**Criminal law**- mainly concerned with law enforcement agencies. Crimes such as murder theft assault robbery arson. Penalties (fines, community service, incarceration). Federal and state are elected representatives

**Civil/tort law-** dispute between individuals and organizations. Such as contract problems, real estate transactions employment matters- Penalties- financial penalties

**Administrative law** – used by executive branch of the government – Govt agencies. Covers policies, procedures, regulations- ex immigration polices

**Common law**- it is based on previous interpretation of law, developed in England. Community orals and expectations. Role of judges.

**Customary law-** mainly with personal conduct and patterns of behavior- penalty is monetary fine

**Religious law-** based on religious belief and of the region

**Mixed law -**2 or more legal systems used together. Consists of civil and common law

**Code law-** most common in Europe. Written law- Rule based law

Both criminal and civil laws are embodied in the **United States Code (USC).**

Administrative law is published in the **Code of Federal Regulations, often referred to as the CFR**.

These intangible assets are collectively referred to as intellectual property

**Computer fraud and abuse act**

Congress first enacted computer crime law as part of the Comprehensive Crime Control

Act (CCCA) of 1984,

The major provisions

of the act are that it is a crime to perform the following:

■ Access classified information or financial information in a federal system without

authorization or in excess of authorized privileges

■ Access a computer used exclusively by the federal government without authorization

■ Use a federal computer to perpetrate a fraud (unless the only object of the fraud was to

gain use of the computer itself)

■ Cause malicious damage to a federal computer system in excess of $1,000

■ Modify medical records in a computer when doing so impairs or may impair the examination,

diagnosis, treatment, or medical care of an individual

■ Traffic in computer passwords if the trafficking affects interstate commerce or involves

a federal computer system

in 1986 the changed the scope in CFAA.

Any computer used exclusively by the U.S. government

■ Any computer used exclusively by a financial institution

■ Any computer used by the government or a financial institution when the offense

impedes the ability of the government or institution to use that system

■ Any combination of computers used to commit an offense when they are not all located

in the same state

**1994 CFAA Amendments**

Outlawed the creation of any type of malicious code that might cause damage to a

computer system

■ Modified the CFAA to cover any computer used in interstate commerce rather than

just “federal interest” computer systems

■ Allowed for the imprisonment of offenders, regardless of whether they actually

intended to cause damage

■ Provided legal authority for the victims of computer crime to pursue civil action to gain

injunctive relief and compensation for damages

**Computer Security Act of 1987**

four main purposes of the act:

■ To give the National Institute of Standards and Technology (NIST) responsibility for

developing standards and guidelines for federal computer systems. For this purpose,

NIST draws on the technical advice and assistance (including work products) of the

National Security Agency where appropriate.

■ To provide for the enactment of such standards and guidelines.

■ To require the establishment of security plans by all operators of federal computer

systems that contain sensitive information.

■ To require mandatory periodic training for all people involved in management, use, or

operation of federal computer systems that contain sensitive information.

It also divided responsibility for computer security among two federal agencies. The National Security Agency (NSA), which formerly had authority over all computer security issues, retained authority over classified systems, but NIST gained responsibility for securing all other federal government systems. NIST

130 Chapter 4 ■ Laws, Regulations, and Compliance produces the 800 series of Special Publications related to computer security in the federal government.

**Federal Sentencing Guidelines**

***prudent man rule****,* which requires senior executives to take personal responsibility for ensuring the due care that ordinary, prudent individuals would exercise in the same situation. This rule, developed in the realm of fiscal responsibility, now applies to information security as well.

**National Information Infrastructure Protection Act of 1996**

**Paperwork Reduction Act of 1995** Information collections include forms, interviews, record‐keeping requirements, and a wide variety of other things.

**Government Information Security Reform Act of 2000(GISRA)**

To provide for development and maintenance of minimum controls required to protect federal information and information systems

**Federal Information Security Management Act-**The National Institute of Standards and Technology (NIST), responsible for developing the FISMA implementation guidelines, outlines the following elements of an effective information security program

Periodic assessments of risk , Policies and procedures that are based on risk assessments, Security awareness training, Periodic testing and evaluation of the effectiveness of information security policies , A process for planning, implementing, evaluating, and documenting remedial actions. Procedures for detecting, reporting, and responding to security incidents.

**Copyrights and the Digital Millennium Copyright Act -**Literary works, Musical works Dramatic works

Pantomimes and choreographic works■ Pictorial, graphical, and sculptural works■ Motion pictures and their audiovisual works■ Sound recordings■ Architectural works

**Trademark** which are words, slogans, and logos used to identify a company and its products or

Services.

***Patents***protect the **intellectual property rights** of inventors. They provide a period of **20 years** during which the inventor is granted exclusive rights to use the invention. The invention must be new. The invention must be useful. The invention must not be obvious

**Trade Secrets -**Many companies have intellectual property that is critical to their business and

significant damage would result if it were disclosed to competitors and/or the public—in other

words, trade secrets*.*

**The Uniform Computer Information Transactions Act (UCITA**) is a federal law designed for adoption by each of the 50 states to provide a common framework for the conduct of computer‐related business transactions

**The Electronic Communications PrivacyAct (ECPA)** makes it a crime to invade the electronic privacy of an individual

**Communications Assistance for Law Enforcement Act (CALEA) of 1994** amended the Electronic Communications Privacy Act of 1986. CALEA requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology in use

**HITECH** Act. This law updated many of HIPAA’s privacy and security requirements and was implemented through the HIPAA Omnibus Rule in 2013.

**Children’s Online Privacy Protection Act of 1998-**Websites must have a privacy notice that clearly states the types of information they collect. Parents must give verifiable consent to the collection of information about children younger than the age of 13

**Gramm‐Leach‐Bliley Act of 1999 -**Banks, insurance companies, and credit providers.

**Family Educational Rights and Privacy Act -**Parents/students have the right to inspect any educational records maintained by the institution on the student.

■ Parents/students have the right to request correction of records they think are erroneous

and the right to include a statement in the records contesting anything that is not corrected.

■ Schools may not release personal information from student records without written

consent, except under certain circumstances.

**European Union Privacy Law -**in place for protecting personal data processed by information systems.

**Notice** They must inform individuals of what information they collect about them and

how the information will be used. **Choice** They must allow individuals to opt out if the information will be used for any other purpose or shared with a third party. For information considered sensitive, an opt‐in policy must be used.

**Onward Transfer** Organizations can share data only with other organizations that comply with the safe harbor principles. **Access Individuals** must be granted access to any records kept containing their **personal information**. Security Proper mechanisms must be in place to protect data against loss, misuse, and unauthorized disclosure. **Data Integrity** Organizations must take steps to ensure the reliability of the information they maintain. Enforcement Organizations must make a dispute resolution process available to individuals and provide certifications to regulatory agencies that they comply with the safe harbor provisions..

**Import/Export**

The federal government recognizes that the very same computers and encryption technologies that drive the Internet and e‐commerce can be extremely powerful tools in the hands of a military force. For this reason, during the Cold War, the government developed a complex set of regulations governing the export of sensitive hardware and software products to other nations. The regulations include the management of trans‐border data flow of new technologies, intellectual property, and personally identifying information. Until recently, it was very difficult to export high‐powered computers outside the United States, except to a select handful of allied nations. The controls on exporting encryption software were even more severe, rendering it virtually impossible to export any encryption technology outside the country. Recent changes in federal policy have relaxed these restrictions and provided for more open commerce.

.