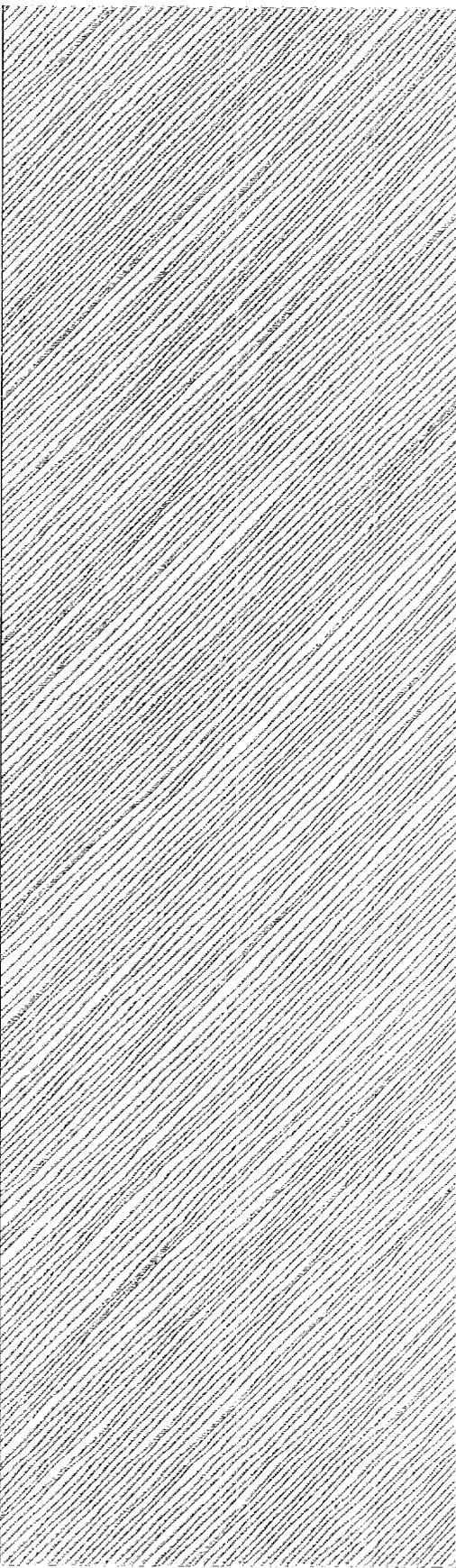


LA-11614-MS

LA-11614-MS

C.3



*Department of Energy
Center For Computer Security*

*Lessons Learned
in the DOE Computer Security
Enhancement Review Program*

AUG 26 1995



Los Alamos

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

Prepared by Sharon Hurdle, Group N-4

An Affirmative Action/Equal Opportunity Employer

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

*Department of Energy
Center For Computer Security*

*Lessons Learned
in the DOE Computer Security
Enhancement Review Program*

W. J. Hunteman



EXECUTIVE SUMMARY

During the last four years, the Department of Energy (DOE) has made the most detailed and extensive computer security self-evaluation of any U.S. Government organization. The breadth and depth of the examination have revealed some problems. Few of the problems are major; most are procedural, some administrative, a few technical, and almost none systemic. The DOE facilities have received a thorough and systematic examination by some of the most computer-security-knowledgeable people in the United States. The examinations were conducted in a nonadversarial manner and at minimal cost to the government.

The reviews were conducted as part of the DOE Center for Computer Security (CCS) Computer Security Enhancement Review (CSER) program. Almost all of the computer security problems found during the reviews involved some form of lack of management or user awareness. Problems of this type do not readily admit to technical solutions. Improving management and user knowledge of the problems and providing access to expert information will help correct these problems.

DOE Order 5637.1 has established policies for most of the computer security issues identified in this report. DOE and DOE contractor sites need additional information, e.g., guides, that outline policy implementation. Development of the guides will provide DOE contractors with suggested approaches for efficient implementation of DOE policies. These guides should contain suggested methods to implement the policy without becoming part of the policy documentation. Maintaining independent guides will allow rapid updating to reflect changes in technology and computer security policy implementation.

This report is not an indictment of the DOE Classified Computer Security Program or any DOE site. The proper interpretation of these findings is that the DOE Classified Computer Security Program is very strong. The largest problems confronting the program are awareness at all levels and the dissemination of computer security information and solutions.

The program has been, and continues to be, a success!

CONTENTS

ABSTRACT	1
I. INTRODUCTION	1
II. INFORMATION SENSITIVITY	1
III. COMPUTER SECURITY ENHANCEMENT REVIEW PROGRAM	2
A. Overview of the CSER Program	2
B. CSER Process	2
C. CSER Benefits	3
D. CSERs and Evolution of the Classified Computer Security Program	3
IV. FINDINGS	3
A. Management Procedures	4
1. Threat Guidance	4
2. Risk Management	6
3. Computer Security Planning	7
4. Incident Program	7
5. Local Inspection/Review Program	7
6. Contingency Planning	8
7. Configuration Management	9
8. Waste, Fraud, and Abuse Monitoring	10
9. Coordination of Facility Changes	10
10. General Management Awareness	11
11. Computer Security Reviews of ADP Procurements	12
B. Certification and Accreditation	12
1. ADP Security Plan Development and Maintenance	12
2. System Security Testing Guide	13
3. Certification and Accreditation Procedures	13
C. Personnel Security	15
1. Uncleared People Developing/Maintaining Software	15
D. Physical Security	15
1. Escort Procedures and Training	15
2. Access List Maintenance	16
3. Unattended Systems	17
4. Emergency Controls and Equipment	17
5. Media Protection	18
E. Telecommunications Security	19
1. Telephones Too Close to Computing Equipment	19
2. Uncontrolled Modems	20
3. Red/Black Separation	21

CONTENTS (cont)

F.	Hardware and Software Security	21
	1. Multi-level Systems	21
	2. Activation of System Security Features	22
	3. Security Evaluation Techniques	23
	4. Technical Computer Security Knowledge	23
	5. Networks	24
	6. Audit Trails and Audit Trail Analysis Tools	24
G.	Administrative Security	25
	1. Education/Awareness Program	25
	2. User Guides	26
	3. Authentication	26
	4. Remote Diagnostics	27
	5. ADP System Inventory	27

**LESSONS LEARNED IN THE DOE
COMPUTER SECURITY ENHANCEMENT REVIEW PROGRAM**

by

W. J. Hunteman

ABSTRACT

During the last 4 years, DOE has made the most detailed and extensive computer security self-evaluation of any U.S. government organization. The breadth and depth of the examination have revealed some problems. Few of the problems are major; most are procedural, some administrative, a few technical, and almost none systemic. This report documents the lessons learned from one part of the evaluation process.

I. INTRODUCTION

This report collects and documents some of the lessons learned in the DOE Center for Computer Security (CCS) program of Computer Security Enhancement Review (CSER). The CSER program, described in Section III, supports the DOE Classified Computer Security Program. The CSER program provides nonadversarial assistance to any DOE site that processes classified information. Although the CSER team will review unclassified computing systems on request, this report does not reflect any specific information collected about unclassified systems.

Over the last 4-1/2 years, the CSER program has included visits to every DOE contractor site except Mound in Ohio. The findings listed in this document are a distillation of all the CSERs conducted by the CCS. These findings are presented to assist in improving the DOE Classified Computer Security Program. Section IV contains the generic findings or issues identified in the CSER process.

II. INFORMATION SENSITIVITY

The "generic lessons" in this report involve computer security problems usually found at more than one site. Typically, any specific automatic data processing (ADP) system at a site will contain only a small number, if any, of these problems. This report contains only the findings common to multiple sites. All other findings are site-specific and are being corrected by the site computer security organization.

This report does not include technical details of findings that deal with specific sites or specific computing systems. Including these details would have violated the basic ground rules of the CSER program and good Operational Security (OPSEC) practices.

III. COMPUTER SECURITY ENHANCEMENT REVIEW PROGRAM

A. Overview of the CSER Program

The CSER program is an independent part of a comprehensive DOE computer security self-evaluation. The entire DOE process includes

- inspection and evaluation (I&E) activities managed by the DOE Office of Security Evaluations,
- annual reviews of every DOE or DOE contractor computer security program by a cognizant Computer Security Operations Manager (CSOM),
- triennial review of each ADP system by the CSOM, and
- CSERs conducted by the CCS.

The initial CSER activities were oriented toward assisting the site in preparing for a formal I&E inspection. Later CSERs shifted to reviewing site programs for compliance with the new DOE Order 5637.1 on classified computer security. All of the DOE and DOE contractor sites have active efforts to implement the new order. This effort is part of overall efforts to improve their computer security programs. The CSER program is evolving towards reviews of specific ADP systems or problem areas identified by site or DOE management.

B. CSER Process

The CSER process begins with a request to the CCS from the site for a review. The request is always voluntary and the CCS or DOE computer security program management never forces a CSER activity. After the CCS accepts the request, the CCS and the site jointly agree on the time, duration, and coverage of the review. The previsit discussions may include such items as computer systems included in the review, areas of emphasis, and CSER team members. The CSER team consists of at least two experts from the CCS and a representative from the site computer security organization.

The actual CSER begins with a briefing by the site computer security organization to acquaint the CSER team with the site. The briefing also identifies any special issues that must be addressed during the CSER. The CSER team then briefs the site management on the CSER process and the extent and timing of this particular CSER. A tentative schedule of facility and individual visits is developed during the discussions. After the in-briefing, the CSER team begins the review.

During the discussions the team probes the details of the site's classified computer security program. The discussions also address the individual's understanding and implementation of the local program. The discussions are characterized by the friendly, unconstrained sharing of information.

The visits and discussions continue until the CSER team has developed a thorough understanding of the site's computer security program. The team's findings are then presented at an outbriefing. The team reviews its findings with the site management and computer security organization at the outbriefing. Attendance at the outbriefing is always controlled by the site.

CSER findings are not routinely documented or disclosed to any audience without the approval of the site computer security organization. All notes collected by the CSER team are treated as classified information. The notes may be left at the site or destroyed following the procedures established for destruction of classified information.

C. CSER Benefits

The CSER program has resulted in a number of benefits at all levels of the DOE Classified Computer Security Program. Computer security officers at the various sites have gained an improved understanding of DOE orders and regulations and have learned of good computer security practices at other sites.

The CCS has gained an enhanced understanding of the issues, problems, and practicality of existing computer security solutions. The CCS understanding is shared with DOE headquarters through general discussions, research activities, and participation in working groups on specific issues.

The CSER program also provides important input to the direction of the CCS Technology Development (TD) program. The present CCS TD program includes the findings and other needs identified during the CSERs.

D. CSERs and Evolution of the Classified Computer Security Program

The CSER program provides significant contributions to the evolution of the DOE Classified Computer Security Program. CSER team members have participated in the development of DOE 5637.1 and are involved in the development of solutions to existing problems. The CSER team members also participated in the development of the Computer Security Standards and Criteria (S&C) used in the DOE I&E program.

IV. FINDINGS

The DOE order on Classified Computer Security (DOE 5637.1) addresses many of these CSER findings by establishing policy requirements. This order requires all DOE or DOE contractor ADP systems to be accredited under the new order within 3 years.

These CSER findings illustrate that a major element in the DOE Classified Computer Security Program is a knowledgeable user. DOE 5637.1 assumes the user is a responsible participant in maintaining the security of classified information. The expectation of a knowledgeable user allows DOE to concentrate its efforts on addressing the malicious insider or outsider. Policy flexibility and the range of computer systems across DOE prevent DOE from specifying a specific approach to computer security, as exemplified by the Department of Defense (DoD) computer security policy. The policy flexibility also creates complex trade-off decisions for management at each site.

The CSER findings are grouped into the following categories:

- Management procedures
- Certification and accreditation
- Personnel security
- Physical security
- Telecommunications security
- Hardware and software security
- Administrative security

Table I lists the findings covered in existing or new DOE orders.

A. Management Procedures

1. Threat Guidance. Virtually every DOE or DOE contractor site has prepared a statement of threat. Many of the statements are so generic or superficial that they provide little assistance in securing a computing system. The development of meaningful site-specific statements has been inhibited by the lack of detailed guidance from DOE headquarters. The lack of specific threat information also affects the quality of the DOE contractor site threat statements.

Another issue frequently observed is a lack of understanding or awareness of the threats against DOE computing facilities. Personnel in some facilities seem to believe that their systems are not attractive targets. Another belief is that they do not have a serious problem because "everyone who can get into the facility is cleared."

Activities in Progress

- DOE/Office of Safeguards and Security (OSS), Computer and Technical Security Branch (CTSB) has released a generic threat statement. The statement is a baseline statement of threat for the development of site statements of threat. The lack of specific threat information continues to hamper the preparation of local threat statements.

Recommendations

- Each site should develop and distribute to all users a generic computer security statement of threat based on guidance from the CTSB.
- Continue enhancement of the DOE CTSB generic statement of threat.
- Conduct a consistency and completeness review for content of all site statements of threat. Distribute the results of the review to each site and the CTSB to enhance the site and DOE statements of threat.
- Continue awareness training of all users and computer security staff, both at the classified and unclassified levels.

TABLE I. Findings and Coverage in DOE Orders

CSER Findings	Addressed in DOE Order 5637.1
Management Procedures	
- Threat guidance	Yes
- Risk management	Yes
- Computer security planning	Yes
- Incident program	Yes
- Local inspection/review program	Yes
- Contingency planning	Yes
- Configuration management	Yes
- Waste, fraud, and abuse monitoring	Yes
- Coordination of facility changes	Yes
- General management awareness	Yes
- Computer security reviews of ADP procurements	Yes
Certification and Accreditation	
- Security plan development and maintenance	Yes
- System security testing guides	Yes
- Certification and accreditation procedures	Yes
Personnel Security	
- Uncleared people developing/maintaining software	Yes
Physical Security	
- Escort procedures and training	Yes
- Access list maintenance	Yes
- Unattended systems	No
- Emergency controls and equipment	No
- Visual access controls	Yes
- Media protection	Yes
Telecommunications Security	
- Telephones too close to computing equipment	No
- Uncontrolled modems	No
- Red/Black separation	No
Hardware and Software Security	
- Multi-level systems	Yes
- Activation of system security features	No
- Security evaluation techniques	No
- Technical computer security knowledge	No
- Networks	Yes
- Audit trails and audit trail analysis tools	Yes
Administrative Security	
- Education/awareness program	Yes
- User guides	Yes
- Authentication	Yes
- Remote diagnostics	Yes
- ADP system inventory	Yes

- Develop a classified, detailed DOE computer security threat statement to assist the sites in developing/improving the site threat statements.
- Develop an active program, within the CTSB, to monitor threat information developed by other DOE and government agencies. Disseminate the appropriate information throughout the DOE computer security program.
- Develop and regularly update a DOE-oriented computer security threat briefing. Present the briefing annually to the DOE and DOE contractor personnel responsible for managing computer security.

2. Risk Management. The lack of DOE guidelines for risk management for site computing resources is a consistent problem across most DOE contractor facilities. Many facilities have independently defined their own risk management programs because of the lack of guidance from DOE. When site guidelines do exist, they often consist only of simple statements requiring the Computer System Security Officer (CSSO) to perform an unspecified form of risk assessment. Another approach is a "fill-in-the-blank" approach that assumes that every computing resource at the site has nearly identical risks. The opposite extreme requires expensive quantitative methods without establishing realistic values for the loss or compromise of classified information.

Comprehensive, current threat information is essential to a high quality risk management program. The lack of detailed DOE threat guidance further inhibits the development of a comprehensive, effective risk assessment program at each site.

There are many risk assessment methodologies commercially available. Most of these packages require a quantified method of risk assessment. The difficulty in establishing a value for classified information negates the value of these packages to the DOE community. Another shortcoming of these packages is their inability to integrate DOE's philosophy on computer security, i.e., a balance between personnel, physical, telecommunications, hardware, software, and administrative security.

Activities in Progress

- DOE 5637.1 requires the development of site risk management programs.
- DOE/OSS and DOE/Office of Automated Data Processing (OADP) are jointly funding the development of a standard risk assessment technique for DOE.

Recommendations

- Continue funding and development of the standard DOE risk assessment technique and tool.

3. Computer Security Planning. The pressure to improve computer security in an era of stable or declining budgets is aggravating the serious problem of limited resources. Computer security is often perceived as affecting productivity and so receives low priority when management distributes resources.

The lack of resources forces many computer security organizations to concentrate on high priority issues and problems. Low priority items receive little or no attention. This gives the users the incorrect message that computer security is unimportant. The identification of resource requirements in the short- and long-range plans required by DOE 5637.1 will help provide the needed visibility and management attention.

Activities in Progress

- DOE 5637.1 requires the development of short- and long-range computer security plans at all site and DOE management levels.

Recommendations

- Continue with CTSB plans for the development of the short- and long-range plans.

4. Incident Program. Before the development of the S&C and DOE 5637.1, some sites lacked active programs to identify computer security incidents. All sites have established incident programs as part of the implementation of DOE 5637.1. Each site program is subject to approval by the cognizant DOE official. Many site personnel visited by CSER teams have suggested DOE guidance on the minimum content of an incident program. DOE 5637.1 provides some guidance, but the sites appear to be asking for additional information.

Activities in Progress

- DOE 5637.1 requires that the DOE Operations Offices and individual sites develop site-specific incident programs.
- DOE 5637.1 requires each Operations Office to develop guides for incident programs at the contractor sites reporting to the Operations Office.

Recommendations

- Develop DOE-wide guides for incident programs, including minimum/mandatory content identified in DOE 5637.1.

5. Local Inspection/Review Program. The CSER activities have revealed there were few comprehensive reviews of local ADP systems conducted by the local computer security organizations. The frequency of reviews has improved dramatically as the I&E process matured along with the development of DOE 5637.1. The lack of guidelines for review content and the limited resources available for reviews continue to affect the review program.

DOE 5637.1 requires several different annual reviews and a review of an ADP system every 3 years. The order does not provide any guidance regarding review content or the conduct of the review.

Activities in Progress

- DOE 5637.1 requires sites to develop programs for the annual review of the site classified computer security program. The cognizant DOE Operations Office must approve the site review program.
- DOE 5637.1 requires
 - annual reviews by the Computer Security Site Manager (CSSM) of the computer security program managed by each CSSO.
 - regular reviews of each contractor site by the cognizant Operations Office.
 - regular reviews of each Operations Office by DOE headquarters.
 - regular reviews (every 3 years) of each ADP system processing classified information.
- The CCS is developing guides for a site review program.

Recommendations

- Adopt guides being developed by CCS as a suggested approach for each site. Annually review and update CCS guides, with assistance from the CTSB and field.

6. Contingency Planning. The lack of contingency and recovery planning makes ADP systems vulnerable to denial of use and possible compromise of information. The failure to adequately plan for restoration of services can also disrupt performance of the site mission.

Most DOE and DOE contractor ADP systems are perceived as not being critical to the mission of the organization. The result is that many of these systems do not have any adequate contingency or recovery plans. The lack of DOE-wide guidelines for (a) determining when an ADP system is critical, (b) developing and testing appropriate contingency and recovery plans, and (c) backing up software, data, and documentation further confuses the issue.

Activities in Progress

- DOE 5637.1 requires the development of contingency plans for every computing resource processing classified information.
- DOE 5637.1 requires the identification, back-up, and proper storage of all critical software and documentation.
- DOE 5637.1 requires the testing of contingency and recovery procedures for every critical ADP system.
- The CCS is developing contingency plan guides and templates for the range of computing resources used in DOE.

- The CCS training program enhances understanding of contingency plans and their relationship to the computer security program.

Recommendations

- Adopt the CCS guides and templates as the suggested approach for each site. Annually review and update the guides and templates.
- User awareness training should include discussion of this problem.
- Alternative approach
 - Contract for the modification of an existing commercial package to meet DOE needs and a DOE-wide basic ordering agreement and license.
 - Evaluate commercially successful back-up and storage plans for their applicability to the DOE environment.

7. Configuration Management. The lack of comprehensive configuration management procedures allows undocumented changes to the computing facility that may affect the security of the facility. Traditional procedures have dealt exclusively with software. Today's distributed computing environment also requires management of hardware and facility changes to provide a secure environment for processing of classified information.

Another aspect of the problem is the unknown or unauthorized introduction of changes to systems or connections to another computing system. Changes such as these can bypass or negate the security of the entire computing system. DOE 5637.1 requires a security review of all applications software that has a security function. The lack of guidelines on the content of the review and insufficient personnel resources makes a realistic review difficult.

The lack of DOE guides for the scope of configuration management procedures is a deterrent to development of site-wide procedures. A related problem is the lack of management of hardware and physical plant changes under the same or parallel procedures.

Activities in Progress

- DOE 5637.1 requires configuration management procedures for every computing resource that processes classified information.
- CCS is developing guides for configuration management.
- CCS training courses are enhancing understanding of the need for and use of configuration management.

Recommendations

- Adopt the guides being developed by the CCS as the suggested approach for each site. Annually review and update the guides.

8. Waste, Fraud, and Abuse Monitoring. Recent U.S. government policies have established a requirement to monitor all government and government contractor ADP systems for waste, fraud, or abuse. Many DOE sites have traditionally allowed computer activities that are now identified as waste, fraud, or abuse, e.g., use of games and other programs to learn new computer skills. The education required to establish new operating habits or awareness is substantial. Another factor is the perception that computer resources are not equivalent to government resources, e.g., copiers, typewriters, vehicles. Many people seem to believe that if the computer is not being used for government business then personal use is not misuse.

The lack of DOE guidance on the content of a site waste, fraud, and abuse program inhibits compliance with DOE 5637.1. Most sites have established programs for periodic review of computer usage, but many of these programs do not clearly define waste, fraud, or abuse. A complicating issue is the widespread distribution of computing resources through personal computers and intelligent workstations. The lack of guidelines regarding what is appropriate monitoring activity for a single user ADP system is a serious problem.

Activities in Progress

- DOE 5637.1 requires awareness training.
- DOE 5637.1 requires the development of (site) programs for monitoring waste, fraud, and abuse.
- CCS is developing guides and procedures for a waste, fraud, and abuse monitoring program.
- CCS training courses are enhancing understanding of the need for and the use of monitoring waste, fraud, and abuse.

Recommendations

- Train the users in their responsibilities.
- Adopt CCS guides as the suggested approach for each site. Annually review and update the guides and procedures.

9. Coordination of Facility Changes. The CSER teams have frequently encountered insufficient coordination between the computer security organization and other site organizations responsible for development and maintenance of the physical facility. Most of the sites have established procedures to notify computer security when electrical power is affected. Other areas, e.g., plumbing, heating, ventilation, and painting, are frequently not coordinated with computer security. This problem is particularly acute in facilities housing distributed computer systems. The smaller facilities seem to be ignored when facility maintenance decisions are made. Computer security organizations responsible for the large central computer complexes generally are notified whenever any physical activity occurs in the facility.

The CSER teams have observed a gradual improvement of coordination at many of the sites, but additional work is needed to ensure that security of the facility is maintained.

Activities in Progress

- DOE 5637.1 requires the coordination of computer security with other site functional areas that may impact the program.

Recommendations

- Develop DOE-wide guides containing suggested areas that should be coordinated with the site computer security program.
- Include the need for coordination in all computer security education and briefing materials.

10. General Management Awareness. Management awareness and support for computer security throughout the DOE has risen significantly since the start of the I&E process and the development of DOE 5637.1. The general lack of responsiveness to computer security issues by all levels of management is demonstrated at some sites by

- Low priority of resource requirements for the computer security organization.
- Low emphasis placed on site-wide procedures and guidelines, e.g., risk management, and contingency planning.
- Management perspective that an engineer or scientist is more important to the site's mission than a computer security person.

Activities in Progress

- DOE 5637.1 requires the development of many site-wide policies.
- DOE 5637.1 requires the development of short- and long-range plans for computer security.
- CCS has developed a briefing designed to improve management awareness of computer security issues.

Recommendations

- Expand and update the CCS management briefing material. Make the material available for each site to conduct its own briefings.
- Collect and disseminate computer security awareness material for use by the local computer security organization to improve management awareness.
- Include criteria for each of the required reviews to check on management participation in computer security issues and procedures.

11. Computer Security Reviews of ADP Procurements. The CSERs have found that a few computer security organizations have not been involved in the review of computing procurements. The larger sites have active programs to review all computing resource procurement requests. Limited resources at some smaller sites affect the effectiveness of the procedures.

Another area that needs improvement is procurement personnel awareness of when a computer security review is needed. The computer security organization routinely reviews major items, such as complete computer systems or software. Smaller items, such as software or hardware updates, hardware additions to existing resources, and equipment containing control computers, are occasionally overlooked during the procurement process.

There is little training provided to procurement personnel on the type of item to be reviewed. Procurement staff members are often trained only through frequent interaction with the computer security staff. When new people are added to the procurement process there is little recognition of the need for computer security training.

Activities in Progress

- DOE 5637.1 requires review and approval by the computer security organization of all purchase requests affecting computer security.

Recommendations

- Develop education/awareness material for use by the local computer security organization to improve awareness in procurement personnel.

B. Certification and Accreditation

1. ADP Security Plan Development and Maintenance. The CSER teams have consistently found ADP security plans that were out of date. Occasionally the teams found security plans that had not been accredited before the processing of classified information. A chronic problem is the lack of clear guidance for when a security plan must be written or updated.

Another significant problem is the lack of resources to develop and maintain the comprehensive ADP security plans required in DOE 5637.1. A good ADP security plan requires considerable resources to produce. Keeping the plan current and consistent with changes in the ADP system also requires considerable resources.

The CSER teams have noticed a lack of consistency in structure and content of ADP security plans between contractors and Operations Offices. Although the plans are approved and accredited, they often reflect local biases. The lack of DOE-wide guidelines results in confusion about what details the plan must include. The CSER teams have encountered the statement, "Why do I have to write that information in my plan when my friend at site X did not have to do that and his/her plan was approved?"

Activities in Progress

- DOE 5637.1 requires the development and maintenance of a security plan for every computing resource processing classified information.
- DOE 5637.1 contains a basic outline for ADP security plans.

- The CCS has developed security plan guides for development and maintenance of security plans.

Recommendations

- Adopt the guides developed by the CCS as the suggested approach for each site. Annually review and update the guides.

2. System Security Testing Guides. A chronic problem across DOE and its contractors is the lack of adequate security testing for ADP systems that process classified information. In many sites, the quantity and quality of security testing is left to the discretion of the individual CSSO. The CSSOs typically do not have any training on testing. The absence of DOE-wide security testing guidelines forces the CSSO to depend on local resources. Some sites, typically the larger ones with more personnel resources, have begun to develop local guides. The many different types of computing systems and rapid changes in technology at each DOE site have complicated an already difficult task.

Another complicating factor is the lack of a clear understanding of what is a secure ADP system in DOE. DOE 5637.1 establishes security objectives and allows the local site to balance physical, personnel, administrative, communications, hardware, and software security to achieve a "secure" system. This flexibility allows each site to make cost-effective trade-offs in securing the system. The flexibility also complicates the security testing, certification, and accreditation of a system.

Activities in Progress

- DOE 5637.1 requires testing of ADP systems and security software before accreditation, whenever security-related changes are made, or every 3 years.
- The Testing and Certification Working Group is chartered to develop test/certification guides.

Recommendations

- Adopt the guides developed by the certification/accreditation working group. Annually review and update the guides.
- Develop security testing training for all members of the DOE accreditation process, e.g., CSOMs, CSSMs, and CSSOs.
- Develop and disseminate a DOE definition of what is a secure ADP system.

3. Certification and Accreditation Procedures. The lack of DOE-wide guidelines for certification of ADP systems aggravates the security testing issues discussed in the previous section. Certification is largely a security testing matter, but other administrative issues are also included in the certification process.

DOE 5637.1 requires accreditation of an ADP system by a DOE official. The CSER teams have found a few systems that were operating without formal accreditation. Most of these systems were granted interim accreditation by the cognizant DOE official. The DOE official typically did not have the time, people, or technical knowledge to conduct the appropriate review of the certification material when it was submitted.

Another aspect of the accreditation problem is the lack of consistency among DOE officials during the accreditation process. This minor problem illustrates the following common issues observed by the CSER teams.

- The lack of definition of what is a secure system forces the accreditor to follow his/her own perspective or negotiate agreement with the site on the required security elements.
- The lack of resources, e.g., time, people, and operating procedures, prevents the DOE official from conducting appropriate reviews of the certification documentation.
- The rapid changes in technology and the proliferation of the types of computer systems can overwhelm the accrediting official's resources. The DOE accrediting officials may simply be unacquainted with the technical issues involved in a particular ADP system. There are no commercial or academic training opportunities that can provide the needed technical information.
- Accreditation requires a DOE official to accept a level of risk in the system presented for accreditation. The lack of adequate threat information and the lack of guidance on the acceptable levels of risk requires the official to rely on his/her own judgement.

Activities in Progress

- The Testing and Certification Working Group is chartered to develop test/certification guides.

Recommendations

- Adopt the guides developed by the Testing and Certification Working Group. Annually review and update the guides.
- Develop training material oriented towards the accreditor's requirements, including briefings on changes and trends in technology. Provide the material in annual briefings and regular bulletins to all accrediting organizations.
- Develop DOE-wide guidelines defining acceptable levels of risk in the various types of ADP systems used in DOE.

C. Personnel Security

1. Uncleared People Developing/Maintaining Software. Modern software engineering techniques contain the implicit assumption that everybody is trying to write "correct" software. The techniques assume that programmers are not malicious, just unaware of the correct approach. None of the techniques allow for the situation where two classes of programmers exist: untrustworthy, i.e., uncleared, and those that are, by definition, trustworthy, i.e., cleared people, in teams of two or more. In particular, no technique can withstand two malicious programmers in collusion. The range of technical capabilities in each category of programmer (call them cleared and uncleared) further complicates the problem. Collusion is unlikely with cleared people, but it is much more likely, in a hostile intelligence sense, among uncleared people. The hostile intelligence services could place two agents in an unclassified shop just about as easily as they could place one. Placing two cleared people in a software shop where they can collaborate is much harder.

The increasing reliance on computing components, such as software, developed by uncleared or unknown individuals is a serious problem. Most CSSOs do not have the time or technical knowledge to conduct an in-depth review of each product. Source programs for much of the software being used on personal computers and workstations are not available to the sites. Security reviews of products must be based on a realistic view of the potential for impact on the security of the information being processed.

Activities in Progress

- DOE 5637.1 requires a security review, testing, and evaluation of all software used in a computing resource processing classified information.
- CCS is developing guides for the review of software developed by uncleared personnel.

Recommendations

- Adopt CCS guides as the suggested approach for each site. Annually review and update the guides.
- Develop methods for quickly and easily determining if a software package has been changed.
- Include information from the Testing and Certification Working Group into software review guides.

D. Physical Security

1. Escort Procedures and Training. The increasing use of computing systems and vendor's efforts to reduce their costs have required the use of uncleared maintenance personnel. These people come to the site only when the computing system has failed and needs maintenance. The infrequent on-site work, long times to obtain a clearance, and the vendor's need to

rotate maintenance personnel have created the need for computer-security-trained escorts. These escorts must ensure that the escorted personnel follow the proper security practices. Computer-security-trained escorts are also needed for other types of activities in a computing facility, e.g., physical construction or maintenance.

The CSER teams have been told of practices that allowed a guard to escort the personnel into the room and then retire to a comfortable chair and read a book. Although this practice is extremely rare, it illustrates the level of training and awareness needed for proper escort of uncleared people.

A legitimate concern is that the escort not be required to know as much as the person being escorted. The escort should be familiar with the ADP system(s) and the security procedures followed for the facility. The escort should provide guidance on what security procedures must be followed, e.g., a circuit board containing memory chips must be reviewed by the computer security organization before it leaves the site.

Many sites are attempting to implement this DOE 5637.1 requirement but lack the resources to develop computer-security-oriented escort training material.

Activities in Progress

- DOE 5637.1 requires escort training and CSSO approval of escorts.

Recommendations

- Develop training guides for escorts.
- Develop escort training materials for use by individual sites.

2. Access List Maintenance. Maintenance of lists authorizing access to computing resource facilities is a difficult problem with a wide range of issues. Some small facilities, typically those used by a small number of personnel who know each other, tend to simply post a list of authorized personnel with informal procedures for updating the list. The larger facilities often have well conceived procedures for updating the access lists.

Many facilities lack the timely information flow from the personnel or administrative organization to keep a CSSO informed of personnel changes.

Other observed problems include no technique for preventing an unauthorized addition to the list. The lists may be updated with a date and signature but are frequently left "open" at the bottom, which permits the easy addition of names.

Activities in Progress

- DOE 5637.1 requires CSSO to develop notification of change procedures.

Recommendations

- Develop DOE guide describing suggested approaches to developing, reviewing, and maintaining access control lists. The guide should include techniques to prevent unauthorized changes or additions. The guide should also include suggestions for timely information flow between the using and personnel organizations so the list will accurately reflect personnel changes.

3. Unattended Systems. Many computing resources are occasionally operated in an unattended mode for the convenience of the user community. The unattended systems are frequently secured by the appropriate physical protections, e.g., locks. The lock combinations or other access controls are often known to a variety of personnel, e.g., janitors. These people can often enter the facility without another person present and thereby gain unrestricted access to the resource.

Classified systems are supposed to be protected as if they were plain-text sheets of paper. That is, access to the system should be as hard as access to the inside of a safe. After hours, this is usually handled by a Sergeant and Greenleaf Type 1 combination lock with an approved alarm system in the facility. During working hours, it is usually handled by a cipher-lock, or equivalent, provided the door is under "constant observation" or the facility is "constantly attended by cleared people."

Activities in Progress

- DOE 5637.1 requires the ADP system be placed into a vault or vault-type room.

Recommendations

- Develop guides for maintenance of access lists and for access control in computer facilities.
- Do not operate classified systems in an unattended mode unless the systems and their peripherals are located in a properly protected security area. The access controls should be sufficient to prevent any single individual from entering the facility without prior approval or notification.

4. Emergency Controls and Equipment. Emergency or backup equipment for continuity of operations is often placed in areas that allow a possible interruption without penetrating the computing facility. The denial of service issue requires the review of the backup and emergency facilities for adequate protection.

Transformers and backup generators have been observed in completely unprotected environments where casual, unauthorized access (or destruction) would not be detected until the service was required.

Activities in Progress

- No known activities in progress to address this issue.

Recommendations

- Produce DOE guides containing suggested techniques for the protection of the emergency and backup equipment. Develop the guides in cooperation with the physical protection organization in DOE.

5. Visual Access Controls. A widespread problem observed by the CSER teams is the visual access to display devices from outside the secure area or by a person walking through the office or equipment area. The lack of user awareness is the apparent cause of this problem. All of the sites have policies describing the requirement to properly place the devices. The occasional movement of display devices within an office area can create the opportunity for casual visual access.

This is not a difficult problem to solve if people are aware of the requirement and pay attention to it.

Activities in Progress

- DOE 5637.1 requires that casual visual access of display devices be eliminated.

Recommendations

- Develop DOE-wide guides for reviewing the placement of output devices to be sure visual access is properly restricted.
- Develop user awareness training based on the guides and requirements in DOE 5637.1.

6. Media Protection. Media protection issues include two broad areas, marking and handling. Media marking is required to provide proper protection for the information stored on the media. Many sites have adopted procedures for the marking of magnetic media containing classified information. A common position is to not mark any media that contains unclassified information. This approach is normally consistently followed for media produced by site personnel. Media introduced by vendors, containing software, diagnostics, etc. are often not marked even though they were used on a system processing classified information. All marking should be positive, e.g., mark everything, including unclassified, to avoid misunderstanding and confusion. Other types of media are not normally marked. These items, circuit boards, memory boards (memory, microcode, etc.), diagnostic media brought in by maintenance personnel, spare parts, etc., should be marked to ensure that all classified information is properly protected.

The proper handling of media is also an area where procedures need to be improved. Most sites have reasonable procedures for the handling, sanitizing, and destruction of magnetic media. Other forms of media, circuit boards, etc., are often not covered in the procedures. There has been some confusion regarding the proper handling of circuit and memory boards that may have contained classified information. Some sites insist on a careful review and retention for several days to help ensure that the

information has been destroyed. Other sites feel that once the power has been removed the information has been destroyed. DOE does not have any guidance covering non-magnetic media.

Another widespread media handling problem is the return of media to receive software enhancements, updates, etc. Many vendors provide discounts to DOE sites for upgrades to the latest software releases. These discounts are often based on the return of the media containing the previous release. The CSER teams have observed many sites attempting to reduce their software costs by using the discounts without concern for the possible loss of information. Many of the policies appear to be based on the incomplete understanding of how software could be used to write classified information on the vendor's media without the knowledge of the user.

A common handling problem related to the upgrade problem is the perception that media used to install new software on a system containing classified information do not need protection or marking. The perception seems to be that the media are not written by the users and therefore it does not contain any classified information (see above comments).

Activities in Progress

- The CCS is developing guides for marking media consistent with the U.S. government standards.
- Standards for marking ADP media have been developed by the U.S. government.
- DOE 5637.1 and CSC-STD-005-85, "Department of Defense Magnetic Remanence Security Guidelines" provide standards for sanitization and declassification of magnetic media.

Recommendations

- Develop DOE-wide guidelines covering the return of media from classified systems. Annually review and update the guides.
- Adopt the CCS and U.S. government guides as suggested approaches for each site. Annually review and update the guides.

E. Telecommunications Security

1. Telephones Too Close to Computing Equipment. Most DOE and DOE contractor sites are implementing the policy requiring a minimum separation between a telephone instrument and computing resources. Considerable confusion exists regarding the required separation and how to measure it. For example, is the separation to be measured from the computer system to the telephone instrument, to the telephone line, or both? Some confusion is also occurring because some sites have obtained a waiver for a smaller separation and the criteria for granting the exception are not available to other sites.

The CSER teams have encountered some inconsistency in the implementation of some TEMPEST rules across the DOE, i.e., some sites require TEMPEST

equipment for all systems processing classified information, some use TEMPEST equipment only for system processing intelligence information, and some do not use TEMPEST equipment.

Activities in Progress

- There are no known activities in progress to address this issue at the DOE-wide level.
- National reviews of the TEMPEST problem may eliminate or alleviate this problem.

Recommendations

- Initiate a complete review of the separation issue. Release DOE guides covering the minimum separation, if any, and the proper technique for measuring the distance (to the instrument or the line).
- Incorporate the results of national policy on emanations into DOE orders.

2. Uncontrolled Modems. The introduction of modems into a computing system is a continuing problem aggravated by increased functionality and reduced cost of modems. Modems are sometimes added to resources as a temporary measure to improve an individual's productivity. Another form of modem introduction is the purchase of computing resource equipment that contains modem capabilities as a secondary function.

Some computing systems contain modems for use by remote maintenance services and occasionally these modems remain connected after the remote service has been completed.

The previous comments on review of ADP procurements and configuration management also apply to the modem problem. Implementation of the recommendations for the procurement and configuration management issues will assist in managing the modem situation.

Activities in Progress

- CCS is developing guides on remote diagnostic use.

Recommendations

- Improve user training to include awareness of the modem concerns and issues.
- Improve awareness in the procurement organizations concerning modem procurements for computing resources processing classified information.
- Computer security organization reviews of all procurements for any computing resource.

- Establish DOE guides on automated review of telephone lines in the facility to identify any unknown modems.
- Establish clear infraction/violation policies regarding the unauthorized connection of modems, or use of any other unauthorized hardware/software, to computing resources processing classified information.
- Several sites have implemented commercial or locally developed software to scan all facility telephone lines outside of normal working hours. This software typically prints a report of every telephone number found with a carrier tone indicating the presence of a modem. The computer security organization manually checks the location of the telephone number to determine if the modem is authorized.

3. Red/Black Separation. The separation of lines carrying classified information from lines that are open to interception is a complex problem. Each facility is different and the location and signal characteristics of most lines present hard-to-evaluate issues. Unfortunately, this is a rather esoteric area and the available knowledge is scattered and overworked with other problems.

Activities in Progress

- Reviews of this issue, among other emanation issues, are being done at the national level.
- Technical guidelines for this area are available in NACSIM 5203, Guidelines for Facility Design and Red/Black Installation, dated 30 June 1982; and MILHANDBOOK-232A, dated 20 March 1987.

Recommendations

- Implement new national policies in this area as they are promulgated.

F. Hardware and Software Security

1. Multi-level Systems. A multi-level computing system is one that is accessed by at least one user who does not meet national clearability standards (cleared) for all the information on the system. A system-high system is one where all users are cleared to or above the highest level of information processed on the system. For example, if all users are cleared for access to secret information and the most sensitive data on the system is confidential, the system is operating in a system-high mode. If the most sensitive data on the system is confidential/restricted data, the system is operating in a compartmented mode (i.e., everybody on the system is cleared for all data on the system, but some users have not been formally indoctrinated for all the data on the system [the restricted data]).

A multi-level system can be created by connecting the system to other computing resources operating at a lower level of protection. A multi-level system can also be created by connecting modems to a system processing classified information. One might call this an inadvertent creation

of a multi-level system. More precisely, this is the conversion of a dedicated (or system-high) system into a multi-level system. This "accidental" creation of a multi-level system can be prevented by application of better management and user awareness and improved configuration management procedures. Creation of computer networks is a classic example of how a multi-level situation can easily occur.

Activities in Progress

- DOE 5637.1 provides guidance for determining the required level of protection for any combination of user clearances, data classification levels, and categories of data.

Recommendations

- Develop DOE guides to explain the required safeguards for any combination of user clearances and data classification levels and categories of data.
- Develop an automated tool to assist the CSSO in reviewing the user clearances and data classification levels. The tool should list the required safeguards as part of the review process.
- Develop DOE-wide guidelines for the configuration management of networks.

2. Activation of System Security Features. The complexities of modern computer systems and limited resources have increased the difficulty of understanding what security features are necessary for the system's operating environment. The CSER teams have found situations where CSSOs admitted that their choice and setting of security features was influenced by a peer or friend who "heard" from another friend, or at a conference, that a particular feature should or should not be selected. Most of these suggestions had the form of "don't use feature x because it uses too much of the computing resource."

The lack of guidelines for DOE computing systems requires a CSSO to rely on possibly incomplete knowledge or recommendations from sources who may not understand computer security requirements in DOE.

Activities in Progress

- Commercial classes exist to train security officers on these security features. Unfortunately, they are expensive, extremely system-specific, and are usually not oriented toward DOE's needs.

Recommendations

- Develop a list of the known security features and their proper settings for each type of commercial computing resource used in DOE. The list should support any acceptable combination of user clearances and data classification levels. There are approximately 20 major system types in DOE for which these lists must be created.

This effort will also require close cooperation with the system vendors to keep the lists current and consistent with the most recent releases of the software.

- Develop a program that checks settings of known security features and warns the CSSO of "improper settings."

3. Security Evaluation Techniques. There are no known workable techniques for evaluating the impact on security of proposed or actual changes in a secure computing resource. The individual CSSO is required to guess at the impact of changes and make decisions based on guess or on folklore.

The CSSO has neither the capability of describing the changes in a rigorous manner (e.g., a programming language) nor the tools for evaluating the changes.

Activities in Progress

- No known applicable activities in this area.

Recommendations

- Initiate a limited research activity to identify the issues and develop a recommended approach to develop the necessary tools.

4. Technical Computer Security Knowledge. Most CSSO assignments are part-time activities and the individuals simply do not have the time to identify and study the available computer security material. The rapid evolution of technology and skills of the potential penetrator is also exceeding the resources of the part-time CSSO to maintain current knowledge of the state-of-the-art in computer security.

Activities in Progress

- The CCS CSSO training provides some of this knowledge.
- The CCS CSSO toolkit will augment the CSSO knowledge by providing automated tools to perform the routine activities, thereby freeing important resources for higher-priority concerns.

Recommendations

- Improve management support and recognition of CSSO responsibilities.
- Develop a program to identify and disseminate sources of information that would be useful to a CSSO. The information should allow the CSSO to selectively obtain the needed information with a minimum of effort. The program should identify the available educational opportunities in the academic and seminar fields that might assist the CSSO. A bibliography for the CSSO should contain other sources, such as books and periodicals.

- Develop a DOE-oriented seminar to present the current knowledge to the CSSO. The seminar should aim towards exposing the CSSO to the information with references for additional individual study outside of the seminar.

5. Networks. The rapid evolution of networks and the lack of security guidelines has raised some serious security concerns throughout DOE. Rapid changes in technology coupled with reduced costs are strong inducements for the user communities to rapidly acquire and install networks for productivity reasons.

The lack of DOE guidance on network security continues to leave the sites in a difficult situation in which they are expected to secure the networks with no guidance from DOE and little or no resources to study the security properties of the hardware and software.

The Trusted Network Interpretation (TNI) developed by the National Center for Computer Security provides a good general base for network security. However, many experts feel that the TNI is too complex, too vague, and too limited to ever be of practical use in the federal government. The TNI needs to be augmented and enhanced to reflect DOE needs and policies. Nationally, there is a debate about the applicability of the TNI because of the difficulty in interpreting the document, even for those who have worked in the field for some years.

For better or worse, DOE probably handles networks better than anyone else in the federal government.

Activities in Progress

- DOE 5637.1 requires that network security be recognized by developing a security plan for each network, appointing a CSSO/CSSM for each network, and appointing a single entity responsible for the entire network.
- There are no known activities in progress that address this issue.
- All major networks in DOE receive a lot of attention relative to computer security.

Recommendations

- Develop a DOE-oriented version of the TNI.
- Develop study teams to assist a site in determining the security of a network.

6. Audit Trails and Audit Trail Analysis Tools. The lack of meaningful analysis of audit trails to detect intrusion or other misuse of a computing system is a widespread problem in DOE. DOE 5637.1 emphasizes accountability for all actions by users of an ADP system. Most modern operating systems used in DOE provide some form of accounting information that can be used in an analysis effort.

A contributing factor is the lack of DOE-wide guidelines on what should be collected and the type of analysis that should be performed. The entire computer security community is presently unable to agree on these issues.

Analysis of an audit trail is very complex and requires substantial resources. Virtually all of the major computing centers in DOE have developed automated techniques to support the analysis activity. The distributed systems typically have more primitive analysis approaches, typically periodic manual reviews. Automated tools that identify anomalies in the collected information are necessary to allow the individual sites to implement the requirements in DOE 5637.1. These tools should organize and present the information in a manner that allows the CSSO to decide which activities require additional investigation.

Activities in Progress

- The CCS is developing an automated tool to analyze audit trails.

Recommendations

- Develop generic guidelines for standard content of audit trails.
- Develop DOE-wide guides on the content of an audit trail analysis activity. Develop automated tools to support the DOE guides.

G. Administrative Security

1. Education/Awareness Program. When the CSER program began, many sites had token or nonexistent education programs for CSSOs and users. Many sites have developed a training program and are beginning to experience difficulty in locating or developing new or updated material for use in their education programs.

The lack of resources in the computer security organizations is aggravating the problem.

Activities in Progress

- Most sites have developed and are continuing to enhance active programs to maintain computer security awareness in the user community.
- The CCS has developed a comprehensive CSSO education program that covers the basic information a CSSO needs to do the job.
- The CCS education program includes the basic CSSO class and a train-the-trainer class. The train-the-trainer class is designed to give local computer security organizations the ability to conduct local training for CSSOs.
- The CCS education plan has identified advanced seminars designed to enhance the CSSO's knowledge and ability to perform the CSSO function.

- DOE 5637.1 requires CSSO training and implementation of a user training and awareness program.
- CCS Bulletin Board System.

Recommendations

- Continue the CCS education program and development of the seminars and materials identified in the CCS education plan.
- Develop a program to identify, and where possible, collect and disseminate, information for use in the local education program.

2. User Guides. When the CSER program began, most sites provided computer security guidance to the user community through infrequent training sessions. The evolution of the CSER activities and the I&E program and the development of DOE 5637.1 have caused the rapid development of user-oriented material at most sites.

The lack of guides for suggested content and sources for materials, e.g., templates, has required each site to commit resources to develop the necessary material. The local material is often redundant or duplicates other information developed or collected by another site.

Activities in Progress

- DOE 5637.1 requires each site to develop user guides for computer security at the site.

Recommendations

- Collect and organize existing user guides developed by the various sites. Extract the common elements into a DOE-level guide for suggested use at each site.

3. Authentication. Early CSERs found that user authentication, typically passwords, was a major problem for many sites. The large central computing facilities generally had good password generation and management procedures. The distributed systems often used procedures that stressed convenience over security. The development of DOE 5637.1, I&E results, and increased awareness throughout DOE have combined to reduce the password management issue almost to a non-problem. The common commercial operating systems all provide reasonable password generation and management facilities. Most sites have implemented the proper software and added appropriate procedures on the multiple user systems to meet the requirements of DOE 5637.1.

Many sites have expressed the belief that DOE-wide guides on acceptable authentication techniques and procedures would aid their efforts. The authentication issue has been extended to include different techniques, e.g., biometrics, smart cards, and distributed computing systems. The proper or required authentication techniques for workstations, such as personal computers, are very unclear. The acceptability of other forms of authentication, e.g., retina scans and hand geometry, are unknown.

Activities in Progress

- DOE 5637.1 requires the development of a complete password management program following DOE and national policy.
- The CCS has developed a password generation product that meets the requirements of DOE and national policy.

Recommendations

- Develop DOE oriented guides and procedures to assist the CSSO in implementing the DOE policies. Incorporate use of the CCS developed password generator into the guides and procedures.
- Develop a program to collect and assess the acceptability of different forms of authentication approaches for DOE. Disseminate the information including guidelines on the proper use of the different techniques.

4. Remote Diagnostics. The increasing costs of computing system maintenance is creating both desire and pressure for the use of remote diagnostics. The lack of DOE guides has required each site to develop local policy for the use of remote diagnostic services. Another aspect of the problem is the lack of properly secured vendor facilities where the remote diagnostic work can be performed.

A difficult problem frequently encountered is the determination of situations where use of remote diagnostic services is appropriate. For example, if a computing resource fails in a manner that prevents clearing of the main memory but allows the disconnection of all other media, can remote diagnostic services be used?

If secure remote diagnostic services are available at an appropriate security level, then the problem becomes the standard "check up to see that the procedures are followed" problem.

Activities in Progress

- The CCS is developing guidelines for the use of remote diagnostics.

Recommendations

- Adopt the guidelines developed by the CCS as suggested approaches for each site. Annually review and update the guides.
- Negotiate with the vendors of the popular computing resources in DOE to develop secure remote diagnostic service centers. Develop guides for the use of the secure diagnostic services.
- Include training on remote diagnostics in the CSSO courses.

5. ADP System Inventory. Prior to the development of DOE 5637.1 there was no requirement for each site to maintain a separate computer security inventory of ADP system hardware and security-related software.

All sites have continued to maintain the appropriate property inventory and controls. The computer security organizations often were unable to provide an accurate composite list of the ADP systems processing classified information. This information was available in the ADP Security Plans for each of the systems, but was not collected into a single list. DOE 5637.1 now requires that the CSSM maintain an inventory of all hardware and security-relevant software. Although this is a minor problem, the maintenance of an inventory is necessary to provide the proper management and to allow response to questions such as, how many systems of type X do you have at your site?, or we have discovered a vulnerability in version 2.1 of a particular type of software--please notify everyone running this version immediately. Previous responses to this type of question and notification were delayed while the site staff collected the information and the notices were simply distributed to every security officer at the site.

Activities in Progress

- The CCS has developed an inventory control product designed to assist the site in meeting the requirements in DOE 5637.1. The product has been distributed to all CSSMs.

Recommendations

- Encourage the use of the CCS product. Maintain and enhance the product to ensure it continues to meet the policy and field needs.

This report has been reproduced directly from
the best available copy.

Available to DOE and DOD contractors from
the Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831
prices available from
(615) 576-8401, FTS 626-8401

Available to the public from
the National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.
Springfield, VA 22161

Microfilm A01

Page Range	NTIS Price Code	Page Range	NTIS Price Code	Page Range	NTIS Price Code	Page Range	NTIS Price Code
001-025	A02	151-175	A03	301-325	A14	451-475	A20
026-050	A03	176-200	A09	326-350	A15	476-500	A21
051-075	A04	201-225	A10	351-375	A16	501-525	A22
076-100	A05	226-250	A11	376-400	A17	526-550	A23
101-125	A06	251-275	A12	401-425	A18	551-575	A24
126-150	A07	276-300	A13	426-450	A19	576-600	A25
						601-up ^a	A99

^aContact NTIS for a price quote.

