Treasury Checks

The Scenario

An auditor was reviewing a list of Department of Defense system generated check disbursements and observed a reoccurring pattern of payments to persons with similar last names that were not agency employees and/or vendors. All of the check disbursements were properly authorized; however, numerous disbursements were made late in the evenings or on weekends when the office was closed. The auditor examined system records and discovered that Employee A or Employee B processed all of the suspect payments. The auditor decided to conduct interviews with these employees to determine why the transactions occurred when the office was officially closed. Interviewees provided the following information:

- The employees could not recall processing or authorizing any of the suspect payments.

- Both employees stated that they did not work on week ends and left the office at five o'clock each day to meet their carpools.

- The last names of several check recipients were the same as Employee C, who also worked in the same department. In addition, some of the checks were sent to states where Employee C's relatives lived.

- Both Employee A and B admitted to sharing their system passwords with Employee C because they were friends, despite knowing that they violated agency security policies. Further, they often left their computers unattended while they were logged on to walk to the cafeteria for coffee.

Auditor review of the phony check payments disclosed that Employee C made fraudulent payments, totaling over $200,000, to his relatives during the past four years.

General Comments / Lessons Learned. Computer security remains a challenge throughout the Federal government. Although employees can cause security breeches by sharing passwords and/or leaving computers unattended, another recent concern for Federal agencies is lost or stolen lap top computers and thumb drives. Equipment that is lost or stolen may contain sensitive information such as an employee's name, social security number, or date of birth. When conducting information technology audits, it is important for auditors to be alert to password protection controls and agency policies to safeguard employee's personal information. Further, each Federal agency is responsible for promptly reporting compromises of sensitive information.

FRAUD INDICATORS

- **A pattern of payments to unauthorized persons or vendors.**
- **Disbursements frequently occur outside of official business hours or during weekends.**
- **The same employees are responsible for processing suspect payments.**
- **Evidence of personal relationships with unauthorized check recipients.**
- **Employees share system passwords.**
- **Computers are unattended while employees remain logged on the system.**