In today's world, the ever-changing social media and digital environments require professionals to have a solid foundation in law and ethics. As a future InfoSec professional, it will be required of you. Your role will be critical in helping to control the organization's liability for privacy and security risks.

Prior to beginning this assignment, view the video "2-1 Introduction to Topic 2," located in the topic Resources.

In a 1,500- to 1,750-word summary, address each item below to demonstrate how one would build a reliable, ethical, and legal information system that businesses and consumers can trust.

**Part 1**

As the computer forensics industry is growing, consider how the methods for handling computer crimes differ from traditional methods. Make sure to address the following:

* What is the purpose of digital forensics?
* Explain why it is important for any organization to sustain a permanent digital forensics team.
* In digital forensics, must all investigations follow the same basic methodology? Justify your rationale and explain the steps involved in this methodology.
* Concerning digital forensics, list the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data. **Note:** This information can be presented in a table or chart.
* Examine the U.S. federal laws and legal issues associated with cyber threats, especially cyber types such as fraud and financial cybercrimes.
* Using the organization you selected in Topic 1, discuss the legal rights of the organization to perform forensic investigations on personal mobile devices that are part of your BYOD policy.

**Part 2**

In many situations, multiple levels of government must work in partnership when ensuring security compliance. As a cybersecurity professional, research the following:

* Describe the federal, state, and local cyber defense partners/structures.
* Examine the laws, regulations, and standards that organizations use to align with government requirements around cybersecurity best practices within their industry.
* Explain federal laws and authorities, including the Computer Security Act, Sarbanes – Oxley, Gramm – Leach – Bliley, Privacy (COPPA) HIPAA / FERPA, USA Patriot Act, Americans with Disabilities Act, Section 508, and other Federal laws and regulations.

**Part 3**

For each scenario, identify the applicable law(s) it would fall under and describe how the type of legal dispute (civil, criminal, or private) affects the evidence used to resolve it. **Note:** This information can be presented in a table.

* Transmission of underage photographs to various email addresses in California, Arizona, and Colorado
* Colonial Pipeline Hack
* Victim's identity used to open a new account
* Bank fraud/scam
* A firm's credit card records are stolen

**Part 4**

When providing information assurance, a sound defense strategy does not only look at the legal aspects but also the ethical abuses of abilities on the job.

* There are three main categories of unethical behavior that organizations must seek to minimize: ignorance, accident, and intent. From your research and your professional/personal experience, provide examples of each category and best practices for how to prevent such activities from happening.
* What happens when a job task borders on unethical from your personal viewpoint? Is your response to the issue any different than what you discussed above? What behaviors/tasks would an organization find acceptable where your personal viewpoint may not? Select 2–3 scenarios and discuss how you would address them from a Christian worldview. Consider Matthew 18:15–18. How could you apply this to a workplace scenario?
* Refer to the ISACA code of conduct. Describe the responsibilities related to the handling of data as it pertains to legal, ethical codes of conduct, and/or agency auditing issues, frameworks, and best practices.
* InfoSec professionals are under increasing pressure to provide access to information/data without sacrificing security or usability. Explore the challenges of balancing security and usability and what results if there is a lack of balance between the two.
* Describe how you would integrate information assurance and security requirements into an organization's processes and practices.
* Examine the ethical considerations of ethics and cyberspace, ethical issues, property, availability, rights of others, respect and principles of community, resource use, allocation, and abuse, censorship, ethics-based decision tools, and cybersecurity and social responsibility.

Prepare this assignment according to the guidelines found in the APA Style Guide, located in the Student Success Center.

This assignment uses a rubric. Please review the rubric prior to beginning the assignment to become familiar with the expectations for successful completion.

You are required to submit this assignment to LopesWrite. A link to the LopesWrite technical support articles is located in Class Resources if you need assistance