Security Design Engineering

CMSC 420

Security 10 Domains of Knowledge

- **Access Control** – a collection of mechanisms that work together to create security architecture to protect the assets of the information system.
- **Telecommunications and Network Security** – discusses network structures, transmission methods, transport formats and security measures used to provide availability, integrity and confidentiality.
- **Information Security Governance and Risk Management** – the identification of an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines.
- **Software Development Security** – refers to the controls that are included within systems and applications software and the steps used in their development.
- **Cryptography** – the principles, means and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- **Security Architecture and Design** – contains the concepts, principles, structures and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity and availability.
- **Operations Security** – used to identify the controls over hardware, media and the operators with access privileges to any of these resources.
- **Business Continuity and Disaster Recovery Planning** – addresses the preservation of the business in the face of major disruptions to normal business operations.
- **Legal, Regulations, Investigations and Compliance** – addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed and methods to gather evidence.
- **Physical (Environmental) Security** – addresses the threats, vulnerabilities and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information.

Legal Regulations

Federal Information Security Management Act of 2002 (FISMA)

- **Purpose:**
  1. Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;
  2. Recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;
  3. Provide for development and maintenance of minimum controls required to protect Federal information and information systems;
  4. Provide a mechanism for improved oversight of Federal agency information security programs;
  5. Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and
  6. Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.
- **Defined in the NIST SP800 documents**