



# MCS Computer Security and Operations

Steve Hahn  
Monitoring and  
Control Systems  
10/01/2001

- CDF Computer Security Operational Readiness Clearance (ORC)
  - For all “critical” systems which impact data-taking: the online systems (including MCS) are “critical” systems
  - Must be completed by **November 14!**



# MCS Computer Security and Operations

Steve Hahn  
Monitoring and  
Control Systems  
10/01/2001

- Main points - from summary by J.J. Schmidt and Jim Patrick
  - Protect against threats and vulnerabilities
    - Password sniffing (Kerberos)
    - OS/applications security holes (patches; anti-virus software)
    - User behavior (education)
    - Networks open to DOS attacks (disconnect online)
    - Portable media, email enclosure, web accesses (remove applications)
    - Physical security



# MCS Computer Security and Operations

Steve Hahn  
Monitoring and  
Control Systems  
10/01/2001

- Disaster recovery
  - Security problem detected, isolated, removed, repaired
  - Regular backups with quick restoration
  - Hardware spares, redundant systems, maintenance contracts
- CDF Implementation
  - User account restricted, all online access via Kerberos from outside
  - Online subnets (lower half) 236, 237 only accessible from ACL (access control list) from outside; can be disconnected from rest of network by CD and is meant to continue working
  - Disaster recovery must be tested and documented



# MCS Computer Security and Operations

Steve Hahn  
Monitoring and  
Control Systems  
10/01/2001

- Currently, we are investigating virus infection on iFIX machines; Mark Knapp and Bill Noe are finishing checking all nodes. Only these nodes had virus:
  - CDFS1
  - CDFS3
  - VNODE-1
  - VNODE-2
- All nodes are being installed with Norton Anti-Virus client; CDFserver1 is server of new virus signatures. Requires some time on each machine. ✓
- Still in negotiations with CD. If they are not satisfied machine has not been compromised (I.e., virus has been activated), they will require us to wipe hard disk and reinstall from scratch. ✗



# MCS Computer Security and Operations

Steve Hahn  
Monitoring and  
Control Systems  
10/01/2001

## ➤ Consequences to MCS:

- Any computer security issue should be immediately reported to operations manager, system manager (Jim Patrick), and mailed to **computer-security@fnal.gov**.
- May have to restrict MCS machines to as few ports as possible
  - **No e-mail**
  - **No web server**
- Control of machines may have to be very tight; only Mark Knapp installs new software?
- Access control lists (ACLs) of outside accesses (especially without Kerberos) into online subnets may have to be shortened as much as possible
- VNC access should only be through Kerberos or secure SSH tunneling



# MCS Computer Security and Operations

Steve Hahn  
Monitoring and  
Control Systems  
10/01/2001

- Action items for Friday meeting with CD:
  - Verify CDF MCS web server (cdf-fs2) on lower half of subnet 236 is secure; change port number from 80 (http://cdf-fs2.fnal.gov:3000/fixpics) ✓
  - Test VNC with SSH tunneling (is Luciana already using this?) ✓?
- Schedule proposed by Dane Skow for CDF implementation:
  - Oct 10 - First disconnect test (Oct 16 ✓ x)
  - Oct 17 - First disaster review and test proposal
  - Nov 1 - Disconnect tests successful
  - Nov 7 - All tests (disconnect and disaster) done
  - Nov 14 - ORC signed



# MCS Computer Security and Operations

Steve Hahn  
Monitoring and  
Control Systems  
10/01/2001

- Long-term operations of MCS group:
  - Security - get CORC signed!
  - Expansion - during shutdown and for Run IIB
  - Robustness, Recovery - redundant hard disks? Computer hot spares?
  - Manpower - MOU commitments, CD help?



# MCS Computer Security and Operations

Steve Hahn  
Monitoring and  
Control Systems  
10/01/2001

- Disconnect test in progress now (waited till Oct. 16 for Frank Chlebana)
  - Problems with DNS “failover” for L3 nodes
  - Problems with some web pages
  - Problems with starting new web browser and displaying online info
  - Problems with MCS NT nodes if rebooted due to NT domain “failover” not working correctly:

Logon message -  
A domain controller for your domain could not be contacted. You have been logged on using cached account information.

Changes to your profile since you last logged on may not be available

iFIX INTERNAL ERROR -  
Alarm Area Database (AAD) file not found in configured path  
D:\Dynamics\AADBACK.EXE

Validating Path Configuration -  
The Pic\_Path S:\\WDMACS\PIC\CDFMACS is invalid.