



a passion for discovery

Cyber and Physical Security Stand Down

Training number: TQ-CYBER-PII-SD

October 5, 2006

Managed for the U.S. Department of Energy
by Brookhaven Science Associates



Cyber and Physical Security Stand Down: Why are we doing it?

- Cyber and physical security maintains the integrity of the research and protects personal information at Brookhaven Lab. It also denies unauthorized access to other government computing resources.
- A strong cyber and physical security program is essential to compete effectively for research and project funding.
- We have made substantial progress, but we have identified continued risks.
- We must raise awareness across the Lab and document areas for improvement.

Cyber Security at Brookhaven

[John Gould or Nick Franco](#)

- Know who your organization's cyber security point-of-contact is.
- Be aware of the SBMS Unclassified Cyber Security subject area.
- Some basics on computer accounts and passwords:
 - Must be active employee or guest appointment
 - Must complete cyber security training
 - Computer accounts (giving access to a computer) are for BNL business and limited personal use only
 - Passwords must comply with BNL password policy

NOTE: The cyber security stand down webpage provides more details about today's presentation:

<http://intranet.bnl.gov/cybersecurity/standdown>

Basic Cyber Security Requirements

- All devices connecting to the network must be registered.
- All computers must display logon banner:

NOTICE TO USERS

This is a Federal computer system (and/or it is directly connected to a BNL local network system) and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. **LOG OFF IMMEDIATELY** if you do not agree to the conditions stated in this warning.

Basic Cyber Security Requirements (cont.)

- Physically protect your computing resources.
 - Use password-protected screen saver
 - Lock office when away. Ensure open-area computers are protected.
- Protect BNL computers used off site.
- Comply with software copyright laws.
- Use virus protection; don't assume disk/memory stick safe.
- Keep the operating system on your computer up to date.
 - The Lab requires that you use supported operating systems.
 - When notified about available software updates, update the software on your computer.
- Report computer security incidents. Call Ext. 5522.
- Disregarding cyber security procedures can result in disciplinary action.

Basic Physical Security Requirements (cont.)

- Wear your ID badge properly at all times and keep it in a safe place when you are off site.
- Lock all windows and office doors (if possible) when you leave your work area for an extended period of time.
- Lock/secure all buildings and facilities after normal business hours, weekends, and holidays.

Basic Physical Security Requirements (cont.)

- Report suspicious personnel, activity, and circumstances to the Police Group.
 - Ext. 2238 or 2239
 - Ext. 2222 (emergency only)
 - 911 (emergency only)
- Update building manager contact information and post it on the exterior of your building.

Basic Physical Security Requirements (cont.)

- Protect any paperwork containing protected personally identifiable information (PII) by keeping it secured in a locked receptacle (room, filing cabinet, desk) when not in use.
- DOE definition of PII:
 - Protected PII: social security number, passport number, credit card numbers, clearances, bank numbers, biometrics (thumbprints, etc.), date and place of birth, mother's maiden name, and criminal, medical and financial records
 - Public PII: first/last name, address, phone number, general education credentials, BNL ID number
- Separate presentation for PII training. Training number: TQ-PROTECTID

Personal Security Suggestions

- The Laboratory's Safeguards & Security Division urges all employees and visitors to take reasonable and prudent steps to protect personal belongings and their own safety and welfare
- Remember that all employees and guests are required to wear their ID badges at all times while at work. This will help to identify any unauthorized persons on site.
- If you are working alone in the evening and feel uncomfortable, contact Police Headquarters at Ext. 2238.

Personal Security Suggestions (cont.)

- After work hours and particularly when dark:
 - Try to keep in well-lit walkways as much as possible; avoid short cuts through the woods.
 - Have your office, room or vehicle key ready before you reach your door.
 - Look inside your vehicle before you get in; lock your doors and park in well-lit areas.
- Trust your instincts. If something or someone makes you uneasy, leave the area or call Police Headquarters at Ext. 2238 or 2239.

Cyber and Physical Security Stand Down: What is planned for the day?

- 8:30 a.m. – 5 p.m. Network connection between the Lab and the Internet disconnected
- Activities that must be completed during the day:
 - Mandatory department/division all-hands meetings
 - Personally Identifiable Information training
 - Using checklists and spreadsheets, take immediate corrective actions for cyber security and identify areas of concern
 - Using checklists, do walk-downs of work areas to assess physical security
 - Discussion of day, concerns, corrective action plans
 - Report back results
- Information Resource Center open all day to respond to questions; call Ext. 8650, 8651, 8652, 8653 [or call John Gould or Nick Franco](#)

You Can Help

- Discussion
- Lab Director Sam Aronson will report stand down results to staff
- What we do today will help the Laboratory compete effectively for research and project funding in the future

Employee Checklist

(a “Bottoms-Up” approach)

Employees will take the following actions on Thursday, October 5, 2006, and report back to their managers.

- Detailed instructions for accomplishing the actions below are at:
- <http://intranet.bnl.gov/cybersecurity/standdown/checklist>
- Check that your passwords meet DOE password requirements and change them if they do not (including e-mail, PCs, PeopleSoft, etc.). Ensure that any hard copy passwords are securely stored.
- Check to ensure that your computers have a password-protected screen saver set for 15 minutes of inactivity or less. Install on those that do not.
- Check to ensure that all computers have the DOE logon banner installed. Install on those that do not.
- Verify that the only Windows operating systems are Windows XP, Windows 2000 (Service Pack 4), or Windows 2003.
- Verify that Windows systems are configured for automated patching.
- Ensure that Trend Micro anti-virus software is installed on all Windows systems.
- Determine if you have protected personally identifiable information (PII) on your computers.

Group Leader Checklists

C-AD Group _____

Group leaders will take the following actions.

- Gather responses from employee checklists and update your group Excel spreadsheet.
- Verify and change, as needed, the owner and system administrator for each computer and list changes on Excel spreadsheet.
- Review and update list of UNIX, Linux, Macintosh systems that are not running currently supported operating system versions.
- Identify rooms/spaces containing computers and/or network jacks where the only protection is locking exterior building doors.
- Gather list of computers containing protected Personally Identifiable Information (PII).
- Identify in the comment column of the Excel spreadsheet any computers that could not be located or accessed
- Within 20 days, group leaders must accomplish the required actions with absent employees, recording when completed and transmit to Marion.

GROUP LEADERS

- **Deliver to Marion by 3:00 Today (2:00 if entered by hand)**
 - **Completed computer documentation spreadsheet**
 - **Answers to the “Group Leaders Stand Down Check List” questions – prefer simply editing the word document**