UNIX SECURITY

EXECUTIVE SUMMARY

Our audit of security practices over Unix-based systems found that those practices were for the most part reasonably effective. Some general issues (user training and password use, written procedures) will be addressed as the Commission takes corrective action on its material weakness in ADP security. We are making several specific recommendations, including updating network maps and periodically changing and validating root passwords.

Generally, the Office of Information Technology concurs with our findings and recommendations (see its comments, attached). The Office of the Executive Director provided informal comments. We have revised the report appropriately to reflect the comments.

SCOPE AND OBJECTIVES

Our objective was to evaluate the Commission's security practices over its Unix-based systems at the Data Center in Alexandria, Virginia. Among other procedures, we interviewed system administrators and security staff, reviewed selected documentation, and tested a judgment sample of 5 out of approximately 80 Unix systems.

We reviewed the application of software patches, documentation of server and network configuration, scripted programming practices, physical access controls for servers, development of security plans, and performance of periodic risk assessments. Our testing was limited by time constraints.

The audit was performed between February and April 1999, in accordance with generally accepted government auditing standards.

BACKGROUND

The Unix operating system is installed on approximately 80 servers throughout the Commission, performing security (firewall), database, and general application functions. Unix systems administration is performed at three locations within the Office of Information Technology (OIT) [1] :

[1] Except for the EDGAR system, which is performed by the EDGAR contractor (TRW, Inc.).

- the Systems Software Branch supports test and production environments for internal applications (except the Internet and Intranet),
- the Applications Development Team supports the Internet and Intranet; and
- the Security Group supports firewalls (security mechanisms controlling entry and exit to the network).

The Commission has reported ADP security as a material weakness since 1989. Formation of the Security Group (during OIT's recent reorganization), is one major step in addressing this weakness.

Currently, the Security Group consists of four employees. Its mission statement indicates that the Group is responsible for Commission systems and network security; prepares and coordinates security policy and procedures; and conducts security audits. While the Group is the focal point for security, it is a Commission-wide responsibility.

The Group maintains a sophisticated near-time intrusion and logging capability for entry and exit to the network. It has held training sessions for system administrators; conducted security posture assessments; and communicated various security deficiencies to system administrators. The Group has started to develop Security Plans for its systems, as required by the Computer Security Act of 1987.

It obtained approval in December 1998 for an administrative regulation that establishes an Information Technology Security Program. In addition, it has drafted technical bulletins providing security guidelines and requirements.

AUDIT RESULTS

Commission security practices over Unix-based systems for the most part are reasonably effective. Some needed improvements relate to the previously identified material weakness in ADP security (*e.g.*, security training, issuance of final security guidance), discussed in the Background section. We identified several improvements specifically relating to Unix security practices, as discussed below.

NETWORK MAPS

Network maps or diagrams provide a logical and physical view of the Commission's data networks. They show network types, server and host addresses, connections to external networks and other devices (such as hubs, routers, gateways and management devices), and the physical layout of buildings, devices and servers.

OIT's Network Engineering Group acknowledged that the maps are out-of-date, and in some respects do not accurately reflect the current network configuration. The Group indicated that resource constraints and other priorities kept them from updating the diagrams.

Network maps are an important control used for security evaluation, troubleshooting, network design, and training new staff.

Recommendation A

OIT should maintain current network configuration data, so logical and physical views of the Commission's networks can be readily developed when needed. As resources permit, it should update the Commission's network maps (including those supported by contractors, *e.g.*, EDGAR).

ROOT ACCESS CODES

Root access provides system administrators with unlimited authority over a computer's operating system. Because they provide superuser privileges, root access codes need to be secure, yet available when administrators are absent.

OIT stores root access codes for its systems in sealed, labeled envelopes in a safe. We examined these envelopes, and noted codes stored for systems no longer in use (*i.e.*, the RS6000 system), and for two departed system administrators. One had left the Commission, and one had been reassigned within OIT; both had the combination to the safe, which has not been changed.

Apparently, OIT has procedures for security and availability of access codes, but the procedures are unwritten and not uniformly followed. Invalid root access codes can cause significant delays, particularly if one has to rebuild the operating system.

Recommendation B

OIT should periodically validate its stored root access codes, and change the safe combination when system administrators depart. It should develop written procedures for storage of codes.

PASSWORDS

Based on our tests of five Unix systems (including EDGAR), password files were for the most part protected. Also, passwords were generally assigned to user accounts. We notified OIT and the EDGAR contractor of a few exceptions requiring corrective action.

Systems administrators informed us that root access passwords were not being periodically changed in some cases, potentially compromising passwords and system security over time. OIT management indicated that this issue will be covered in a password management bulletin, currently in draft.

Recommendation C

OIT should notify system administrators that root passwords should be periodically changed.

Recommendation D

OIT, in consultation with the Office of the Executive Director (OED), should finalize the password management bulletin. The bulletin should require root access passwords to be changed periodically (*e.g.*, every six months), and whenever a system administrator leaves.

PERFORMANCE PLANS

We reviewed the performance plans of four OIT system administrators. None of the plans included security as an element, even though administrators have significant security responsibilities. System administration is also performed by staff outside OIT, according to OIT.

Recommendation E

OIT should include security as an element (or as part of an element) in the performance plans of its system administrators.

Recommendation F

OIT, in consultation with OED and the Office of Administrative and Personnel Management, should ask offices with system administrators to consider including security as an element in their performance plans.