**C844 TASK 2 Steps to Success notes**

**Many students tend to confuse the Federal/State regulations for cybersecurity with standards for cybersecurity. Regulations are mandated by the state of government. Standards are usually chosen by the sanctioning body in charge of the network accreditation process. Please review the example below if you have questions schedule an appointment with your assigned Course Instructor.**

**Federal Government Regulations**

[**Health Insurance Portability and Accountability Act**](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act)**(HIPAA),** the **1999**[**Gramm-Leach-Bliley Act**](https://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act), and the 2002 [Homeland Security Act](https://en.wikipedia.org/wiki/Homeland_Security_Act), which included the [**Federal Information Security Management Act**](https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act)**(FISMA)**. The three regulations mandate that healthcare organizations, financial institutions, and federal agencies should protect their systems and information.[[3]](https://en.wikipedia.org/wiki/Cyber-security_regulation#endnote_heiman) For example, FISMA, which applies to every government agency, "requires the development and implementation of mandatory policies, principles, standards, and guidelines on information security." However, the regulations do not address numerous computer-related industries, such as [Internet Service Providers](https://en.wikipedia.org/wiki/Internet_Service_Provider) (ISPs) and software companies.[[4]](https://en.wikipedia.org/wiki/Cyber-security_regulation#endnote_lemos) Furthermore, the regulations do not specify what cybersecurity measures must be implemented and require only a "reasonable" level of security.

**State Regulations**

[California](https://en.wikipedia.org/wiki/California) passed the **Notice of Security Breach Act**, which requires that any company that maintains personal information of California citizens and has a security breach must disclose the details of the event. Personal information includes name, [social security number](https://en.wikipedia.org/wiki/Social_security_number), driver's license number, [credit card number](https://en.wikipedia.org/wiki/Payment_card_number) or financial information

The [California State Legislature](https://en.wikipedia.org/wiki/California_State_Legislature) passed **California Assembly Bill** 1950, which also applies to businesses that own or maintain personal information for California residents. The regulation dictates for businesses to maintain a reasonable level of security and that they required security practices also extend to business partners.[[9]](https://en.wikipedia.org/wiki/Cyber-security_regulation#endnote_rasmussen) The regulation is an improvement on the federal standard because it expands the number of firms required to maintain an acceptable standard of cybersecurity. However, like the federal legislation, it requires a "reasonable" level of cybersecurity, which leaves much room for interpretation until case law is established.

**VS**

**Cyber Security Standards**

Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization.This environment includes users themselves, networks, devices, all software, processes, the information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.

The principal objective is to reduce the risks, including the prevention or mitigation of [cyber-attacks](https://en.wikipedia.org/wiki/Cyber-attack). These published materials consist of collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies.

**ISO/IEC 27001**, part of the growing [**ISO/IEC 27000** family of standards](https://en.wikipedia.org/wiki/ISO/IEC_27000-series), is an [information security management system](https://en.wikipedia.org/wiki/Information_security_management_system) (ISMS) standard, of which the last revision was published in October 2013 by the [International Organization for Standardization](https://en.wikipedia.org/wiki/International_Organization_for_Standardization) (ISO) and the [International Electrotechnical Commission](https://en.wikipedia.org/wiki/International_Electrotechnical_Commission) (IEC). Its full name is *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems*

[***National Institute of Standards and Technology***](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology)*:* The [**NIST** Cybersecurity Framework](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework) (NIST CSF) "provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." It is intended to help private sector organizations that provide [critical infrastructure](https://en.wikipedia.org/wiki/Critical_infrastructure) with guidance on how to protect it, along with relevant protections for [privacy](https://en.wikipedia.org/wiki/Privacy) and [civil liberties](https://en.wikipedia.org/wiki/Civil_liberties).