



Technology and Privacy Management

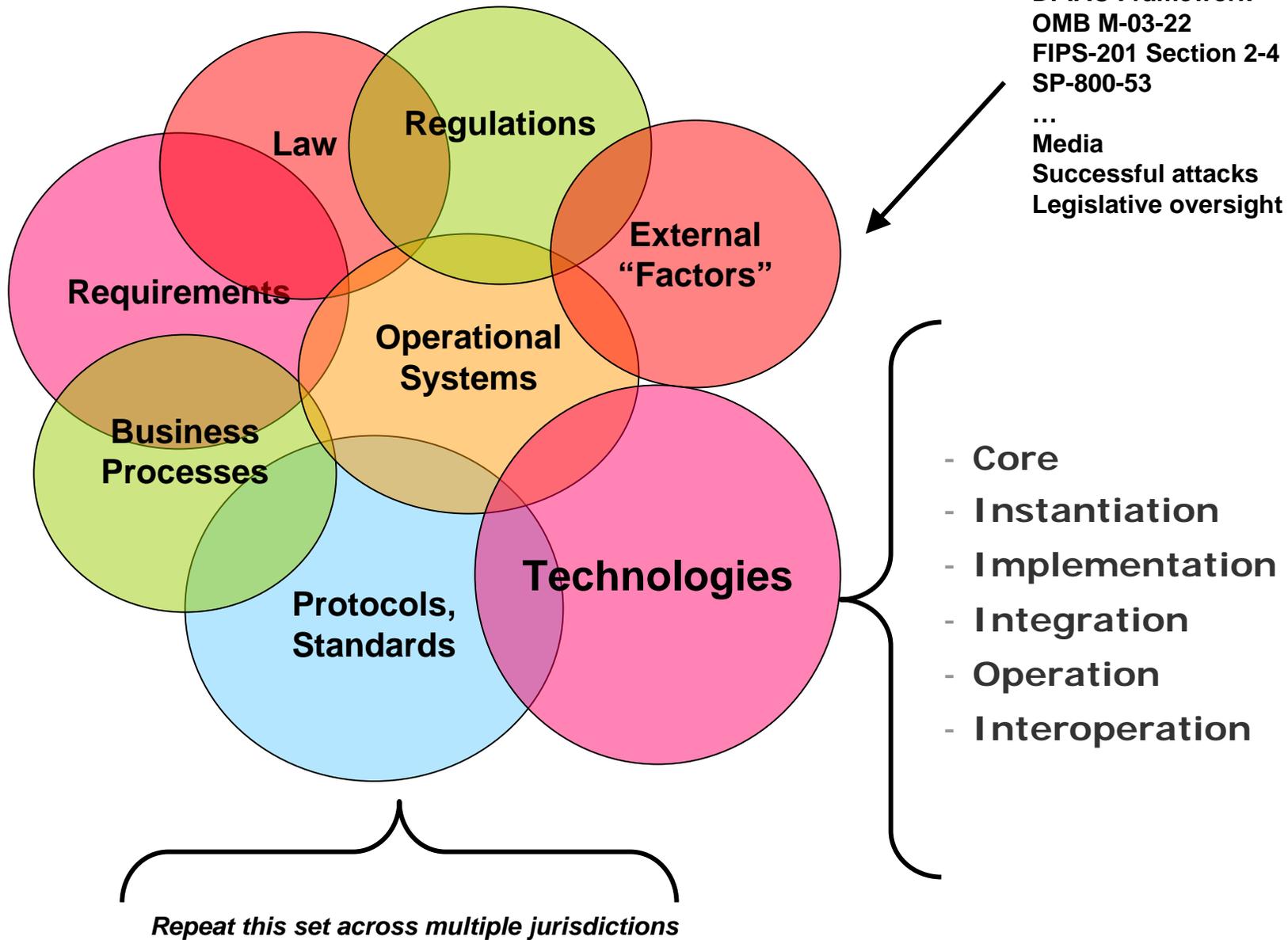
John T. Sabo, CISSP
Director, Security and Privacy Initiatives
CA

Information Security and Privacy Advisory Board
September 15, 2006

Work Underway

Privacy Framework - International Security Trust and Privacy Alliance (ISTPA – www.istpa.org)

Information Privacy "Environment"

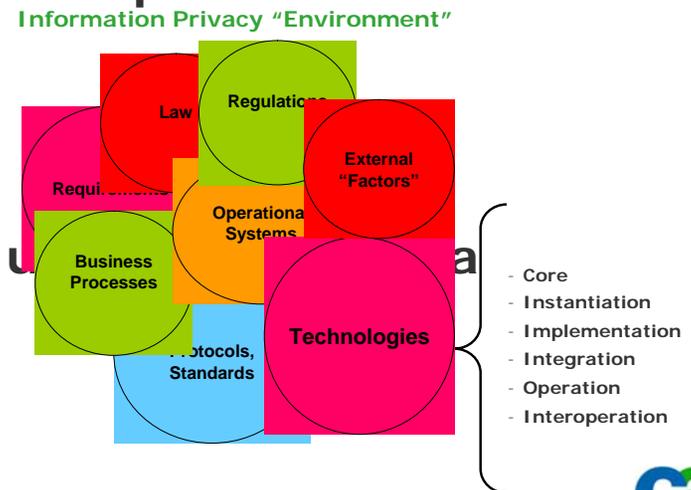


Rigor Needed to Improve Information Privacy Operations, Management, and Compliance

- Technology will change
- New technologies will be invented and used
- Use will change
- “Environment” will change
- ...everything will change
- Therefore...address technology in structured way

Possible Approach to Mapping Technology

- Model the Technology Set (agree on how to structure “left column” of matrix)
- Define Core technology (relational dbms, RFID Chip, search engine, Internet, etc.)
 - Instantiation (particular core technology as delivered, installed)
 - Implementation (its use in a particular system or application)
 - Integration (its operational relationship to other technologies)
 - Operation (its actual use)
 - Interoperation with Other Sets
- Prioritize analysis – start with most u mining? Externally-collected data?)
- Test the Model



Discussion

John T. Sabo
john.t.sabo@ca.com

DHS Data privacy and Integrity Advisory Committee Evaluation Framework for Programs, Technologies, Applications

- **Step 1. Scope**

- Description of the program, technology, or application.

- **Step 2. Legal Basis**

- Description of the legal authority and legal limits for program, technology, or application.

- **Step 3. Risk Management: Efficacy**

- Results of their risk analysis and estimation of the efficacy of the program, technology, or application.

- **Step 4. Effects on Privacy Interests**

- Analysis of the privacy interests implicated by the program, technology, or application – privacy, fairness, liberty, data security.

- **Step 5. Recommendations**

- Assessment of the results of the first four steps and recommendations on the program, technology, or application.

Privacy Impact Assessments

- M-03-22 - OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- Section 208 of the E-Government Act of 2002 - privacy impact assessments for electronic information systems and collections addresses:
 - **what information is to be collected**
 - **why the information is being collected**
 - **intended use of the information**
 - **with whom the information will be shared**
 - **what opportunities individuals have to decline to provide information**
 - **how the information will be secured**
 - **whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a**
- Not Addressed:
 - **Individual access**
 - **Amendment of records**
 - **Maintain accounting of all disclosures of information**
 - **Assure records are accurate, relevant, timely, complete**
 - **Notice**
 - **Integrated systems**