OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: May 17, 1995

TO: Chairman

FROM: Acting Inspector General

SUBJECT: Internet Penetration Analysis

As part of our on-going effort to ensure protection of the Commission's information resources, this office has recently completed an Internet Penetration Analysis. The purpose of this analysis was to evaluate the controls in place to prevent an unauthorized and potentially hostile penetration of the internal FCC network via the internet.

In general, our review indicates that the Associate Managing Director - Information Management (AMD-IM) has established effective controls over access to the internal FCC network from external sources. These controls include use of a firewall to manage data traffic, control over the use of potentially risky software utility products, and patches to commonly exploited software weaknesses. However, the review revealed four areas where improvements in control are recommended. The Office of Inspector General (OIG) is currently working with AMD-IM to address these areas. While the Commission cannot be assured that a skilled and deliberate "hacker" cannot penetrate internal FCC computers via the internet, we believe that AMD-IM has taken necessary and prudent measures to minimize this risk.

The Internet Penetration Report (OIG Report Number 95-3) is being maintained in a secure file area within the OIG. The report will not be disseminated due to the risk that sensitive information contained in the report could be used in a manner inconsistent with the normal operations of the Commission. If you would like to discuss this review, or require a copy of the report, please contact me at 418-0470.

H. Walker Feaster III

cc: Chief of Staff
Managing Director

REVIEW OBJECTIVE

The objective of this analysis was to attempt to penetrate the internal Federal Communications Commission (FCC) network from an external source through the internet, identify any potential weaknesses in the system security infrastructure, and document the controls in place to prevent a successful penetration.

REVIEW SCOPE

The scope of this analysis was limited to that of a technically skilled individual with internet access but no internal knowledge of the Commission or its computing environment. In addition, the scope was restricted to activities that were within the limitations of acceptable internet use policies (as proscribed by internet provider services) and all applicable federal, state, and local laws. It should be noted that a malicious attacker would not necessarily be concerned about such restrictions. Furthermore, the scope did not address exposures that could occur through acts of fraud or collusion.

The Office of Inspector General (OIG) selected the Certified Public Accounting firm of Coopers & Lybrand L.L.P. (C&L) through a competitive procurement to attempt to penetrate the FCC using the same readily available techniques an unauthorized party or "hacker" would employ. Officials in the office of the Associate Managing Director - Information Management (AMD-IM) were notified in advance and entered into a cooperative arrangement with the OIG to facilitate this project. As part of this agreement, AMD-IM personnel were involved in the planning of the penetration analysis and visited C&L's computer laboratory located in Floral Park, New York during testing. In return, AMD-IM officials agreed to ensure the integrity of the project by making only routine adjustments to the configuration of the FCC's internal operating system pending conclusion of the audit field work.

To conduct the review, computer professionals from C&L developed a custom methodology to guide the penetration efforts. The methodology employed was as follows:

- ○gathered information about FCC resources recognized on the internet (e.g., public host, firewall, etc.),

- ○manually probed available hosts to determine the existence of published security weaknesses and to identify specific accounts to target for "brute force" password attacks, and

- ○used readily available automated software "tools" to attack these resources.

Among the automated tools used in the review was a recently released product called Systems Administrator Tool for Analyzing Networks (SATAN). SATAN was developed as a security tool which systems administrators can use to identify particular vulnerabilities in their networks. However, once released into the public domain on April 7, 1995, SATAN became another tool which could be employed by hackers to attack systems.

BACKGROUND

In February 1994 the FCC established connectivity to the internet. The FCC internet connection supports three functions: (1) the ability to send and receive mail, (2) access to databases and files on other internet systems, and (3) the making of FCC information and data available to other internet users. Since it's implementation, internal and external use of the FCC connection has been heavy. The Commission has made hundreds of documents available for public review, provided extensive round by round coverage results of spectrum auction activities, and supported e-mail traffic of approximately 5000+ messages per day.

In response to the success of internet access, and as a result of increased customer demand, the FCC is currently pursuing various initiatives for expanding the Commission's use of the internet. Specific initiative items include posting engineering databases, enabling MOSAIC access from FCC workstations, and allowing access to FCC bulletin board systems through the internet. The total cost of these initiatives in AMD-IM's FY 1995 IRM budget is $1,325,000.

Although the opportunities afforded by the internet are numerous, the risks associated with connectivity can be significant. Reports of attacks on internet hosts are increasing and the level of sophistication associated with these attacks is also on the rise. Many individuals who have either been apprehended by law enforcement agencies, or have boasted of their exploits, have listed government agencies and Fortune 500 companies as prime attack goals. The nature of the work the FCC conducts, and the leadership role being taken by the Commission in the development of the information superhighway make the FCC host a likely target for attack. For this reason, it is especially important for the Commission to secure it's valuable and high-profile information.

REVIEW FINDINGS

Our initial attempts at penetration focused on the FCC's firewall. In the Commission's computing environment, a firewall is a computer used to manage traffic between the internet and the internal FCC network. A primary function of a firewall is to prevent unauthorized access to internal data. Based on the testing conducted, the audit team concluded that the FCC's firewall appeared to be properly configured (i.e., sensitive utilities were disabled, published weaknesses were patched, etc.).

Following unsuccessful efforts to compromise the FCC firewall, the focus of the attack shifted to the Commission's router and the public host that serves as the anonymous FTP, gopher, world wide web, and backup mail server. The intent of this approach was to obtain "root" access to the public host and launch a spoofing attack on the firewall (i.e., appearing to the firewall as an internal host). Although this objective was not met, concerns related to the configuration of the public host were identified. The OIG is working with representatives from AMD-IM to address these concerns. For purposes of security, the details of these issues are not detailed in this document.

Based upon the knowledge gained in this review, the OIG plans to continue to perform work in the computer security area. Projects are currently being formulated to ensure that the

Commission has developed adequate levels of internal controls to address the risks that reside in complex automated networks such as that being used by the Commission.