

**Fermilab Computer Security Program**  
**Combined Self Assessment and Peer Review**  
**March 22-23, 2005**

**Report submitted May 27, 2005**

## EXECUTIVE SUMMARY

This document is the report of the combined self-assessment and peer review of the Fermilab computer security program, conducted in March 2005. These periodic reviews are mandated in the Fermilab Computer Security Program Plan (CSPP). The review committee was charged with assessing the effectiveness of the computer security program and providing feedback on the evolution of the CSPP.

The Fermilab computer security program has been effective. As measured against the contract metric outlined in the CSPP – that no scientific opportunity has been lost as a result of a computer security incident – the program has succeeded. Further, the program is active and evolving in its attempts to secure the Fermilab computing systems. The committee has several recommendations for improvement of the program, but finds it to be sound and well considered.

Fermilab strives to maintain an open computing model to allow the greatest flexibility and ease of innovation in fulfilling its scientific mission. To maintain a secure environment within this model has required Fermilab to develop a culture in which computer security is important at all levels, from the user to the managers of large critical systems. Awareness, training, configuration management, system registration and vulnerability testing are all components of this methodology. Fermilab has been successful in maintaining the balance between these restrictions and the desire to remain as open as possible. The review committee endorses this philosophy, and believes that it can be both maintained with appropriate care and justified to oversight agencies with appropriate documentation.

Fermilab is embarking on a rework of the CSPP, to bring it up to date with current oversight requirements and practices and to incorporate the evolving needs of the grid environment. The committee has noted the importance of evaluating the changing threat environment in the preparation of the risk assessment component of the CSPP. The committee also feels that the CSPP is of high priority, and encourages the laboratory to devote sufficient resources for a timely completion. The committee notes the extensive similarities in requirements and procedures for computer security with other laboratories, and comments that development of the CSPP would benefit from the lessons learned elsewhere.

The computer security program at Fermilab is sound. The open environment has been successfully managed. The personnel involved in the computer security effort, not only the dedicated computer security team but also those drawn from elsewhere in the Computing Division and the laboratory, are dedicated to maintaining a productive, secure environment.

## TABLE OF CONTENTS

<b>Executive Summary .....</b>	<b>2</b>
<b>1 Introduction .....</b>	<b>4</b>
<b>2 Responses to recommendations of prior review .....</b>	<b>5</b>
<b>3 Analysis of management structure.....</b>	<b>6</b>
<b>4 Computer Security policies.....</b>	<b>7</b>
<b>5 Computer Security implementation and enforcement.....</b>	<b>8</b>
<b>6 Analysis and assessment.....</b>	<b>10</b>
<b>7 Recommendations.....</b>	<b>11</b>
<b>8 Conclusions.....</b>	<b>12</b>
<b>Appendices</b>	
<b>A. Attendees .....</b>	<b>13</b>
<b>B. Review Agenda.....</b>	<b>14</b>

# 1. Introduction

## *Review summary*

The Fermilab Computer Security Program Plan (CSPP) calls for a periodic peer review and self-assessment of the cyber security program. This is the report of the review of March 22-23, 2005. A list of reviewers is in Appendix A. The agenda for the review is attached in Appendix B.

## *Charge to Reviewers*

The review committee was asked to assess the effectiveness of the Fermilab computer security program. The contract metric, used as the ultimate measurement of program effectiveness, is taken as the amount of scientific opportunity lost as a result of a computer security incident. The committee was also asked to provide feedback and advice on the evolution of the computer security program and the creation of a new CSPP for Fermilab.

## *Questions inherent in the charge*

There are several issues inherent in the charge:

- What is the cost of the program versus the cost of potential disruptions?
- What is the potential cost of remaining vulnerabilities?
- Is the Fermilab program evolving in the right direction?

The first two of these require a detailed cost-benefit analysis. The limitations of the review did not allow the committee to develop an independent analysis, nor even to fully explore any analysis by the Fermilab Computer Security team. We will, however, note the importance of such analysis in the development of the future program.

Similarly, the committee was able to explore some details of the evolution of the Fermilab computer security program, but did not have the time to completely explore all avenues. Most of our comments will be aimed at specific items in the plan, and we'll have to settle for a few general statements about the direction of the program.

The committee also saw it important to address and comment upon a principle of the Fermilab policy – the open, self-administered scientific computing environment.

## *Organization of the report*

The report is organized into the following sections:

- Responses to recommendations of prior review
- Analysis of management structure
- Computer Security policies
- Computer Security implementation and enforcement
- Analysis and assessment
- Recommendations
- Conclusions

## 2. Responses to recommendations of prior review

In the report of the April 22-23, 2003 review the following recommendations were called out:

***“...the committee recommends the implementation of more formal training for system administrators, and larger participation of the line management for incident response.”***

This committee's impression is that the system administrator training is proceeding well. We believe that continued attention is warranted to increasing the awareness and involvement of line management to system administrator responsibilities. This seems to be particularly necessary in the management of smaller, more independent systems throughout the laboratory.

***“The committee recommends reviewing the access strategy to the Beams critical system from the Beams general LAN.”***

This committee perceives the further review of the access strategy to have been completed, and foresees no additional exceptional attention necessary beyond the level normally required for a critical system.

***“The committee recommends that this practice [periodic review of router ACLs] continue for both DØ and CDF critical systems on a regular basis and this practice should be incorporated into the critical system plans.”***

A periodic review of critical system router ACLs has not been formalized as a procedure set forth in the critical system plans. However, the ACLs are examined at each update, and the critical system coordinators are aware of the ACL contents. We expect this issue to be addressed in the lab's new CSPP, taking into account the review mechanism that has naturally evolved as the model for the critical system policy.

***For the Business Systems, “The committee recommends creating a remote access policy addressing access to PeopleSoft and Oracle Financials.”***

This policy has been successfully established.

***In the area of grid security, “we strongly recommend the group to take and/or strengthen a/their role in related efforts carried out by the GGF (in standardization), and the Grid Projects, in particular the LHC Computing Grid Project.”***

We believe that the Fermilab computer security team has shown a high degree of awareness of the necessity for involvement in the grid security effort. This is a substantial and continuing effort, to which we believe adequate attention is being given.

### **3. Analysis of management structure**

#### ***Methodology***

The approach used by Fermilab is aptly described as *Integrated Computer Security*, in which all levels of users and management are responsible for computer security. This is modeled upon the *Integrated Safety Management* system that has been effective at Fermilab. This is seen as a method that can be employed to keep awareness high at all levels. One consequence of this method is an environment under which a broadly constituted FCIRT team can be formed and supported. It also aids, by enabling collective input from all levels, in defining the appropriate balance among policy, prevention, and response. The committee believes this style of management is consistent with both the Fermilab cultural style and the mission of the lab, and endorses it in principle and in action.

#### ***Priorities***

There is an ambitious program to add extended functionality to the effort to monitor the Fermilab computer systems. These efforts and future plans may exceed the safeguards and security budget. The committee believes that the risk assessment and self-assessment processes should drive the prioritization of activities.

#### ***Effort***

Placing the responsibility for security on system administrators is an important aspect of an integrated posture, but places an additional burden upon departmental resources. Management may complain of insufficient resources to implement security policies, and that such activities can interfere with the “primary job” of their staff. There is an additional difficulty in assessing the time and money spent on computer security, particularly as it is seen as having an ever-enlarging burden that creeps into every operational activity. Fermilab needs to emphasize the culture change necessary to incorporate computer security in much the same way as safety – that such a change is not at the expense of the mission but to the protection of the mission.

#### ***Comparisons to other Laboratories***

Fermilab’s existing computer security program appears to be effective, based on the low level of serious incidents in the last three years. There are, however, a number and variety of lesser impact incidents that could be categorized and enumerated. The collective experience of the other national open science laboratories can be used as a performance benchmark.

## 4. Computer Security policies

### *Risk Assessment*

The proposed rework of the risk assessment, as a part of the CSPP rewrite, is a bottom-up analysis where individual nodes can be assessed as being members of larger, well-understood, classes of systems. The committee points out that the nature of the threat is evolving, with a much greater presence of skilled hacker activities becoming evident. There is also a concern that significant exposure may come from nodes that are not members of the well-managed classes – and hence may not be evaluated in light of these more serious threats.

A reevaluation of the threats and vulnerabilities prior to embarking on the risk assessment effort would ensure that the best available information was used. This information should be propagated to all levels involved in the development of individual risk assessments.

As there is a similar threat environment, Fermilab's risk assessment should be similar to that of other labs. Some effort should be expended to compare the risk assessment process and results to that of other open science labs.

### *Adherence to External Requirements*

Much of the burden of external reporting placed upon the computer security program is in the collection and management of the appropriate information. A consistent mechanism for the recording of internal computer security activity should lead to an easier path for external reporting.

### *CSPP Rewrite*

The current version of the lab's Computer Security Program Plan (CSPP) has been effective in guiding the efforts to date. Parts of the document are now out of date, even with respect to internal operations. More importantly, the committee feels the CSPP cannot survive in the face of increasing documentation requirements. The Fermilab Computer Security team has appropriately chosen to embark upon a rewrite of the CSPP.

The rewrite appears to have a high priority. The committee endorses that priority, but has a concern that inadequate resources are being applied to the effort. During open discussion it was noted that LBL's rewrite of their CSPP required 1.5 FTEs of concentrated effort over 6 months, and that the document grew from 20 to ~150 pages. The revised Fermilab CSPP is due 01-Jan-2006, roughly 9 months from this review. It is not obvious that sufficient resources exist within the Computer Security team to successfully complete the rewrite during this time frame, given the level of ongoing work performed by the group and the number of open questions associated with the requirements of the new CSPP.

### *Perimeter Control*

The current Fermilab policy allows for a *default allow* open perimeter, with access statically restricted for some ports/addresses and dynamically restricted to specific addresses by an auto-blocker mechanism. The philosophy of perimeter protection "as a last resort" is thought to aid in the avoidance of "deep fried security" – the policies which produce a hard shell but allow a soft interior.

The Fermilab wireless network is treated identically to the wired networks. The committee notes that this is logical, but points out that the absence of additional perimeter protection for the wireless networks may require a more detailed risk analysis to show an acceptable level of residual risk.

The topic of Perimeter Protection is also addressed in a following section.

## **5. Computer Security implementation and enforcement**

### ***Methodology***

The current computer security defense is “vulnerability oriented”. The program needs to strengthen its “attack oriented” defenses. This is alternatively stated as noting that a lot of effort is spent to find and seal vulnerabilities, but comparatively little effort is spent on actively looking for attacks. The Fermilab computer security team should include in its risk evaluation process an examination of the mechanisms of recent attacks. This might be implemented as an extension to the current mining of netflow data records.

### ***Networks***

Fermilab does an excellent job of recognizing the appearance of new systems on the network. Requiring new systems to go through a registration process is a good feature.

### ***Perimeter Protection***

Fermilab’s computer security policy has always assumed a mostly-open perimeter, with only Major Applications / Critical Systems employing more restrictive perimeters. This policy has been successful for the lab, requiring only few and infrequent restrictions on particularly vulnerable protocols or ports. The committee also considered the benefits of restricting outbound traffic. There are protocols that may be possible to block with no adverse effect, for example a block of outgoing Windows Networking Protocols could further limit the lab’s external exposure from compromised local machines. Other restrictions, for example limiting outgoing SMTP to registered mail servers, are worth consideration.

The committee comments that there appears to be value in a more rigorous auditing of perimeter rules at the site boundary and the Major Application boundaries. For example, periodic rechecks of firewall rules / ACLs, and/or scheduled nmap scans could identify unintentional deviations from the baseline.

### ***Zoning***

Fermilab’s internal network currently consists of Major Application areas and a General Security area. It is proposed to further divide the general security area into protected and open zones. Fermilab is considering whether this subdivision is consistent with and supportive of its computer security plan. The committee endorses this proposal.

### ***Wireless (and Dial-in) Networks***

The frequency at which poorly managed machines appear on the network is much higher in the wireless realm, where short-term visitors are most apt to connect. Fermilab attempts to mitigate this vulnerability by requiring node registration and performing an initial vulnerability scan of attaching systems. Despite these precautions, it is worth considering whether additional steps are appropriate for the wireless networks. The committee notes the following:

- A procedure to locate rogue wireless access points should be in place.
- The wireless program needs to be reconciled with the DOE PCSP.

### ***Training***

Fermilab should be commended for their efforts in raising cyber security awareness through their cyber security awareness day recently. Attendance at the training program is well tracked. The committee comments that it would be useful to evolve the content as threats change in an effort to maximize relevance and value to the community. The training has begun to help explain the need

and purpose behind cyber security to the general lab population, but a continual and consistent program is needed.

### ***Virus Protection***

Many compromises involve viruses. The lab may want to examine whether a centrally licensed and distributed anti-virus package could reduce the exposure to this threat.

### ***Configuration Management***

Fermilab should be commended for their installation base of Fermi Linux and the cross-realm Kerberos trust mechanism software. The lab may want to investigate whether it would be possible to impose a more standard Windows configuration on lab-owned PCs, and whether such a requirement would mitigate any perceived vulnerabilities from user-configured systems.

### ***Major Applications / Critical Systems***

The requirements for reviews of Critical System plans are to be addressed in conjunction with the CSPP rewrite. The committee suggests that more frequent lightweight reviews be considered in the future.

### ***Incident Response***

The incident response mechanism at Fermilab is very good. The technical people involved are very skilled. There is a minor concern that the mechanism can be slowed, as responsibility for certain corners of the network is not clearly defined. There is also a concern that the “line management” interface to non-employee users may not be effective.

### ***Vulnerability Scanning***

Fermilab should be commended for their procedure of scanning of new nodes. This helps ensure that machines are checked prior to accessing the network. The committee notes that host based firewalls are a simple way to evade the check. The committee encourages the Computer Security team to find a way to build on and extend the vulnerability scanning to include in-depth scans of critical systems during maintenance periods.

## **6. Analysis and assessment**

### ***Metrics***

The contract metric for the Fermilab computer security program is taken as the amount of scientific opportunity lost as a result of a computer security incident. Data was presented in this review that could form the basis of internal performance metrics. The committee believes that these internal metrics are useful indicators of the health of the computer security program, and can provide leading indicators of situations that might have impact upon the contract metric.

There also exist no good metrics to evaluate the effects that computer security is having on science. There is a value to computer security in that costs are avoided because of the computer security efforts. There is a cost to the computer security effort, not only of the budgeted amount and direct expenditure of manpower, but also of the potential interference with the scientific process. In the new CSPP, the committee would like to see an assessment of these competing costs.

### ***Process***

The feedback from incidents to policy and implementation clearly takes place, but is not well recorded. A procedure should be developed to make a historical record of policy and implementation changes undertaken by the Computer Security team, with reference to the motivating factors and/or incidents.

The committee additionally suggests that a wider range of participants contribute to the analysis process. A reconstituted Computer Security Working Group (CSWG) would seem the appropriate body to participate.

## 7. Recommendations

In this section the committee reiterates several previous comments as formal recommendations for further action by the Fermilab Computer Security team.

1. *The Computer Security team should reevaluate the threat list prior to embarking upon the risk assessment effort. All levels of system managers should be educated in the threat list, and should be instructed to apply its contents in the development of their individual risk assessments.*
2. *The CSPP update is of high priority, and should be assigned sufficient resources for a timely completion. The experience of other laboratories should be utilized in creating the CSPP.*
3. *Fermilab should define and develop internal metrics for use in determining the health of the program. The choice of metrics should be guided by the risk assessment.*
4. *Fermilab should evaluate the expansion of their intrusion detection systems and the value of routine checks of their perimeter protection.*
5. *The lab should consider the purchase of site-licensed anti-virus software.*
6. *Fermilab should consider implementing more intensive system scans on a periodic or scheduled basis. Critical system scanning should be emphasized.*

## 8. Conclusions

The Fermilab computer security program is effective. The program has clearly met the contract metric performance goal of no lost scientific opportunity as a result of computer security incidents. The system is capable of collecting and reporting information on vulnerabilities and lesser incidents, and this capability is evolving and improving. The incidence response mechanism is excellent.

The magnitude, scope, effort, and cost of the program are in line with the requirements of the computer security plan. The effort appears adequate to pursue planned projects, maintain a high degree of vigilance, and we believe to also implement this committee's recommendations. One possible exception is in the mustering of effort for the timely completion of the new CSPP, which the committee believes will require additional effort. Risk assessment and self-assessment processes should drive the prioritization of efforts.

There are several notable and laudable achievements since the last review. The effort put into Kerberos by the Fermilab community – computer security administration, system managers, and users – is paying off. The single point of authentication works well, giving good central control over authentication. This is something with which other labs are struggling. The achievements in recognizing, scanning, and registering new and visiting systems have also greatly reduced the exposure to introduced vulnerabilities. The auto-blocking mechanism of either internal or external systems indicating possible problems is an effective way to mitigate risks.

There has been an exceptional effort to incorporate computer security into the lab culture. This includes awareness efforts, cross-organization involvement in incident response, the degree of authority given by Divisions to the GCSCs, and the existence of the CSWG. The committee believes that this Integrated Computer Security methodology is consistent with the Fermilab scientific mission, and endorses its principles.

The committee thanks the members and management of the Fermilab Computer Security program for the excellent presentations and background material.

## APPENDICES

### **A. Attendees**

#### ***Review Committee:***

Bill Boroski, Fermilab, PPD Technical Centers, SDSS  
David Carlson, Fermilab, Business Services Section Head  
Bob Cowles, SLAC  
Matt Crawford, Fermilab, past Fermi Computer Security Program Manager  
Stu Fuess, Fermilab, DØ Major Application Coordinator (Chair)  
Bob Lukens, Jefferson National Laboratory  
Jim Rothfuss, Lawrence Berkeley National Laboratory  
Mike Skwarek, Argonne National Laboratory  
Dan Stenman, Fermilab, Accelerator Division, Controls Department

#### ***Speakers:***

Phil Demar, Fermilab, Head of Networking Group  
Mike Diesburg, Fermilab, Fermi Computer Incident Response Team (FCIRT) Head  
Irwin Gaines, Fermilab, Deputy FCSC for Training  
Mark Kaletka, Fermilab, Deputy FCIRT Head, CD Department Head  
Joe Klemencic, Fermilab, Fermi Computer Security Coordinator (FCSC) \*  
Mark Leininger, Fermilab, Fermi Computer Security Program Manager \*\*  
Frank Nagy, Fermilab \*  
Randy Reitz, Fermilab \*  
Dane Skow, Fermilab, Deputy Computer Security Executive  
Vicky White, Fermilab, Computer Security Executive, Computing Division Head

#### ***Others in attendance:***

Tom Ackenhusen, Fermilab, BSS Major Application Coordinator  
Jon Cooper, Fermi Area Office, DOE  
Donna Lamore, Fermilab, Networking Group  
Arthur Lee, Fermilab, BSS General Computer Security Coordinator  
Ron Lutha, Fermi Area Office, DOE  
Don Petravick, Fermilab, CD Department Head  
Bob Tschirhart, Fermilab, Deputy CD Division Head  
Mike Witherell, Fermilab, Laboratory Director

\* Denotes member (\*\* Leader) of Fermilab Computer Security Team

## B. Review Agenda

### FERMILAB COMPUTER SECURITY PROGRAM COMBINED SELF ASSESSMENT AND PEER REVIEW AGENDA March 22 – 23, 2005

#### *Tuesday*

8:00 AM	Executive Session with FNAL Management	
8:30	Welcome	Directorate
8:45	Introduction and Charge to Committee	Vicky White
9:15	Results of 2003 Computer Security Peer Review	Dane Skow
9:30	Overview of Computer Security Program	Mark Leininger
10:00	Break	
10:15	Introduction of new CSPP	Mark Leininger
11:00	Overview: Security Controls	Joe Klemencic
11:20	Training	Irwin Gaines
11:30	Strong Authentication	Frank Nagy
11:40	Major Applications (Critical Systems)	Joe Klemencic
12:00	Working Lunch	
12:15	Network	Phil Demar
12:45	Scanning	Randy Reitz
1:00	Incident Response	Mike Diesburg
1:30	Configuration Management	Mark Kaletka
2:00	Break	
2:15	Self Assessment	Mark Leininger
3:00	Evolution to new CSPP	Mark Leininger
	General Computing Enclave	Mark Leininger
3:30	Network Configuration	Phil Demar
3:40	Open Science Enclave	Dane Skow
4:00	Open Discussion with Committee	
5:00	Committee Executive Session (if desired)	
6:30	Social gathering	Chez Leon
7:00	Dinner (Committee and Speakers)	Chez Leon

#### *Wednesday*

8:30 AM	<b>Committee Executive Session to write report</b> (speakers available for questions)	
11:30	Closeout and Delivery of Report	