

BROOKHAVEN NATIONAL LABORATORY

SBMS Interim Procedure

Interim Procedure Number: 2004-002 **Revision:** 0

Title: Critical and Sensitive Computer Systems, Identification and Access

Point of Contact: Kathleen Hauser

Management System: Information Resource Management System

Effective Date: August 21, 2004

Expiration Date: December 31, 2004

Approved by (Line management, Management System Steward): Kathleen Hauser, Thomas Schlagel

Approved by (Deputy Director, Operations): Michael Bebon

Applicability: Computer Users, Owners, and System Administrators.

General:

This interim procedure describes how to identify critical and sensitive systems, and how to apply for a computer account on these computer systems.

Computers requiring special access restrictions and protective measures are identified as either critical or sensitive.

1. Critical System - a system is considered critical when the laboratory or a department cannot complete its mission if the system is unavailable for a period of 24 hours.
2. Sensitive System- a system is considered sensitive when the information stored on it meets certain criteria such as the following, and access to the system must be limited.
 - Confidential Foreign Government Modified Handling (CFIG/Mod)
 - Unclassified Controlled Nuclear Information (UCNI)
 - Export Controlled Information (ECI)
 - Certain Official Use Only Information (OUO) not listed below.
 - Proprietary Data- Technical data that embodies trade secrets developed at private expense (i.e. design procedures or techniques, chemical composition of materials, etc.).
 - CRADA Information- A CRADA (Cooperative Research and Development Agreement) is a written agreement between a private company and a government agency to work together on a project.
 - Privacy Act- Data related to records maintained on individuals (e.g. Medical Records, Payroll, etc.) Generally, computers holding large personnel databases fall into this category, not individual work stations with a few employee records.
 - Protected Health Information (PHI)- Individually identifiable health information that (a) relates to the past, present, or future physical or mental condition of an individual, (b) can either identify the individual, or there is a reasonable basis to believe the information can identify the individual, and (c) is received or created by or on behalf of a health plan. This information is covered by HIPAA. Note that employment records held by BNL or BSA in their capacity as employers are not PHI.

Note: A computer containing UNCI, CFIG/Mod, ECI or certain OUO are subject to restricted foreign national access. If the owner of a critical system determines that FN access should be restricted, the critical system would be identified as both critical and sensitive, and hence, would follow the procedures for access to such systems.

IDENTIFYING CRITICAL AND SENSITIVE COMPUTERS

Owners of critical or sensitive systems must do the following:

1. Determine the category of information on the system.
2. Inform the system administrator to register the system and perform the risk assessment questionnaire.

System administrators must do the following:

1. Complete the administrator's network registration form at <https://intranet.bnl.gov/itd/reg/admin/>.
2. Identify the computer as critical or sensitive by selecting the link at the bottom of the registration page.
3. Complete the risk assessment questionnaire (along with the system owner) that will identify the protective measures employed for this computer.

Information Technology Division (ITD) will do the following:

Maintain a database of Critical and Sensitive computers recording the [category](#) of information on the computer (e.g. Critical or Sensitive - Privacy Act), the [risk assessments of the computers](#), and any restrictions on foreign national access to the computers

The OPSEC Working Committee will do the following:

Notify the ITD [Chief Cyber Security Officer](#) of all sensitive programs, indicating the Principal Investigator (PI) of the program and any foreign national access restrictions.

The Office of Intellectual Property will do the following:

Notify the [ITD Chief Cyber Security Officer](#) of all CRADAs and Proprietary Research Agreements, indicating the Principal Investigator (PI) of the program, and any foreign national access restrictions.

The ITD Chief Cyber Security Officer will do the following:

1. Work with the principal investigators (PIs) of sensitive programs to identify the computers that hold sensitive information.
2. Provide to the OPSEC Working Committee and the BNL Counterintelligence Office access to the Critical and Sensitive Computer database.
3. Perform a risk analysis for each critical or sensitive system based on the completed risk assessment questionnaires. They will then assist the system administrators to improve security based on the results of the risk assessment.

ACCESS TO CRITICAL AND SENSITIVE COMPUTERS

A user must do the following to apply for an account on a critical or sensitive computer:

Request an account from the system administrator. This may be done using the [Account Request Form](#) if it is used for that system. Otherwise, the user should speak to the system administrator directly.

A system administrator must do the following to create an account on a critical or sensitive computer:

1. Verify that the user has an active appointment as an employee or guest and has completed cyber security training before creating a computer account via the [Computer Access Verification and Registration Form](#).
2. Check with the PI before creating an account for a user on a system with restricted foreign national access.
3. Maintain a record of the account indicating:
 - a. The user's name and the name used to log into the account.
 - b. The user's BNL status (employee, guest, etc.)
 - c. The user's citizenship and country of birth.

- d. The computer on which the account was created.
- e. Who created the account.
- f. The termination date for the account (no later than the termination date of the user's BNL appointment).
- g. For systems with restricted foreign national access – PI approval.

The account information must be recorded by one of the following three methods:

- a. The information can be entered in the BNL account database using the [Computer Access Verification and Registration Form](#).
 - b. It can be entered in the BNL account database using scripts provided by ITD. (Contact the ITD Enterprise Service Desk (itdhelp@bnl.gov) for more information.)
 - c. The system administrator can maintain the information individually.
4. **Note:** A system administrator must not create an account for a foreign national on a system with restricted foreign national access (UNCI, CFG/Mod, ECI or certain OOU) without explicit instructions from the PI.

A principal investigator responsible for sensitive systems must do the following:

1. Approve accounts on systems with restricted foreign national access.
2. Inform the OPSEC Working Committee of any foreign nationals who need access to computers with restricted foreign national access and wait for their approval before allowing a system administrator to assign an account.

The OPSEC Working Committee must do the following:

Coordinate the appropriate reviews of requests for access by foreign nationals to computers containing foreign national restricted information and inform the PI of the decision.

Definitions

Foreign national – A foreign national is any person who is not a U.S. citizen, and includes permanent resident aliens.

OPSEC (Operations Security) - is an analytic process used to deny an adversary information (generally unclassified) concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations. OPSEC does not replace other security disciplines - it supplements them.

OPSEC Working Committee – The OPSEC Working Committee reviews the programs at the Laboratory to determine if classified or unclassified sensitive programs require operational security measures to prevent the inadvertent release of sensitive or classified information. The committee determines if programs are sensitive and what measures, if any, are required to protect the program. See <https://sbms.bnl.gov/LD/LD16/ld16d261.htm>

Principal Investigator – The leader of a research program.

System administrator – A person responsible for maintaining and operating a computer. A system administrator's responsibilities include creating, maintaining, and terminating accounts on the computer.

Questions about this Procedure can be directed to the [Chief Cyber Security Officer](#).