Status of phase 2 encryption initiative

Validation of need-to-know decisions

Reducing number of classified systems and system administrators

Identification of sensitive/high value information types

Media-less implementation / encloures

Recommendations and near-term strategies for

Accelerate near term enhancements

Opportunity to talk about issues, options, and alternatives
Meeting Objectives

- Roles and responsibilities
- Cost benefit analyses
- Consider impact of multi-plant TPSOS
- Develop cost estimates
- Recommended schedule (quick/short-term, long-term)
- Policy impacts
- Applicability (labs/plants/both?)
- Expected outcome (risk assessment)
- Recommended courses of action
- Identity short/long-term issues (must integrate with long term)
Recommendation for media-less systems

- Identity new or modified policies
- Identity activities to start, continue, or enhance
- Explain what has been accomplished
Develop Report and briefing on accomplishments since April 1999

Explanations of Accomplishments

Plants

Labs

Policy

Direct Report to Group by 9/18

Input due to DP-11 by 9/11

NTK accomplishments needed to be communicated better
Activities to Start/Continue/Enhance

- Automated configuration management
- Automated log analysis
- Off host log analysis
- Intrusion detection
- **Review number of systems approved for classified processing**
  - Current information to DP-11 by 9/15
  - Complete review within next 60 days
- Review accounts on multi-user systems
  - Review results to DP-11 within next 60 days
- Red team review
Credential review (Yellow)
Automated intrusion detection response
Honey pots
Modern detection
Port locking
Switched networks (Yellow)
Anomalous use detection

Start/Continue/Enhance
Activities to

ICSI
Stop scanning of archives

Approach

Experience indicates minimal results for expended resources

Archive scanning

Provide capability to conduct selected email scanning

Leverage CN MAC

Approach (classified in common email)

Counterintelligence doing traffic analysis (looking for

Policy that says we don't think this is cost effective

Policy that will preserve ability to monitor email

Options

Email scanning

Policies
• Media-less Workstations
  - Default workstation configuration for classified data processing is media-less
    Exceptions must be documented
    Exceptions must be approved by Designated Approving Authority
    Policy must be part of defense-in-depth solution

• Laptops for Classified Data Processing
  - Default - Classified data processing on laptops is NOT allowed
    Exceptions must be documented
    Exceptions must be approved by Designated Approving Authority
    DP work with labs and plants to develop migration plan
Implement for highest priority information types first.

Completion date to DP-11 by 9/11

Sites report number of systems, estimated costs, and target dates.

Develop plan for migration to new policy.

Implement as funding is made available.

Draft complete by 9/15

DP-11 convene working group.

Develop standard approach or common operating environment.

Prioritize assets.

Recommendation.

Steps to implement media-less workstation.

Media-Less Workstation

CISSI
CNIS
SNIS
Other sigmas

Priority 3 Information Assets

Priority 2 Information Assets

Weapon test data collection

Top Secret data

Special Access Programs

Special Access Program

SIGMA I 5 data

Priority 1 Information Assets

(continued)
They are classified,
some sites are not aware of numerous incidents because
Need to be able to communicate and share information;
Classified via FIS
Malicious codes
Separation of roles
PKI
Standards for system administrator certification
Hiring more system administrators

ICSI Planning and design
Long-term issues for
Implement funded recommendations

Fund decision

Presentation of recommendations to DP-1

Group review of documentation

Recommendations, policies

Complete documentation of accomplishments

Next Step