**MEMORANDUM – 2 MINUTE BRIEFING 7**

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

**FROM:** CENSORED

**DATE:** 10/28/19

The main concerns for the application are whether it has availability, integrity, and confidentiality; without these, the application is not secure. Availability is a measure of how available the application is; in this case, it should always be available during business hours for management to use. This is also a measure of how much processing power it takes, how much data it stores, the resources it uses (bandwidth, memory, disk space, etc.); if it uses too much system power, it will not always be available and could result in system errors.

Integrity refers to ensuring the authenticity of information, i.e., that the information was not altered in any way and that the source of it is genuine. The main part of this application that would affect integrity would be the Database Communications Software, as it is the program that must form the trust relationship between the database and the application. If this part of the application were to malfunction or be implemented incorrectly, as a result, incorrect user data could be returned from the database, which would have a drastic overall negative result on the business.

Confidentiality refers to protecting information from being accessed by unauthorized parties; so, regarding this application, it would be confidential if no 3rd party could access the data being sent through it. 3rd parties could access the application through backdoors, viruses, or other malware (direct loss) or it could be lost through unauthorized disclosure (indirect loss). The application would need to be strengthened so that it could not be accessed by any person that is not authorized.