**MEMORANDUM – 2 MINUTE BRIEFING 3**

**TO:** CASEY G. CEGIELSKI, PH. D, CISSP, CISA, CRISC

**FROM:** CENSORED

**DATE:** 9/23/19

Your firm will need three types of access controls for security purposes: administrative, technical (logical) and physical access controls. Administrative controls are policies/procedures used by upper management, such as security clearances, background checks, etc. Technical (logical) access controls are security measures that go directly on the technology, such as anti-virus software, firewalls, password protection, etc. Finally, physical access control are the security aspects that are physically in place, like locks, alarms, or even badge systems.

There are plenty of physical access control systems available on the Internet, but some important ones to setup would be CCTV cameras, fire extinguishers, alarms, and tightly locked doors that require keycard access (so that no systems are accessible without the proper identification). Some technical access control systems that could be implemented are system logs, anti-virus software, firewalls, password protection, tape backups (for the CCTV cameras), or even keystroke monitoring (if the risk from employees is significant). Some administrative access controls that could be put in place would be policies, user registration procedures, job rotation, separation of duties, supervision, security clearances, and background checks.

I would suggest implementing these access controls the heaviest within the “high security” area (i.e., the area containing the printing area, IT Infrastructure, and shipping dock). The technical controls should be used on the machine that accesses the electronic data, and CCTV cameras should be implemented in the area alongside tape backups as a result of this. The physical access controls are all important so that no one can access this area physically without showing up in a log or on camera, and so they should all be implemented. The administrative access controls are necessary for any employees that work within the “high security” area, so that security is not at risk due to any employees.