

“Town Hall” Meeting DOE Exascale Computing

May 18, 2007

Greg Hinkel
Computer and Network Security
Oak Ridge National Laboratory

Areas for Improvement

- **Training and Communication**
- **Incident Response and Communication**
- **Intrusion Prevention and Detection**

Training and Communication

- **Users - proper use of tools, file sharing**
- **Admins - monitoring, access controls**
- **Security Analyst - monitoring, network controls, data/log correlation**
- **Management - get input from "experts"**
- **Language barriers**
- **Communication with other sites**

Incident Response and Communication

- **TeraGrid has good model**
 - (At least) weekly communication
 - Encrypting electronic communication
 - “Tightly” controlled membership
 - Quick notification and response
 - Info sharing
 - Incident checklist
 - Someone in charge (with sense)
- **Keep management at bay**
- **Common procedures**

Intrusion Prevention/Detection

- **More anomaly detection**
- **Less “signature” based**
- **Merge, parse, analyze various logs**
- **Unusual “normal” traffic (e.g. DNS, NTP)**
- **Profile user activity and system traffic**
- **Separation of SC from desktop and infrastructure**
- **Centralize remote access**