is eligible for access to Restricted Data, other classified information, or special nuclear material. Clearances granted by the DOE at BNL are designated as "Q" or "L."

**Classified Information:** Any information that requires protection against unauthorized disclosure in the interests of the national defense and security or foreign relations of the United States pursuant to U.S. statute or Executive order. The term includes Restricted Data, Formerly Restricted Data, and National Security Information, each of which has degrees of importance denoted by the classifications Top Secret, Secret, or Confidential.

**Derogatory Information:** Unfavorable information concerning an individual which creates a question as to the individual's eligibility or continued eligibility for access or suitability for Federal employment.

**Need-To-Know:** Official determination by a knowledgeable official, which allows an employee, contractor, or properly cleared individual access to specific classified information in the performance of official duties.