Outline: Lecture 18

Date: May 26, 2011
Topic: Government Standards and Regulations

1. Federal laws
   a. Sarbanes Oxley Act (SOX)
   b. Federal Information Security Management Act (FISMA)
   c. Gramm-Leach-Bliley Act (GLBA)
2. State laws: California
   a. Notice of Security Breach Act
   b. Electronic Recordation Delivery Act and supporting regulations
3. Regulations
4. Certifying computers
   a. Department of Defense Trusted Computer Security Evaluation Criteria
   b. Common Criteria
   c. FIPS 140-3: Security Requirements for Cryptographic Modules (Draft)
   d. Certification process; modifications such as RAMP
5. Certifying and licensing people
   a. Common bodies of knowledge
   b. Security society certifications: CISSP ($(ISC)^2$)
   c. Training institute certifications: GIAC (SANS)
   d. Commercial firms: Cisco's CNA, Microsoft's MCSD, MCSE
6. Protecting systems
   a. FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
   b. ISO 9000
   c. NIST SP-800 series (lots of them on securing systems and servers)
7. Other issues
   a. Procurement
   b. Supply chain issues
8. Other standards
   a. Voluntary Voting System Guidelines (VVSG)
   b. Payment Card Industry Data Security Standard (PCI DSS)
   c. Secure Electronic Transaction (SET)