

# Practical Guide for a Cyber-Compliant Computer at NSTX

Rev 0 09AUG2006

P. Sichta

---

## 1.0 Introduction

### 1.1 A Cyber Security Perspective

The DOE has become pro-active regarding cyber security and has mandated all its entities, including PPPL, to follow requirements established by the Federal Information Security Management Act (FISMA) and the National Institute of Standards and Technology (NIST) to provide security for the information and information systems that support the operations and assets of the entity. The Office of Security and Safety Performance Assurance <http://www.ssa.doe.gov> is responsible for evaluating cyber security programs throughout the complex. PPPL is revising its Computer Policies and Procedures [http://sharepoint.pppl.gov/sites/CDPolicies\\_Procedures](http://sharepoint.pppl.gov/sites/CDPolicies_Procedures) to document and demonstrate compliance to the DOE.

The aforementioned website contain links to numerous documents that describe the requirements and user's responsibilities for owning and operating an Information Technology (IT) asset; this document is intended to be a concise, practical guide for NSTX researchers who want to connect a computer or networked device to PPPL's network for NSTX experimental operations.

The basic steps are shown below. These will be described further in subsequent sections.

- A. Contact the Computer Systems Division (CSD) for guidance.
- B. Register your computer.
- C. Work with the CSD to add your *Windows* PC to the *PPPL* domain. This is a **crucial step** for compliance with DOE's cyber security mandates.
- D. Request the CSD to assign your computer to a specific *Organizational Unit* (OU).
- E. Consider installing NetBackup software to your PC.

These efforts reflect yet another 'culture change' for the way we do business at PPPL. PPPL management and the DOE support and approve of PPPL's Computer Usage Policies and Procedures. These are operational requirements.

## **1.2 Examples of IT equipment**

- Windows PC
- Macintosh
- Linux/Solaris/Unix computer
- Network Device (netcam, 'scope, ACpwr\_Ctlr)
- X-terminal (this is a deprecated device)
- Thin Client
- Router/Switch

## **1.3 NSTX Collaborators**

NSTX Collaborators who bring IT assets to PPPL for NSTX research (e.g. computer hardware, operating system software, or application software which are the property of their home institution) need special consideration. Collaborators and their PPPL sponsor should contact the Computer Systems Division (CSD), e.g. [psichta@pppl.gov](mailto:psichta@pppl.gov) or [helpdesk@pppl.gov](mailto:helpdesk@pppl.gov) .

## **2.0 General Information**

### **2.1 Operating Systems: Windows, Macs, Unix**

*Windows* and Macintosh computers are centrally managed by the Computer Systems Division. In addition to maintaining a standard level of security, this central-management significantly reduces the 'total cost of ownership' (to the lab). Central-management includes installing anti-virus software, data backup software, and installing software updates (also referred to as patches) to the operating system and applications.

- New Windows and Macintosh systems will be subject to an anti-virus scan and other vulnerability scans before they are permitted onto a (Virtual Local Area Network (VLAN) other than the non-visitor VLAN.

### Windows versions:

- Windows XP SP2 is the preferred Windows OS.
  - Generally speaking, each newer version of the Windows OS requires more disk space and memory than its predecessor. You may need to upgrade your computer hardware if you want to upgrade to XP.
  - If considering an upgrade to XP, you need to verify that your application/control software will operate in the XP environment. Most Win2k software will work on XP, many Win98 applications will not.
- Windows 2000 is acceptable but less desirable than XP.
- Windows 98 and earlier are strongly discouraged since these systems are not maintained by Microsoft and critical security updates are not available. Use of such an OS on a PPPL network requires a review and approval by PPPL Management.

### Macintosh versions:

- MacOSX version 10.3.5 (Panther) or higher is recommended.
- The computer must have an Apple Remote Desktop (ARD) account.

### UNIX versions:

- Red Hat Enterprise Linux - Workstation is the standard Linux used at PPPL.
- Others may be used but support from the helpdesk/CSD will be less timely.

## **2.2 Operational Concerns**

Centralized management of your computer will affect the operation of your diagnostic or control system. Older computers will be affected more. Some of the factors for you to consider are shown below. Some will argue that central management will not affect system behavior in any way. The point is to proceed with caution.

- Disk Usage
  - Adding your computer to the PPPL domain will add about 1 GB of software to your primary hard drive.

- CPU, memory, network consumption

The central-management software on your PC will tax your system's resources. You should consider a hardware upgrade if your system performance margin is small.

  - o NetBackup

Veritas' (now part of Symantec) NetBackup software can optionally be installed on your system to provide automatic backup of your hard drive.

    - If your CPU is less than 2 GHz, this may *significantly* tax your system resources *while the backup is occurring*.
    - It is recommended that you request to be placed into the appropriate 'NSTX real time' NetBackup policy. These special policies will not perform backups during normal working hours (such as when NSTX is running).
    - A 100 Mb/s line is strongly encouraged. If not full backups may not complete during the night.
- Automated reboots

Some computer control and data acquisition systems should not be shutdown or restarted without active user control since this may adversely affect the operation of the diagnostic. Owners of such systems should ask the CSD to add their computers to a special class of OU called 'Experiments'.

If your computer is not in the *Experiments* OU then your system will be automatically rebooted after updates are installed. If your system is not in the *Experiments* OU then Microsoft updates will be automatically downloaded and installed at any time of day, but usually on the second Wednesday (pre-dawn hours) of each month.
- Startup of application software

When your computer is rebooted, whether automatically or manually, you must design the application/control software to automatically start **or** you must manually start the software. If the latter is the case, it is recommended that you write a *Startup Guide* so others can start your software after a reboot in the case of your absence.

- Centralized monitoring by NSTX Operations  
The CSD is currently developing software that can alert NSTX operators and cognizant personnel that a computer system is not running or NSTX shot data is not being acquired. This project is in early development. If you are interested in having your computer participate in this system please contact [psichta@pppl.gov](mailto:psichta@pppl.gov) .

## **2.3 System Design Considerations**

On a collaborative research device such as NSTX it is understood that there will be a variety of application programs, computing and data acquisition hardware, programming and scripting languages, and design-styles. DOE/PPPL's cyber security environment must be given consideration during the design and integration-planning phases.

The list below shows some of the considerations.

- how to store/access/transfer NSTX data to/from an NSTX PC (e.g. CIFS/SMB, sftp, scp, NFS, etc..).
- how to remotely access NSTX PCs, e.g., use Remote Desktop on Windows. Enterprise-VNC is secure, but (free) VNC is not. Timbuktu is secure.
- removal of unnecessary software (e.g., Microsoft Access).
- closing unneeded open network ports.
- removal of unnecessary local computer accounts.
- discourage the use of a PC that is for controlling an NSTX diagnostic, from being used as a personal desktop (i.e., for checking email, web browsing).
- Implement system access passwords consistent with PPPL Cyber Security Policy  
<http://user-support.pppl.gov/Guides/Password/Password.html>.  
Note that PPPL policy states that passwords must be changed every six months.

### 3.0 Detailed Guidance

Details concerning the basic steps mentioned earlier are described below.

Action	Description
Contact the Computer Division for Guidance	<p>The primary contact for PPPL Computing assistance is <a href="mailto:helpdesk@pppl.gov">helpdesk@pppl.gov</a> and for NSTX-specific computing issues is <a href="mailto:psichta@pppl.gov">psichta@pppl.gov</a> .</p> <p>To smooth the integration of your computer at NSTX provide the following information in an e-mail:</p> <ul style="list-style-type: none"> <li>• your name.</li> <li>• If a collaborator, your institution and your PPPL sponsor.</li> <li>• whether you currently have a PPPL computer account.</li> <li>• name of diagnostic/system.</li> <li>• type of equipment (e.g. PC, Mac, 'scope).</li> <li>• operating system .</li> <li>• application software.</li> <li>• planned location for computer.</li> </ul>
Register your computer	<p><b><u>Before Network Registration (on or about 9/15/2006):</u></b>  e-mail to <a href="mailto:helpdesk@pppl.gov">helpdesk@pppl.gov</a> and request a static IP address. NSTX diagnostics should request a .15 subnet assignment. You will also need the following network information to configure your computer's network interface's (card) tcp/ip settings.</p> <p><u>Default Gateway IP#</u>  For .15 subnet: 198.35.15.10</p> <p><u>Subnet Mask:</u> 255.255.255.0</p> <p><u>DNS IP#</u>  Primary: 192.55.106.5          Alternate: 192.55.106.24</p> <p><b><u>After Network Registration goes online (on or about 9/15/2006):</u></b>  Connect to the PPPL network, start your computer, and open a web browser. This action will bring up the <b>Network Registration</b> web page, which will contain further instructions.</p> <ul style="list-style-type: none"> <li>• The Net-Reg process will assign your computer an (DHCP) IP address.</li> <li>• NSTX diagnostics should request assignment to the '<b>Experimental Diagnostic Systems</b>' VLAN.</li> <li>• NSTX control systems should request an assignment to the '<b>Experimental Control Systems</b>' VLAN.</li> </ul>
Add your computer to the domain	<p>This must be performed by CSD personnel. Contact <a href="mailto:helpdesk@pppl.gov">helpdesk@pppl.gov</a> to schedule a time to escort the CSD personnel to your PC.</p>

Add your  
Windows PC to  
an  
Organizational  
Unit (OU).

This step must be performed by CSD personnel. However, you may request inclusion into a special class of OU for computers used for experiments. Entry into these OU must be approved by PPPL management

Some computer control and data acquisition systems should not be shutdown or restarted without active user control since this may adversely affect the operation of the diagnostic. Owners of such systems should ask the CSD to add their computers to a special class of OU called 'Experiments'. Two OU's have been designated for systems used for experimental operations, such as NSTX Diagnostics. Each OU has a further classification 'with software' which should be selected if you have any Microsoft Office applications installed.

**Experimental-Managed:** In this OU, the PC will be directed by the central-management software to automatically download and install Microsoft Windows 'updates' to your computer. The computer will be rebooted automatically.

- The updates usually occur during the pre-dawn hours on the second Wednesday of each month but could occur any day.
- The updates usually occur 'overnight' but could potentially happen at anytime.
- If an update is installed and the computer is automatically rebooted, be aware that the diagnostic-specific software may need to be manually started.
- A Windows update will rarely cause the computer or application programs to operate incorrectly. If you do suspect this to be the case, the CSD can assist in 'rolling back' or 'uninstalling' a Windows update.
- This OU provides the best cyber security environment.
- If there are Microsoft Office products on the PC then you should request the OU entitled **Experimental-Managed-with-software**.

**Experimental:** In this OU, the PC **will not** be directed to perform automatic actions, with the exception of placing a yellow 'shield' icon on your Windows taskbar. The shield icon will indicate that Windows Critical Updates are available and should be downloaded and installed by you at the earliest opportunity.

- You will receive an e-mail from the helpdesk alerting you to the fact that critical updates are available.
- **It is the user's responsibility to fulfill their computer-usage obligations and manually install the updates in a timely manner.**

Cont'd next page  
→

Cont'd next page →

<b>Action</b>	<b>Description</b>
<p>→ <i>Cont'd</i></p> <p>Add your Windows PC to an <i>Organizational Unit</i> (OU).</p>	<p>→ <i>Cont'd</i></p> <ul style="list-style-type: none"> <li>• The Computer Division has the ability to remotely examine the computer to see if it is up to date.</li> <li>• You may have to 'install' updates and reboot the PC several times to fully complete the installation process.</li> <li>• A Windows update will rarely cause your computer or application programs to operate incorrectly. If you do suspect this to be the case, the CSD can assist you in 'rolling back' or 'uninstalling' an update.</li> <li>• If there are Microsoft Office products on the PC then you should request the OU entitled <b>Experimental-with-software</b>.</li> </ul>
<p>Install an Apple Remote Desktop (ARD) account to your <b>Macintosh</b>.</p>	<p>This step must be performed by CSD personnel</p>
<p>Install <i>NetBackup</i> software on your computer and select a <i>Group Policy</i>.</p>	<p>To get periodic, automatic backups of your hard drives request the <a href="mailto:helpdesk@pppl.gov">helpdesk@pppl.gov</a> to install the NetBackup software and to add your computer to the group policy <b>NSTX_Real_Time-PC</b> (for Windows) or <b>NSTX_Real_Time</b> (for Unix) and ??? (for Macintosh). These policies will not attempt a backup during normal working hours (such as when NSTX is running).</p> <ul style="list-style-type: none"> <li>• The CSD can assist you with this installation and configuration.</li> </ul>