**MEMORANDUM – 2 MINUTE BRIEFING 8**

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

**FROM:** CENSORED

**DATE:** 11/11/19

I think implementing remote access in a bank is a terrifying idea. For one, there are multitudes of attacks for remote access enabled systems that must be handled (usually more than with a physical connection); second, there will be a lot of other software/tools that must be used with remote access enabled systems to help keep things secure. To generally keep a remote access system secure, there must be a policy on how to access/use it correctly, a justification process for remote access users that comes yearly, an audit process that is designed for all remote access systems to determine if they are safe, use 2FA and VPNs to access the remote systems, and keep some form of antivirus software on each machine alongside a general firewall for use with the bank.

The most important thing to set up for remote access to work is the SSH or SSH2 protocol (NOTE: It is integral to use SSH or SSH2 instead of Telnet or something similar for remote access, for security reasons). SSH is important to use because it provides a layer of encryption over the sent packets; this helps provide confidentiality and integrity when sending data back and forth. SSH will provide support for host/user authentication, data compression, and the aforementioned confidentiality and integrity that we desire for remote communications. It is also integral to use a Virtual Private Network (VPN) to help with tunneling and encryption. A VPN will help protect private traffic over an untrusted network, such as a home network that an employee might be using to connect to one of the remote machines. If everything listed here is implemented correctly and tested rigorously, then remote access in a bank could be acceptable; however, if it is not moderated and maintained correctly, this could become the Single Point of Failure for the business.