GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-282543

August 27, 1999

The Honorable Greta Joy Dicus
Chairman, Nuclear Regulatory Commission

Subject: Information Security: NRC's Computer Intrusion Detection Capabilities

Dear Ms. Dicus:

As part of our ongoing efforts to examine intrusion detection and response capabilities in the federal government, we initiated a review of the Nuclear Regulatory Commission's (NRC) policies and practices in this area. Our objectives were to review NRC's ability to prevent, detect, respond to, and report on incidents of computer intrusion and misuse. Our findings are based primarily on interviews with NRC's security managers, reviews of related documentation, and limited observation of NRC operations. We did not test NRC intrusion detection techniques and, therefore, cannot attest to their effectiveness in operation. Our work was performed from February 1999 through June 1999 in accordance with generally accepted government auditing standards.

We briefed officials from NRC's Office of the Chief Information Officer and Incident Response Operations on the results of our work on July 30, 1999. These officials agreed with our findings, noting that they were already considering some of the actions we suggested. This letter provides a high-level summary of that briefing. Our briefing charts are enclosed.

Overall, we found that NRC has instituted an integrated network and security management program to detect and respond to anomalies that may indicate computer and network intrusions and misuse for the systems that support its daily operations. Positive aspects of NRC's program include well-designed controls over user access, well-protected network boundaries to prevent intruders, and frequent testing of the network for security deficiencies. We found that NRC has (1) the capability to respond quickly to specific computer attacks once they have been detected and (2) a variety of tools that can be used to isolate, delay, confuse, and stop intruders. In addition, NRC's security managers regularly report on computer security incidents by providing monthly summary reports to management on the number and type of incidents. Further, we found that NRC's security managers communicate frequently with outside organizations in order to stay abreast of the latest hacker techniques—knowledge that helps them anticipate and defend against attacks.

We noted, however, three areas that pose a significant risk to systems supporting NRC operations:

- NRC's security management activities do not extend to the automated systems that NRC would rely on to facilitate an initial response to a nuclear emergency. As a result, NRC

would have to depend on other means of communication, which could diminish the agency's effectiveness.

- While NRC protects its network boundaries from intruders with a strong firewall, it places less emphasis on monitoring internal network activity. As a result, if an intruder successfully breached the firewall without detection, there is a risk that NRC would not promptly detect his or her activity on the system.

- NRC's oversight of its security specialists is somewhat limited. In order to carry out their responsibilities, these security specialists have been granted (1) broad access to NRC's systems and data and (2) use of powerful detection and response tools. Accordingly, it is important that NRC officials monitor their activities closely to ensure that their actions are in accordance with NRC policy and that the tools they use are fully documented.

Security risk management requires a continuing reassessment of risk, and reviews such as ours can serve as a useful means of highlighting risk factors that are significant enough to merit NRC management's ongoing attention. The enclosed briefing charts contain several suggested improvements for addressing the weaknesses we identified, including

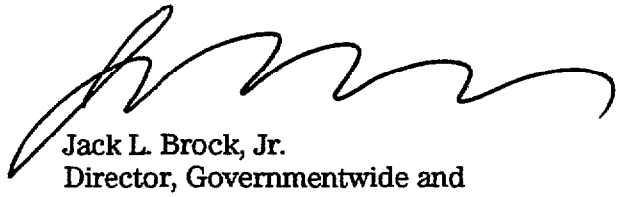
- extending network management and security controls to emergency systems,

- expanding monitoring to activity on key servers throughout the network, and

- providing additional management direction to and oversight of security specialists.

If you have any questions, please contact me at (202) 512-6240 or by e-mail at brockj.aimd@gao.gov or Jean Boltz, Assistant Director, at (202) 512-5247 or by e-mail at boltzj.aimd@gao.gov. Other major contributors to this work were William Wadsworth and Michael Gilmore.

Sincerely yours,



Jack L. Brock, Jr.
Director, Governmentwide and
Defense Information Systems

Enclosure

GAO

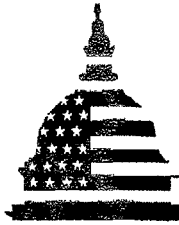
Accountability * Integrity * Reliability

NRC's Intrusion Detection and Response Capabilities

Strengthened Oversight Would Improve Established Practices

Objectives, Scope and Methodology

- Evaluate NRC's practices for
  - Preventing computer and network intrusion and misuse
  - Detecting anomalies that may indicate computer and network intrusion and misuse
  - Responding to incidents
  - Analyzing and reporting data.
- Methodology
  - Document reviews
  - Interviews with security specialists and managers
  - Limited observation
  - No testing of controls in operations
  - Followed generally accepted government auditing standards

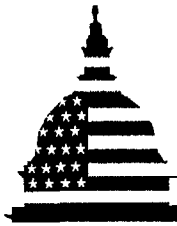


GAO

Accountability * Integrity * Reliability

Federal Requirements & Related Guidance

- OMB A-130, Appendix III
  - Protect agency information systems from unauthorized access and misuse.
  - Provide help to users when a security incident occurs.
  - Share information on vulnerabilities and threats.
- National Institute of Standards and Technology
  - Establishing a Computer Security Incident Response Capability (CSIRC), Special Pub 800-3, 11/91
  - An Introduction to Computer Security: The NIST Handbook, Special Pub 800-12, 10/95



Federal Requirements & Related Guidance (Con't)

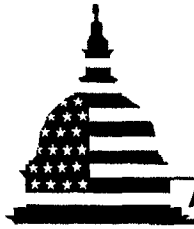
- Other guidance from
  - Carnegie-Mellon University's Software Engineering Institute (SEI), including the Computer Emergency Response Team/Coordination Center (CERT/CC)
  - Department of Energy's Computer Incident Advisory Capability (CIAC)

Intrusion Detection Program Elements

- Preventative controls
  - Protect systems, networks, and data from unauthorized access by establishing related policies and implementing physical and logical access controls.
- Detection capabilities
  - Collect and analyze data on system and network activity to detect potential problems.
  - Alert appropriate system and network managers.
- Incident response capabilities
  - Develop and communicate procedures to be taken when indications of suspicious activity are recognized.

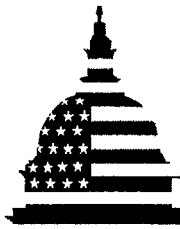
Intrusion Detection Program Elements (Con't)

- Long term analysis and reporting
  - Maintain and analyze records of incidents to identify trends and gain a more thorough understanding of risk factors.
  - Share information on vulnerabilities and threats with others.



NRC's Preventative Controls -- Strengths

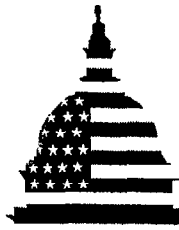
- Physical and logical access controls enforce NRC policies.
  - Policies describe allowed and prohibited network services and activities.
  - Controls limit user access.
  - Firewalls maintain network boundaries.
- Systematic tests identify network security deficiencies on an ongoing basis.
- Senior management participates in decisions regarding network security.



Preventative Controls -- Weaknesses

- Centralized network and security management activities do not encompass the systems that NRC would rely on to coordinate a response to nuclear power plant accidents.

- For networks covered, day-to-day management oversight of access control implementation is limited.



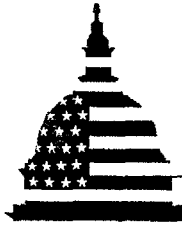
Detection--Strengths

- Integrated network and security management activities help ensure prompt detection and resolution of anomalies.
- Intrusion detection software is frequently adjusted to respond to specific threats.
- Real-time monitoring at key points connected to external networks facilitates prompt detection.
- Firewall and intrusion detection logs are continuously monitored.

Detection--Weaknesses

- Lack of emphasis on internal network activity monitoring increases the risk that inappropriate activity will go undetected.

- Location and settings of non-standard detection tools are not documented making
  - day-to-day oversight difficult
  - training of new personnel challenging.



GAO

Accountability * Integrity * Reliability

Response--Strengths

- A variety of tools are used to
  - trace and record intruder activity
  - isolate, delay, confuse, and stop intruders.
- Network managers are automatically notified as software detects anomalies.
- Some events prompt automatic responses.
- Countermeasures and alarm settings can be quickly adjusted based on specific intruder profiles and patterns.

Response--Weaknesses

- No emergency response team has been formally designated.
- Day-to-day management oversight of response actions is limited.

GAO

Accountability * Integrity * Reliability

Reporting--Strengths

- Monthly summary reports are provided to management on number and type of incidents experienced.

- Frequent communication is maintained with certain outside organizations--CERT/CC and others with knowledge of hacker techniques.

Reporting--Weaknesses

- Little coordination with other federal agencies.
- No long term trend analysis.

GAO

Accountability * Integrity * Reliability

Improvements to Consider

- Extend network management and security controls to emergency systems.
- Provide additional management direction to and oversight of security specialists.
- Document details such as location, version, and potential uses of software tools used for detecting, responding, and managing intrusions and computer misuse.

Improvements to Consider (Con't)

- Expand monitoring to activity on key servers throughout the network.
- Designate an emergency response team.
- Build relationships with other federal entities.
- Develop methods to perform trend analysis.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested