

<b>Subject:</b>  <b>Cyber Security Threat Response Procedure</b>	<b>Effective Date:</b>  May 7,2004	<b>Initiated by:</b>  Head, Engineering & Technical Infrastructure
	<b>Supersedes:</b>  NEW	<b>Approved:</b>  Director

**Applicability**

This Procedure is applicable for all real or perceived cyber threats at PPPL that have the potential to adversely impact laboratory operations.

**Introduction**

Computer Security at PPPL is an important issue. The number of machines world-wide which have been infected with viruses and worms is in the millions. On a daily basis the PPPL firewall drops unauthorized attempted connections. Our automated firewall protection and anti-virus protection on desktop machines as well as our patch management policy have provided a good first line of defense against incidents, however as new methodologies of attack are devised, PPPL may not have all of our resources automatically protected from these new threats. The purpose of this procedure is to define the steps that will be taken when a cyber attack that potentially poses an imminent threat to PPPL occurs. Roles and responsibilities for cyber security are defined in the Cyber Security Program Plan.

**Reference Documents**

Princeton Plasma Physics Laboratory Cyber Security Program Plan (CSPP), April 2003  
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, October 2001

**Procedure****Responsibility****Action**

- |                             |   |
|-----------------------------|---|
| CIO                         | 1. Approves CSPP which define cyber roles and responsibilities.   |
|                             | 2. Delegates responsibility for cyber response to the Cyber Security Line Manager.  |
| Cyber Security Line Manager | 3. Identifies or is notified of potential threat. Notification could come from observations, internal sources, DOE's CIAC, or other external sources. |
|                             | 4. Appoints Response Team Leader (usually Cyber Security Line Manager) and Response Team.   |
| Response Team               | 5. Classifies threat level as risk, based on perceived impact and likelihood of compromise (see Attachment 1. Risk Matrix)                            |
|                             | 6. Notifies CIAC, if risk level is medium or higher or if otherwise appropriate.  |

- |                             |  |
|-----------------------------|--|
|                             | 7. Determines if an initial and immediate “safing” is required, and if so, develops and implements initial response. (e.g. removing PPPL from all internet connectivity).  |
|                             | 8. If initial response is implemented, and response will have an adverse impact on PPPL operations, notifies CIO, and notifies Helpdesk and instructs Helpdesk in assisting staff.                                     |
| CIO                         | 9. Notifies Deputy Director and Head of Engineering and Technical Infrastructure.  |
| Helpdesk                    | 10. If initial response is implemented, and response will have an adverse impact on PPPL operations, notifies staff either through e-mail or through EVES system if e-mail is unavailable. Assists staff as necessary. |
| Response Team               | 11. Analyzes threat, by gathering information from CIAC and other sources as appropriate.  |
|                             | 12. Develops final technical solution  |
|                             | 13. Determines if final solution will require an unplanned expenditure of resources or if solution will significantly impact daily PPPL operation.   |
|                             | 14. If final solution will require an unplanned expenditure of resources or if solution will significantly impact daily PPPL operation, presents proposal to Cyber Security Review Board.                              |
| Cyber Security Review Board | 15. Reviews proposal, and makes recommendation of action to CIO  |
| CIO                         | 16. Approves (disapproves) recommendation and if significant additional funding is required, takes appropriate steps to obtain funding.  |
| Response Team               | 17. Implements final solution.   |
|                             | 18. Documents incident and notifies CIAC, if required (DOE reportable incident).   |
|                             | 19. Notifies Helpdesk, if changes to operations are required.  |
| Helpdesk                    | 20. Notifies staff, if significant impact to operations was implemented.   |

**Attachments**  
Risk Matrix

### Risk Assessment Matrix\*

Impact \ Likelihood	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
VERY LOW	White	White	White	White	White
LOW	White	White	Gray	Gray	Gray
MEDIUM	White	Gray	Gray	Black	Black
HIGH	White	Gray	Black	Black	Black
VERY HIGH	White	Gray	Black	Black	Black

White=Low Risk

Gray=Consider for attention

Black=Requires immediate attention

\* Note: Risk Assessment Matrix is adapted from NIST SP 800-30