

# Working to Secure the Future

MBA, MISMO and SISAC

**John D. Simon**

Vice President, Strategic Initiatives, eHereNow  
Chair, MISMO Information Security Workgroup

# Disclaimers & Credits

- **Disclaimers**

- » The information in this presentation is educational in nature.
- » General information about legal developments is included, but it is not legal advice.
- » Consult an attorney for any specific legal questions.

- **Credits**

- » To Nancee Gorenstein, Mike Fleck, Dick Taylor and the other ISWG members that contributed so much time and effort to the year-long effort to develop the ISWG White Paper, *Identifying and Safeguarding Personal Information: Recommended Guidelines and Practices*.
- » To Yuriy Dzambasow and his employer, A&N Associates, Inc., who contributed to MISMO their methodology for developing a comprehensive and complete information assurance solution.
- » To Robert Schlecht, the MBA staff liaison to the ISWG, who has provided essential insight, support and guidance.



# Historical Perspective

- **MBA Board of Directors Technology Steering Committee** – [www.MBAA.org](http://www.MBAA.org)
  - » October, 2005
    - Protecting Personal Information: The Good, the Bad, the Ugly
      - > <http://www.MortgageBankers.org/documents/NewsLink/Misc/102705security.pdf>
  
- **MISMO: Information Security Work Group** – [www.MISMO.org](http://www.MISMO.org)
  - » MBA wholly-owned, nonprofit subsidiary
  - » February, 2006
    - Identifying and Safeguarding Personal Information: Recommended Guidelines and Practices
      - > <http://www.MISMO.org/files/mismo/InformationSecurityWhitepaper.pdf>
  
- **SISAC (Secure Identity Services Accreditation Corporation)** – [www.SISAC.org](http://www.SISAC.org)
  - » MBA wholly-owned, nonprofit subsidiary
  - » Establishing a mortgage industry PKI “federation”
  - » December, 2003
    - KPMG: first accredited auditor for identity management compliance
  - » January, 2004
    - VeriSign: first accredited issuer of digital credentials



# State Privacy Breach Notification Legislation

	AR	CA	CT	DE	FL	GA	IL	IN	LA	ME	MN	MT	NJ	NY	NV	NC	ND	RI	TN	TX	WA
<b>NOTIFICATION EXCLUSIONS</b>																					
Encrypted Data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Harm Not Likely	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Confidentiality & Integrity	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓
<b>APPLICABLE ORGANIZATIONS</b>																					
Information Brokers Only	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
State Agencies Only	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Financial & HIPPA Excluded	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
<b>APPLICABLE MEDIA</b>																					
Computerized	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
All	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
<b>PERSONAL INFORMATION</b>																					
Name / Initials	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Social Security Number	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DL# / State ID#	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Acct # / PIN / Password	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Date of Birth	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
Mother's Maiden Name	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
Digital Signatures	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
Biometric Data	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
Fingerprints	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
Medical Information	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Employment Information	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗



## Federal Privacy Breach Notification Legislation

- H.R. 3997 - Financial Data Protection Act of 2005
  - » Key Provisions
    - Preempts state legislation.
    - Standardizes data protection standards.
    - Requires policies and procedures to protect personal information.
    - Requires immediate investigation of any reasonable potential breach.
    - If consumers may be harmed or inconvenienced by breach, law enforcement, regulator(s), and other businesses in transaction chain must be notified.
    - If financial fraud against consumers may result from breach, consumers must be notified via mail and must be offered free credit monitoring.
    - Consumers who have been a victim of identity theft may freeze their credit reports.
    - FTC to maintain a public list of breaches that resulted in consumer notification within last twelve months.
    - FTC to provide voluntarily supplied information on race and ethnicity of victims of data theft and account fraud.
    - Credit monitoring activities are exempted from the Credit Repair Organization Act.



## **Federal Privacy Breach Notification Legislation (continued)**

- **H.R. 3997 - Financial Data Protection Act of 2005**

- » Current Status

- Approved by House Financial Services Committee on March 16, 2006.
- Strongly opposed by consumer groups and privacy advocates.
  - > Would preempt stronger state laws already in place.
  - > Would give companies too much discretion in disclosing breaches.
  - > Would not regulate activities of data aggregators such as ChoicePoint.
  - > Would prevent consumers from freezing their credit reports prior to identity theft (consumers would first have to be victims of identity theft).

- » Next Steps

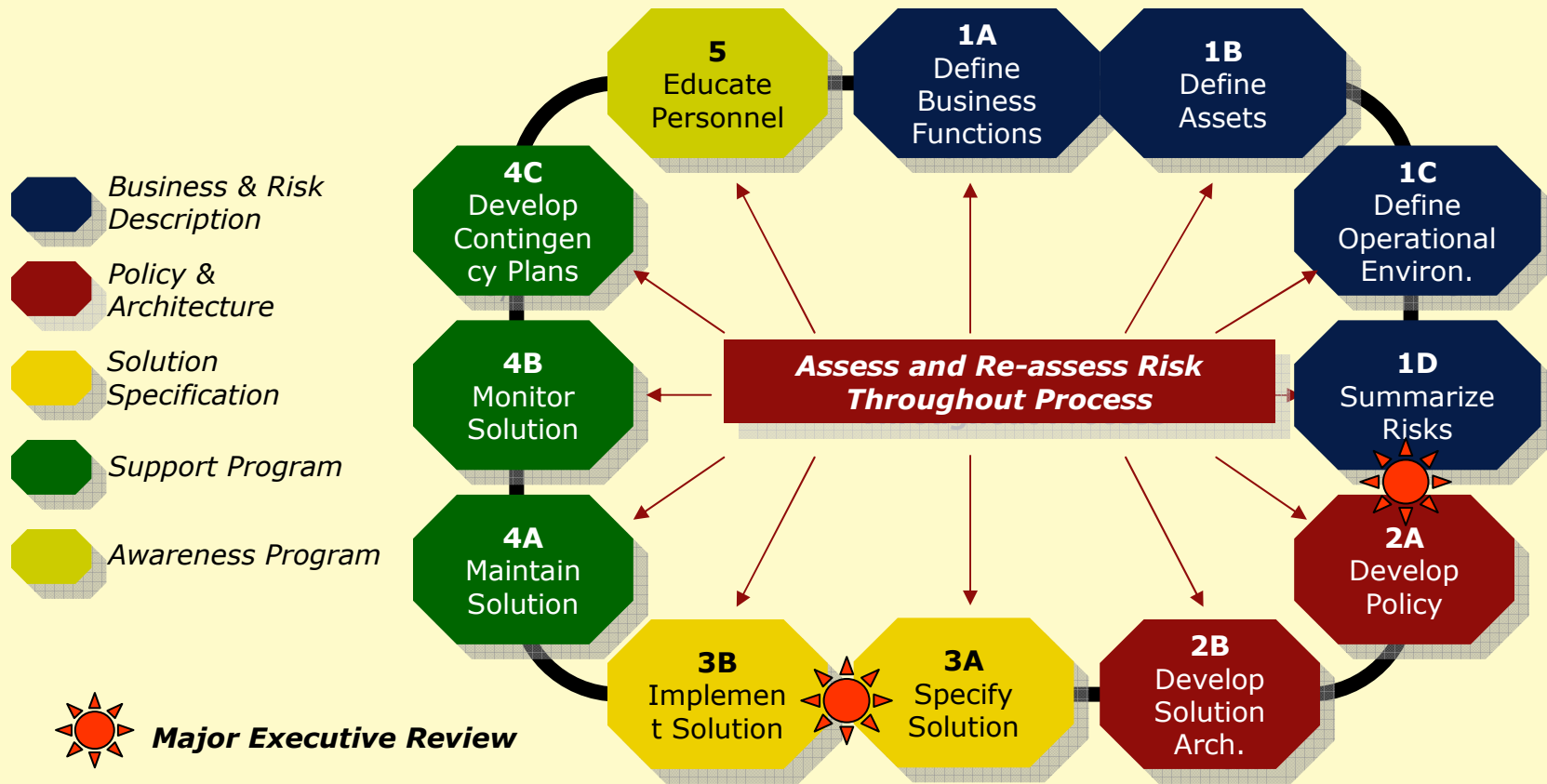
- Full House must vote.
- Companion Senate bill required.



## Implementing a Phased-in Security Program



# MISMO Five Step Model in Practice



## **Best-In-Class Approaches to Data Security**

- **Adhere to Authoritative Guidelines and Practices**

- » ANSI (American National Standards Institute)
- » BITS (fka Banking Industry Technology Secretariat)
- » CIO Executive Council
- » COPP (California Office of Privacy Protection)
- » IEC (International Electrotechnical Commission)
- » IETF (Internet Engineering Task Force)
- » ISACA (Information Systems Audit and Control Association)
- » ISO (International Standards Organization)
- » NIST (National Institute of Science and Technology)
- » SEI (Software Engineering Institute)
- » SISAC (Secure Identity Services Accreditation Corporation)



## **Best-In-Class Approaches to Data Security**

- **Incident Response Plan**

- » Recommendations and are based on:
  - California Office of Privacy Protection (COPP)
  - NIST SP 800-61
- » At a minimum, incident response plans should include:
  - Monitoring and notification
  - Impact assessment of the security incident
  - Internal notification procedures
  - External notification procedures
  - Follow-up assessment to mitigate the security incident from recurring
  - Updates to incident response plans



# Best-In-Class Approaches to Data Security

- **Incident Response Plan (continued)**

- » Should also identify specific individuals responsible for plan execution and management
  - Central Incident Response Team (one team)
    - > Handles incidents throughout an organization
    - > Effective for small organizations and for large organizations with centralized IT
  - Distributed Incident Response Teams (multiple teams)
    - > Each handles incidents for a particular logical or physical segment of the organization
    - > Effective for large organizations or organizations with major distributed computing resources
    - > Teams should be part of a centralized entity so that response is consistent across the organization
  - Coordinating Team
    - > Provides guidance and advice to distributed teams without authority over them
    - > Improves consistency and information sharing among teams



## **Mortgage Industry PKI Federation Business Drivers**

- **Sarbanes–Oxley (SOX)**
  - » Strengthen Corporate financial governance; restore investor confidence
  - » Applies to public companies; adhered to by an increasing number of private companies
- **Gramm-Leach-Bliley Act (GLBA)**
  - » Protect privacy rights of customers; ensure security of non-public personal information
  - » Applies to Financial Services industry and many of their service providers
- **State Privacy Breach Notification Legislation (Enacted and Pending)**
  - » Define non-public personal information (PI); stipulate conditions for notifications
  - » Applies to most public, private and governmental organizations
- **Federal Privacy Breach Notification Legislation (Pending)**
  - » Preempts state legislation
  - » Applies to most public, private and governmental organizations



# A Look Toward the Future

- Labeling of Personal Information in MISMO Logical Data Dictionary
- Security and Privacy sections in MISMO Implementation Guides
- Standard security practices for Web Services and AS2
- Periodic updates to ISWG White Paper and State Legislation Matrix
- Drive to establish mortgage industry PKI federation via SISAC

