

Interagency Advisory Board

Meeting Agenda, December 7, 2009

1. **Opening Remarks**
2. **FICAM Segment Architecture & PIV Issuance** (*Carol Bales, OMB*)
3. **ABA Working Group on Identity** (*Tom Smedinghoff*)
4. **F/ERO Repository** (*Elisa Cruz/FEMA*)
5. **Correlation of SP 800-53 rev. 3/ FIPS 201/ SP 800-63/ PIV-I/ FICAM Segment Architecture** (*Matt Scholl/Bill Macgregor, NIST*)
6. **Use of Optional Form Factor to Meet PIV-I** (*Andrew Sheedy, ActivIdentity*)
7. **Closing Remarks**

Cyber Security: Interoperability

How to Achieve Federal and Non-Federal Trust

Interagency Advisory Board (IAB)



Presentation By:

Elisa Cruz

Chief Information Security Officer

Federal Emergency Management Agency

7 December 2009

Agenda

- Background
- Cyber War
- Headlines
- Gartner “Top Ten”
- Business & Security Strategy
- Identity & Access Management
- FIPS 201
- System Accreditation
- PIV-I
- FRAC & ERO
- Interoperability & Trust
- Security Technologies/Cost
- Barriers to Federal Reliance
- Future Trends
- Summary
- A closing Note/
- Questions

Background

CYBER-ATTACKS

on our nation's federal, military and commercial computers have grown a lot more sophisticated since the days of the lone hacker targeting a system's defenses just for the thrill of it.

Your business is at risk,

if you do not have a core Cyber Security strategy

Cyber War

- **1990's:** Early Cyber War Warnings
- **2000/01:** *'Houston, We have a Problem' in Cyber Space*
- **2002:** Letter to President Bush urges immediate Cyber Security Initiatives to Protect Critical Infrastructure;
- **2003:** Cyber Security transferred from White House to Department of Homeland Security
- **2004/06:** Cyber Security "Second-tiered" to Global War on Terrorism
- **2007/09:** New Focus Towards Cyber Security began; Reflected in Budget, Personnel, Policy, Resources, Standards
- **2008/09:** PIV-I and NIMS
- **2009:** White House Stands Up Cyber Security Czar

Cyber Security Headlines

- *'Russia, 3 and 0, in Cyber Warfare Attacks'*
- *'Chinese Hackers Penetrate White House Computers'*
- *'Hacker attacks in US linked to Chinese Military'*
- *'Cyberscams On the Uptick in Economic Downturn'*
- *'Experts question fallout from new Monster and USAJOBS hack'*
- *'MySpace: 90,000 Sex Offenders Purged From Web Site'*
- *Cybercriminals targeting Twitter "trending topics"*

Cyber War Rages On - Are You Ready?

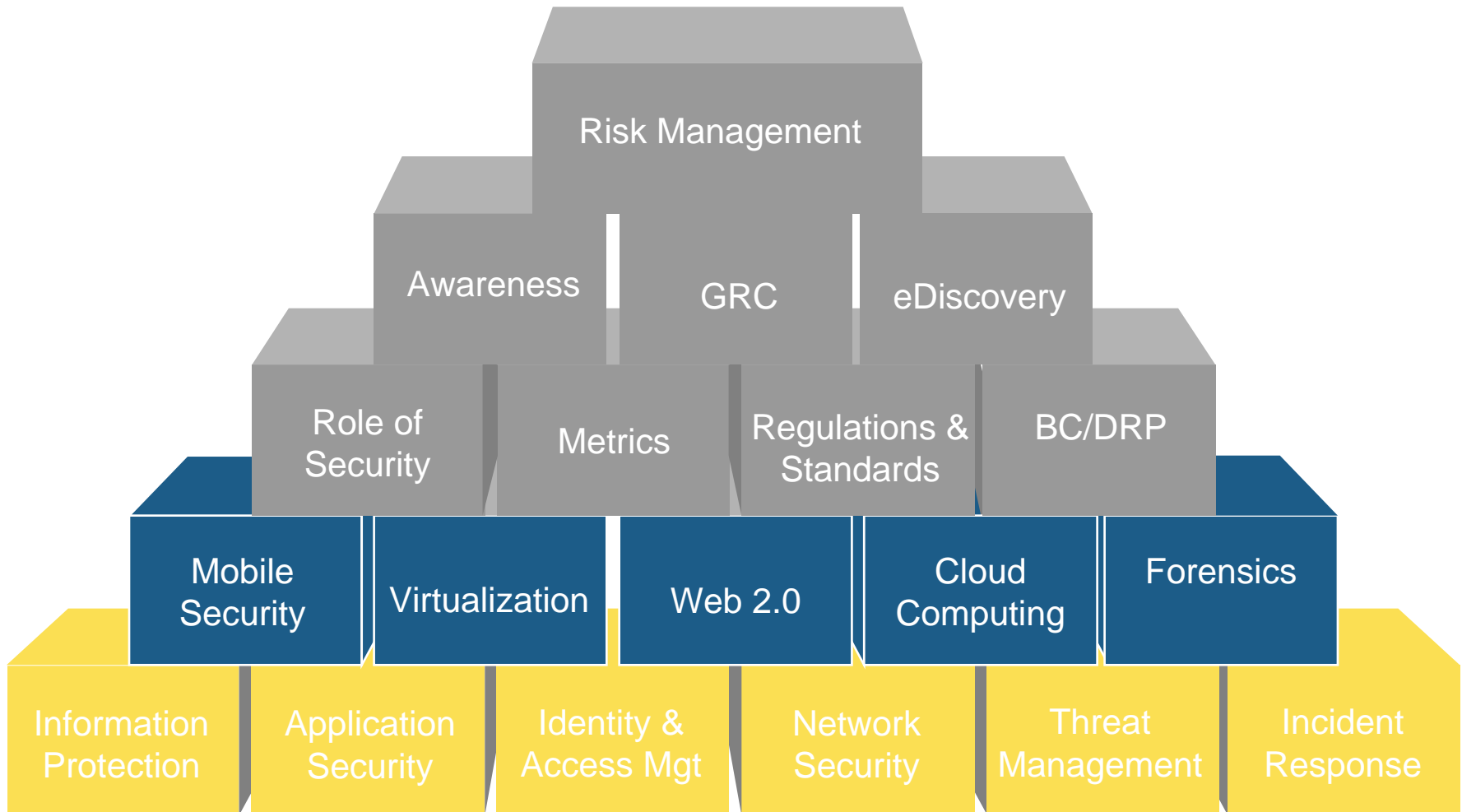
KAL
THE ECONOMIST
London
ENGLAND



Gartner's Top 10 for 2009 and Beyond

- **Social software / networking**
- **Virtualization**
- **Cloud computing**
- **Servers (beyond blades)**
- **Web oriented architectures**
- **Enterprise mash ups**
- **Specialized systems**
- **Unified communications**
- **Business intelligence**
- **Green IT**

Business & Security Strategy



Identity and Access Management

- Federal CIO Council established Information Security & Identity Management Committee (ISIMC)
- ISIMC oversees Cyber Security and Identity Management
- Four sub-committees
- Identity, Credential, and Access Management Subcommittee (ICAM)
- Six working groups
- Enables trust; reduces burdens; achieves and enhances interoperability

FIPS 201 Helps

- Specifies the architecture and technical requirements for a common identification standard
- Contains two major sections
- Minimum requirements for a Federal PIV per HSPD 12
- Detailed specifications to support technical interoperability among PIV systems

System Accreditation Mandated

- **FIPS 199 Standards for Security Categorization of Federal Information and Information Systems**
- **SP 800-37 Guide for Security Authorization of Federal Information Systems**
- **SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations**
- **Other (ISO 27001, State Standards, etc)**

PIV-Interoperability

- **PIV Card** – an identity card that is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV Cards are interoperable with and trusted by all Federal government relying parties.
- **PIV Interoperable Card** – an identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal government relying parties to trust the card.
- **PIV Compatible Card** – an identity card that meets the PIV technical specifications so that PIV infrastructure elements such as card readers are capable of working with the card, but the card itself has not been issued in a manner that assures it is trustworthy by Federal government relying parties.

FRAC & ERO Attribute Programs

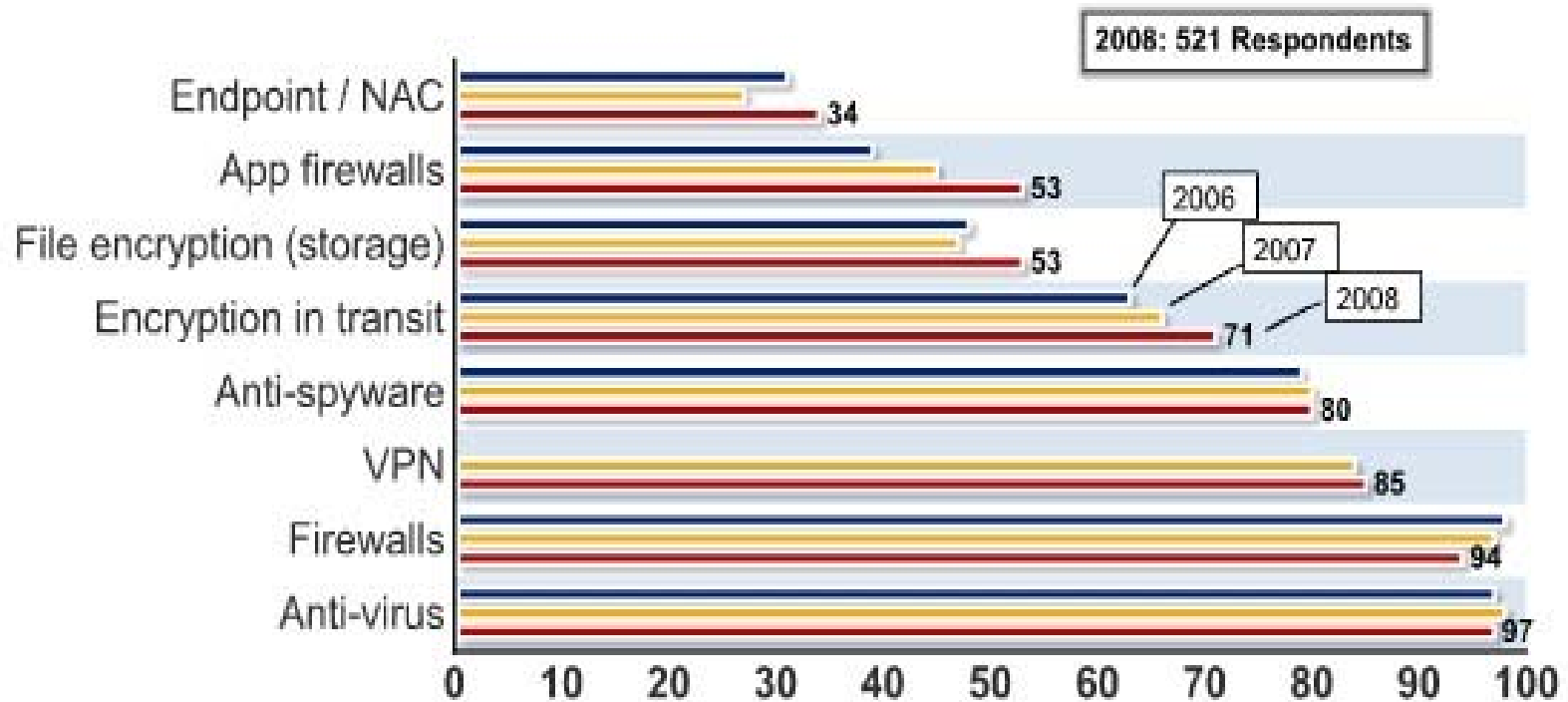
- **Identity Proofing**
- **Registration**
- **Vetting/Issuance**
- **Maintenance**
- **Interoperability/Tech Requirements**

Interoperability & Trust

- HSPD-12
- FIPS 201
- NIMS
- PIV and PIV-I
- Authentication Assurance Levels

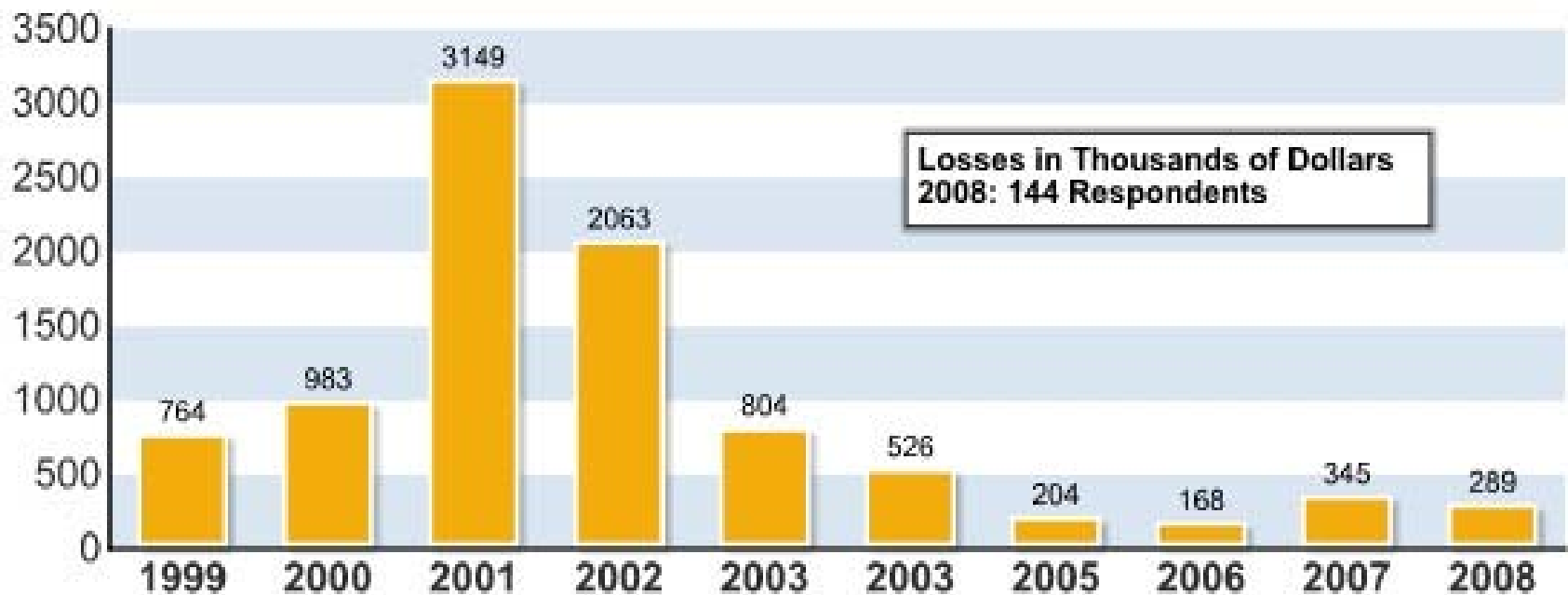
Security Technologies

Figure 16: Security Technologies Used



The Cost of Security Clean Up

Figure 14: Average Losses Per Respondent



2008 CSI Computer Crime and Security Survey

Barriers to Federal Reliance

- **Common terminology for identity cards** – in order to ensure consistency, a lexicon for differentiating a Federal government PIV card from a non-federally issued identity card seeking PIV system interoperability must be developed;
- **Technical requirements** – for non-federally issued identity cards to interact with federal infrastructure, basic technological requirements must be met;
- **Identifier namespace** – effective use of identity cards requires an identifier that is unique across all identity cards. Lack of a unique identifier may result in incorrect access control decisions; and
- **Trusted identity** – the fundamental purpose of an identity card is to establish the identity of the card holder. Therefore, an identity card must be issued in a manner that provides Federal government relying parties with a requisite level of trust.

Future Threats to Federal & Non-Federal

- New technology adoption will be employed to cut costs and increase efficiencies. For all the right business reasons, virtualization, Web 2.0/3.0 services, cloud computing models and advanced wireless devices are quickly migrating into the computing environment.
- A robust Cyber Security program is integral and comes with the cost of doing business; without it these technologies will bring exponential risk to an Agency's network infrastructure.

Summary

- Cyber Security Best Practices
- Application/Software Security
- Database Security Controls
- Data Protection
- Challenges/Risk Management/Law
- Future – ‘Secured Trusted Interoperability’

A Closing Note

“Often security is thought of as an event rather than a process, as a stitch in time rather than a thread that runs throughout each phase of a system’s life cycle. Security is often not considered during the initial planning, design, and development of the system, attempts to retrofit security into the system after development are typically more expensive and less effective than it if is incorporated from inception.”

“Information Assurance”

Boyce & Jennings

Questions



Contact Information:

Elisa.R.Cruz@dhs.gov