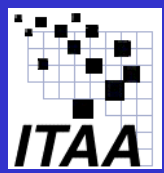
Law, Regulation and National Cyber Security: An Overview

Presented to: Information Security and Privacy Advisory Board
September 14, 2006

Greg Garcia, Vice President, Information Security
Information Technology Association of America



Existing Laws, Regulations and Guidance

- **National Infrastructure Protection Plan, July 2006;** Lays the framework for industry government partnership in critical infrastructure protection and cyber security

- **Office of Management and Budget, Memo to Agencies, June 2006:** Outlines requirements for protection of sensitive agency information, using guidance documents developed by the National Institute of Standards and Technology: 1) FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004; 2) NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005; and 3) NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006.

Existing Laws (continued)

- **Energy Policy Act (EPACT), 2005**: Introduced Federal Energy Regulatory Commission penalty enforcement of industry-developed (North American Electric Reliability Council) cyber security standards for electric utilities.

- **Federal Trade Commission Settlement with CardSystems**: FTC's proposed consent order will require CardSystems to implement a comprehensive information security program and obtain audits by an independent third-party security professional every other year for 20 years.

ITAA

Existing Laws (continued)

- **Federal Trade Commission Rulings on BJ's Wholesalers and DSW Shoes, 2005**: Held that companies not meeting certain minimal security practices are liable for "unfair trade practices".

- **Clinger-Cohen 1996, as amended 2004**: Requires agencies to implement sound management practices in the acquisition and use of information technology, including information security systems

- **HSPD-12, 2004**: Policy for a common identification standard for federal employees and contractors.

ITAA

Existing Laws (continued)

- **HSPD-7 2003**: Establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

- **CA 1386**: Requires entities doing business in the state of California to notify consumers when their personal data has been lost or stolen due to a security breach of an information system.

- **National Strategy to Secure Cyber Space, February 2003:** Lays the foundation for a national five-part strategy involving: 1) cyber security response system; 2) threat and vulnerability reduction program; 3) awareness and training; 4) government security; and 5) national security and international cooperation.

ITAA

Existing Laws (continued)

- **FISMA 2002:** requires each agency to inventory its major computer systems, to identify and provide appropriate security protections, and to develop, document, and implement an agency-wide information security program.
- **Sarbanes Oxley, 2002**: Requires a company to provide an internal control report attesting to the adequacy of the internal control structure and procedures for financial reporting. The internal control report must also contain an assessment of the effectiveness of the internal control structures and procedures.
- **Cyber Security R&D Act 2002**: authorizes funding for computer and network security research and development and research fellowship programs

ITAA

Existing Laws (continued)

- **Homeland Security Act, 2002**: Authorizes DOJ research in tools and techniques that facilitate investigative and forensic work related to computer crimes. Also authorizes the Undersecretary of Science and Technology of the Department of Homeland Security, when establishing university research centers, to consider universities with nationally recognized programs in information security.

- **Patriot Act 2001**: Authorizes a national network of electronic crime task forces for the purpose of improving computer crime forensics and prosecuting electronic crimes, including potential attacks against critical infrastructure and financial payment systems.

ITAA

Existing Laws (continued)

- **Gramm Leach Bliley 1999**: Requires financial institutions to protect the security and confidentiality of their customers' nonpublic personal information.
- **HIPAA, 1996**: protects employees' health insurance coverage when they change or lose their jobs and provides standards for patient health, administrative and financial data interchange.
- **National Security Directive 42 (NSD-42), 1990**. NSD-42 established the Committee on National Security Systems (CNSS), an interagency committee chaired by the Department of Defense. Directs the CNSS to provide system security guidance for national security systems to executive departments and agencies.

ITAA

Existing Laws (continued)

- **Computer Security Act 1987**: Gives NIST responsibility for developing and promulgating standards for the implementation of security for Federal, non-classified information systems. Created ISPAB.
- **Electronic Communications Privacy Act 1986**: Lays ground-rules for investigating computer crimes.
- **Computer Fraud and Abuse Act 1984**: Makes certain acts associated with the unauthorized access to computers a federal crime.

ITAA

Recent Cyber Security Bills

- **Putnam Draft**- proposed that publicly traded U.S. corporations would have to certify that they have conducted an annual computer security audit

- **Data Breach Notification Bills-**outlines when government and the private sector must notify the public about cyber security breaches that compromise confidential information

- **H.R. 4127** T*he Data Accountability and Trust Act*: Energy and Commerce Committee
- **H.R. 3997** *The Financial Data Protection: Financial Services Committee*
- **H.R. 5318** *Cyber-Security Enhancement and Consumer Data Protection: Judiciary Cmte*
- **S. 1789** *Personal Data Privacy and Security Act*: Judiciary Committee
- **S. 1326** *Notification of Risk to Personal Data Act*: Judiciary Committee
- **S. 1408** *Identity Theft Protection: Commerce Committee*

ITAA

Gaps and Tensions in our Cyber Security Profile

- Systems and Policies- governance
- Personnel
- Technology
- Standards and Best Practices
- Incentives and Liability

ITAA

Why Regulating Cyber Security is so Hard

- Technology is Dynamic; law is static
- No one-size-fits-all solution for systems and enterprises with widely varying security requirements

ITAA

What Government Can Do

- Law Enforcement Funding
- Research and development funding
- International coordination
- Better Federal procurement
- Partnership with the private sector

ITAA

What Industry is Doing

- Sector Coordinating Councils
- Information Sharing and Analysis Centers
- Partnership for Critical Infrastructure Security
- National Cyber Security Alliance
- National Cyber Security Partnership

ITAA

To Follow Up...

Greg Garcia
Vice President,
Information Security
ITAA
703-284-5357
Ggarcia@itaa.org