**MEMORANDUM – 2 MINUTE BRIEFING 2**

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

**FROM:** CENSORED

**DATE:** 9/4/19

Some information security regulations that might apply to your business are the Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act (GLB), the Electronic Fund Transfer Act (EFT), the Fair and Accurate Credit Transaction Act (FACTA), the Federal Information Security Management Act (FISMA), and Title 21 of the Code of Federal Regulations (21 CFR Part 11). These are just the broadly applicable and industry-specific regulations, you may want to do some further research into Key State Regulations for yourselves.

The SOX act is a regulation that was designed to protect investors and the public. It is a set of rules and regulations that define audit requirements and the records businesses should store and for how long. This act would be highly important to your business, because you need to know how long to normally store customer/employee data for in the systems and what records are important to keep. The PCI DSS is a set of requirements for enhancing security of payment customer account data. This is also incredibly integral to your business because anybody handling sensitive credit card data must explicitly conform to these requirements to protect customer information and assets.

The GLB act is yet another set of provisions that protect consumers’ personal financial information. Any financial institution (such as yourselves) is required to follow these provisions, so you may want to look into the 3 parts of this act: The Financial Privacy Rule, the Safeguards Rule, and the Pretexting Provisions. The EFT act is only important to you if you have a banking application for electronic fund transfers. Since this is most likely the case (as you must have ATM transfers or pre-auth transfers or something similar to this) you must observe the rules and regulations of this act as well.

FACTA is an amendment to the Fair Credit Reporting Act and is necessary for customers to avoid identity theft. These rules and regulations will help with storing customer information, privacy, and limiting sharing of that information. FISMA is a regulation that will require your business to implement some form of security for all information systems so that information is not mishandled, stolen, or destroyed. The last set of regulations that you must be compliant with is 21 CFR Part 11, which imposes guidelines on electronic records and electronic signatures.