U.S. SECURITIES AND EXCHANGE COMMISSION

"We are the investor's advocate."
William O. Douglas
SEC Chairman, 1937-1939

PBX and Analog Lines Security Assessment

U.S. SECURITIES & EXCHANGE COMMISSION

March 31, 2000

Prepared by
Deloitte & Touche LLP
Enterprise Risk Services

1 Executive Summary

1.1 Overview

Deloitte & Touche LLP (D&T) was engaged to assist the Office of the Inspector General (OIG) of the Securities and Exchange Commission (SEC) in evaluating the effectiveness of security controls over their telecommunications infrastructure, consisting of the Private Branch Exchange (PBX) and analog telephone lines (fax machines, computer dial-up, etc).

The overall objective of the review was to determine the degree of protection the SEC's existing security controls provide their telecommunications system against "hostile" threats from the public and from within the SEC. The objective was accomplished by performing a two-phased assessment: 1) Manual evaluation of the PBX and 2) Automated and manual evaluation of all identified analog telephone lines.

The scope of the review included the SEC headquarters in Washington, DC, and the Operations Center (and Annex) in Alexandria, VA. Testing activities were performed between September 21 and November 19, 1999 at the SEC Headquarters located in Washington, DC and external D&T locations. Analog telephone line testing was limited to the telephone numbers provided by Bell Atlantic and the SEC's security group. All testing was coordinated through Nelson Egbert, Office of the Inspector General.

1.2 Testing Approach

The D&T project team performed controlled tests to gather information about potential vulnerabilities and exposures within SEC's telecommunications environment. While the objective of these tests was to simulate potential threats faced by SEC, limitations existed relative to testing. For instance, ethical considerations and legal consequences prevented D&T from exploring telecommunications systems of third parties that provide telephone or data connectivity to SEC. As such, D&T confined testing to only those telephone numbers and PBX equipment owned by SEC. D&T realizes that real world attackers may not allow these limitations to prevent them from attempting a variety of other attack methods. After evaluating the results of testing performed, areas of concern and corresponding recommendations to mitigate potential risks were documented (Refer to Section 2 – Detailed Testing).

1.2.1 Private Branch Exchange (PBX)

To evaluate the effectiveness of security controls over the PBX environment the D&T project team:

- Interviewed telecommunications personnel and reviewed relevant documentation in order to understand how the PBX is configured and operated at the SEC.
- Generated and reviewed on-line reports (with the assistance of telecommunications personnel) to confirm configuration parameters and security control settings identified during the interview process.
- Toured the data center where the PBX equipment is located to observe the physical security controls.

1.2.2 Analog Telephone Lines

To evaluate the effectiveness of security controls over the analog telephone lines the D&T project team:

- Obtained an informal inventory of analog telephone lines that had been developed by the Information Security department.
- Obtained a formal inventory of analog telephone lines from Bell Atlantic, generated from billing records.
- Interviewed telecommunications personnel to identify any telephone exchanges that may not be assigned or that are assigned to unauthorized individuals.
- Utilized a war dialer in an attempt to establish a connection via each analog telephone number identified in the known universe of telephone numbers.
  - Telephone numbers with modem tones were further investigated to identify what type of system was connected to (computer, FAX machine, router, terminal server, etc.)
  - Attempts were made to gain access into systems using basic methods (e.g., common User IDs and passwords, known exploits). NOTE: Brute force methods were not employed for this review due to scope limitations and the specific requirement of the OIG to not disrupt legitimate business activity (e.g., locking out users).

1.3 Summary of Assessment

The results of test procedures performed revealed that many effective controls and procedures exist to assist in safeguarding the PBX and analog telephone lines. For instance:

- The PBX system is configured to disable the communications port after three unsuccessful login attempts.
- The PBX room is physically secure within the data center in the basement of the SEC headquarters building. Access to the data center is controlled via card access. Access to the PBX room is through a separate combination lock (combination is only known by telecommunications personnel).
- The PBX utilizes redundant communication circuits with separate vendors in order to eliminate a single point of failure.
- The PBX has built-in redundancy in the form of multiple control units.
- The majority of systems that can be connected to via analog telephone lines utilize an authentication mechanism to prevent an attacker from gaining easy access into the SEC's internal network.

However, numerous areas were identified where security controls and procedures require strengthening to ensure the integrity of the PBX and of internal systems. Specific areas of concern include:

- Certain security controls appear to be deficient in protecting the PBX from remote access connections including:

Area	Issue	OAPM Response

Auditing & Monitoring	**Periodic reports are not generated and/or reviewed in order to detect unusual or unauthorized activity.**	**Reports are not generated due to an IG/OGC request to shut down the SMDR sub-system that generates the documentation, that could be subject to FOIA requests, that could be utilized to track Investigators activities during an investigation.**
Access Control	**Although the PBX provides the capability to assign granularity of access to various functions of the PBX the SEC only uses a single level of security that provides privileged access to all system users.**	**The PBX does have the ability of establishing levels of password protection. However since there are only three Telecommunications Staff at the SEC and the work is accomplished in a cooperative manner, with one or more technicians handling various levels of each job, it has been determined that one password to permit access provides sufficient system security.**

- The project team identified numerous SEC managed (by OAPM and/or OIT) analog telephone lines that are connected directly to computer systems. Many of these systems provide a direct login prompt and do not provide strong authentication mechanisms that would minimize the potential for unauthorized access. Specifically, the project team obtained privileged access to the PBX Management Console via dial-up using PC AnyWhere with no requirement to authenticate (i.e., no user ID or password required). ***Once we notified the telecommunications group of this issue additional security controls were implemented and appear to be effective (Refer to section 2.2 for additional detail).***

- There does not appear to be an effective mechanism to effectively manage the maintenance and revocation of analog telephone lines. Without a clear understanding of who is responsible for an analog line and what the authorized purpose for the line's use, there is a potential for misuse that may not be detected in a timely manner.

  Currently, the OAPM is responsible for assigning ownership of an analog line. This assignment is contingent on an E-mail request to OAPM and approval process from OIT. Once the analog line is assigned there is no periodic review nor is there documentation as to the specific owner of the line or its intended purpose. Individuals within the OAPM and OIT appear to have informal knowledge of who owns and is responsible for a significant number of lines, however there does not appear to be an effective process to:
  - Reconcile existing analog lines to individual, group, or function in a timely manner
  - Determine if an analog log is no longer in use
  - Revoke/Disable access for analog line owners that leave the organization or no longer require access to the line.

1.4 Conclusion

Generally, the effectiveness of security and control over telecommunication lines leading into the internal network infrastructure components is dependent, to a great extent, on the existence of consistent and effective security administration and monitoring practices (e.g., system and user management, change management, security management, intrusion detection, etc.) strong

authentication and authorization controls. The absence of any one of these may result in increased risk of compromise to the integrity of the entire network infrastructure and application systems. As such, it is imperative that robust change management practices, periodic software integrity checking, effective management oversight, auditing and intrusion detection features, and strong authentication and authorization capabilities exist.

It was noted during this review that PBX and analog telephone line security administration, monitoring and access control practices require strengthening to assist in mitigating the risks posed to electronic information resources. To address these deficiencies, the Telecommunications and Information Security groups should work closely together to develop a comprehensive security architecture. Recommendations to consider include:

- Develop and implement a formalized process to manage the distribution and use of analog telephone lines. The process should include maintaining:
  - An accurate inventory of line numbers
  - Knowledge of who is assigned responsibility for each line
  - An understanding of what each line will be used for

  Additionally, the process should also clearly articulate management responsibilities for all departments involved with the assignment and use of analog lines (e.g., telecommunications, corporate security, human resources, etc.).

- Develop and implement a comprehensive monitoring process to detect fraudulent or unauthorized telephone activity. This may include the use of an automated software package that continuously monitors and tracks PBX activity or possibly involve reliance upon a manual process that requires the generation and review of daily, weekly, monthly reports to detect unusual or unauthorized activities.

OAPM Response
The SEC feels proper protection is provided, but will continue to be aware of the potential for intruder access and improve controls as determined necessary.

- Develop comprehensive telecommunications security policies and baseline standards to establish an environment that adequately safeguards telecommunications resources. The policies and standards should address, among other things, the following:
  - Strong authentication
  - Access control
  - Security administration
  - Auditing, and monitoring

OAPM Response
The SEC feels proper protection is provided, but will continue to be aware of the potential for intruder access and improve controls as determined necessary.

- Perform periodic assessments of telecommunications security to determine compliance with security policies and standards and to evaluate the effectiveness of controls in safeguarding telecommunications and other resources.

OAPM Response
The SEC feels proper protection is provided, but will continue to be aware of the potential for intruder access and improve controls as determined necessary.

- Establish more effective authentication controls to restrict unauthorized access to information resources via analog lines and via the PBX.

OAPM Response
The SEC feels proper protection is provided, but will continue to be aware of the potential for intruder access and improve controls as determined necessary.

Lastly, the management should be aware that due to the nature of the telecommunication and network technology utilized at the SEC and the regularity in which new vulnerabilities are identified with information technology, results of test procedures performed may not have revealed all potential vulnerabilities.