

Compliance

- **What** = Compliance for purposes of this discussion is the overarching guidance established as Federal & State Statutes; Federal Regulations, Directives, Instructions, Guidelines, Policies, & Memoranda; and Executive Orders.
- **Why** = Most of us have aspirations of promotion, or at least avoidance of demotion. Are opposed to the idea of financial punitive judgments against ourselves, and the organizations we work for, and have a strong desire to maintain and continue our employment.
- **Value** = We get to keep our jobs because we still have a organization to work for, since they are more secure, compliant, available, and ready to carry out mission objectives
- **Methods** = adherence to guidance as mandated by statute or guidance from higher organizational authority.

Compliance Cont

- So is Compliance good, or bad?!?!?!
 - Remember that I'm not above a trick question!!!!
- We shall see.
 - Slavish adherence (DoD Gold Disk)
 - Cogent adherence using mitigation factors where and when needed to mitigate an accepted risk.

Compliance Cont.

- Federal statutes:
 - HIPAA (Health Insurance Portability & Accountability Act)
 - FISMA (Federal Information Security Management Act)
 - Clinger/Cohen (Major Automated Information Systems) acquisition
 - Sarbanes/Oxley (Financial constraints)
- State Statutes:
 - Texas, Massachusetts, South Carolina, Florida, Georgia, Alaska, Tennessee, and Colorado are proposing to forbid the use of technology that conceals, “the existence or place of origin or destination of any communication.”
 - Good, Bad, what do you think?!?!?!?!?

Compliance Cont.

- What about Proxy Servers, Firewalls, Security Routers, and Virtual IPs
 - Depending on the legal language, all of these could be deemed inappropriate
 - What about Freedom of Information Act requests if this law is passed without careful scrutiny.
 - Are businesses subject to FOIA???? Do you know?!?!?!?
- State of Virginia HB 2271 Computer & Digital Forensic Services

Compliance Cont

- Organizational regulations, directives, instructions, etc.
- DoD 8500 series
- NIST Special Publications (e.g. SP 800-53)
- HSL/Presidential Directives
 - Local HSL policies created in conjunction with FEMA (e.g. Local CACs)
 - HSPD 5, HSPD 12, HSPD 13

Compliance Cont

- **HSPD - 12**

- There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification

Compliance Cont

- HSPD – 5

- To prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies, the United States Government shall establish a single, comprehensive approach to domestic incident management. The objective of the United States Government is to ensure that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management. In these efforts, with regard to domestic incidents, the United States Government treats crisis management and consequence management as a single, integrated function, rather than as two separate functions

Compliance Cont

- HSPD – 13
- The security of the Maritime Domain is a global issue. The United States, in cooperation with our allies and friends around the world and our State, local, and private sector partners, will work to ensure that lawful private and public activities in the Maritime Domain are protected against attack and criminal and otherwise unlawful or hostile exploitation. These efforts are critical to global economic stability and growth and are vital to the interests of the United States.

Compliance Cont

- Executive Orders (Directional authority across organizational boundaries)
- PS PREP
 - The Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep) is mandated by Title IX of the *Implementing Recommendations of the 9/11 Commission Act of 2007 (the Act.)* Congress directed the Department of Homeland Security (DHS) to develop and implement a voluntary program of accreditation and certification of private entities using standards adopted by DHS that promote private sector preparedness, including disaster management, emergency management and business continuity programs. The purpose of the PS-Prep Program is to enhance nationwide resilience in an all-hazards environment by encouraging private sector preparedness. The program will provide a mechanism by which a private sector entity-a company, facility, not-for-profit corporation, hospital, stadium, university, etc.-may be certified by an accredited third party establishing that the private sector entity conforms to one or more preparedness standards adopted by DHS.
 - Impacts for businesses? Your business??
 - Who are those independent auditors and who certifies them?

Compliance cont.

- Take away!!!
 - What is critical and what isn't?
 - You must do your homework to be prepared!
 - What local laws can affect you and your business?
 - What federal laws can affect you and your business?
 - As an IA, Risk, and/ Continuity Manager you must know:
 - What is ground truth, and how does it affect me!!!!