



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555

PDR  
PDR: John Vogelside

FEB 01 1993

MEMORANDUM FOR: Hugh L. Thompson, Jr.  
Deputy Executive Director  
for Nuclear Materials Safety,  
Safeguards, and Operations Support

FROM: Gerald F. Cranford, Director  
Office of Information Resources Management

SUBJECT: REVIEW OF NRC'S OFFICE OF INFORMATION RESOURCES  
MANAGEMENT COMPUTER SECURITY PROGRAM

Attached is the Office of Information Resources Management (IRM) action plan to correct the weaknesses in NRC's Computer Security Program that were identified in the Office of the Inspector General's (OIG) audit report entitled, "Significant Weaknesses Hamper NRC's Computer Security Program," dated December 15, 1992.

IRM's action plan is organized to correlate directly with the five categories of weaknesses listed in the OIG audit report. Under the five categories we have grouped the fourteen Los Alamos National Laboratory (LANL) recommendations that the OIG audit report noted had not been implemented by IRM. Accordingly, IRM is addressing all of these LANL recommendations in its corrective action plan.

Gerald F. Cranford, Director  
Office of Information Resources Management

Attachment:  
As stated

cc: JLFunches, OC

090040

9303110044 930201  
PDR ORG NE ED  
PDR

DF03

## COMPUTER SECURITY PROGRAM ACTION PLAN

Inspector General Category 1. System tests and audits were not being performed.

LANL recommendation E1. Develop system security test methodologies oriented to the different computing environments, such as PCs, minicomputers, and LANs.

LANL recommendation E2. Develop and implement a program of regular security testing to support certification and accreditation and to ensure that the system security mechanisms are functioning correctly.

LANL recommendation F1. Develop certification and accreditation methodologies oriented to the different computing environments, such as, PCs, minicomputers, and LANs.

LANL recommendation F2. Develop and implement a regular program to certify and accredit all NRC computer systems and LANs that process classified or sensitive information.

LANL recommendation L1. Modify the NRC computer security policy to describe the minimum contents of audit trails for the systems that provide this capability.

LANL recommendation L2. Modify the NRC computer security policy to define accountability procedures for systems that do not provide an automated audit trail capability.

LANL recommendation L3. Modify the NRC computer security policy to require documented periodic reviews of the audit trail/accountability information.

Action Source:

Division of Information Support Services

Tracked By:

Work Item Tracking System (WITS)

**Action Description and Completion Milestone:**

The NRC has identified many of its sensitive systems (Criminal History Check, Drug Testing, Property and Supply, Contract Information, SINET, NUDOCs, Payroll, IFMIS, and Personnel) as major systems of importance to the agency and thus prime candidates for certification and accreditation. Many of these systems have been subject to systems security testing and contingency plan testing in recent years, and have approved security plans. NRC is planning to begin this process for three of these systems during FY93.

The wording of Management Directive and Handbook 12.5 will address review of audit trail/accountability information for those systems where the operating system has a collection function for this information (see Inspector General Category 4).

1. Negotiate and award a contract to develop a methodology for certification and accreditation - February 28, 1993.
2. Negotiate and award a contract to develop a methodology for system tests of differing computing environments such as PCs, minicomputers, and LANs - December 31, 1993.
3. Negotiate and award a contract to begin certification and accreditation process of 3 major systems - August 31, 1993.

System 1 certification and accreditation final deliverable - April 30, 1994

System 2 certification and accreditation final deliverable - January 31, 1995

System 3 certification and accreditation final deliverable - September 30, 1995

4. Negotiate and award a contract to describe minimum contents for audit trails and develop a plan for review of audit trails - October 1, 1993.

Inspector General Category 2. Configuration management was not being exercised for sensitive systems.

LANL recommendation Q1. Implement the required configuration management for systems processing classified information.

LANL recommendation Q2. Develop and apply appropriate configuration guidelines for systems processing sensitive information. The guidelines should include more stringent controls for systems that are essential or critical.

Action Source:

Division of Information Support Services

Tracked By:

WITS

Action Description and Completion Milestone:

Systems processing classified information within the NRC are limited to microcomputer applications with configuration management requirements contained in the approval letter for the system security plan.

Minor sensitive unclassified information systems reside on microcomputers with configuration management requirements contained in the approval letter for the system security plan. In many cases, IRM staff visit microcomputer sites and audit the sensitive unclassified system as part of the initial review of the security plan.

Major sensitive unclassified systems reside on minicomputers. The NRC will develop configuration management guidelines, as appropriate, for changes to major sensitive unclassified systems. Change documentation guidelines will also be provided for smaller management information systems developed or maintained by individual offices within the agency.

1. Negotiate and award a contract to establish criteria for configuration management changes (e.g., software change control) for systems processing sensitive data - February 28, 1994.
2. Negotiate and award a contract to establish change documentation guidelines for smaller management information systems developed or maintained by individual offices within the agency - February 28, 1994.

The established criteria will then be provided to the Division of Computer and Telecommunications Services (DCTS) for incorporation into the life cycle management process for agency systems processing sensitive data.

Inspector General Category 3. NRC had not identified potential threats to its sensitive and classified information.

LANL recommendation C. Identify NRC-specific risks. Perform an assessment of the actual and likely threats and examine the situations that could compromise the NRC's ability to perform its stated tasks, e.g; situations that could embarrass the NRC or could lead to public distrust of the NRC. Document the assessment and distribute it to all employees and contractors, either in written form or during periodic security briefings.

LANL recommendation N. Develop and incorporate into the comprehensive training program a description and explanation of the "threats" to NRC information.

**Action Source:**

Division of Information Support Services

**Tracked By:**

WITS

**Action Description and Completion Milestone:**

The results of applying the Los Alamos Vulnerability and Risk Assessment (LAVA) software on ten NRC computer facilities (to date) will provide some data to use in developing an NRC specific threat profile. The current GSA contract to assess the security posture of the NRC Local Area Networks (LAN), subtask 3, will produce a list of LAN specific vulnerabilities. Some interviews and other data gathering will be necessary, as well as the development of a report document. Information from this document will be added to all of the NRC computer security training modules.

1. Negotiate and award a contract to develop a threat profile and training materials - September 30, 1993.
2. Incorporate "threat" information into NRC training modules - June 30, 1994.

Inspector General Category 4. The NRC computer security policy was outdated.

LANL Recommendation B1. Review the NRC computer security policy to remove redundant information and to incorporate the computing technology and activities underway in the NRC. Draft computer security directive (Management Directive 12.5).

LANL Recommendation B2. Establish a program to ensure periodic reviews and updates of the NRC computer security policy.

**Action Source:**

Division of Information Support Services

**Tracked By:**

WITS

**Action Description and Completion Milestone:**

The Codes and Standards staff rewrote the Directive portion of Management Directive 12.5 during FY92 and it has been reviewed by IRM and the Division of Security, Office of Administration. Handbook 12.5 is in the process of being developed by a contractor. The Handbook, itself, will require periodic review and update.

1. Contract awarded for Handbook development August 15, 1992.
2. Draft Handbook, for review and comment, due to NRC by April 30, 1993.
3. Final version of Handbook due to NRC by June 30, 1993.
4. The Handbook will be updated by NRC staff as needed.

Inspector General Category 5. The staffing and organizational placement of the computer security function were questionable.

LANL recommendation A.

Increase the computer security program staff to a level that ensures that all computing activities in the NRC receive the appropriate guidance, support, and oversight to ensure they comply with all NRC and federal requirements.

Relocate the Codes and Standards Section to an organization where it can operate without influence from the Division of Information Support Services or the Division of Computer and Telecommunications Services.

Action Source:

Director, IRM

Tracked By:

WITS

Action Description and Completion Milestone:

Organizational placement of the computer security function will be resolved when the overall IRM organization restructuring is resolved - September 30, 1993.