2009 HIPAA Security Rule Conference

Framing the Two Days

Julie Boughn

CMS Chief Information Officer

Questions to Run On

- How do we collectively “raise our bar” for Security?
- How do we move past compliance to value-driven security?
- What are the key information security issues that we need to resolve to make progress on Interoperable Health IT?

How to “BE” for the Two Days

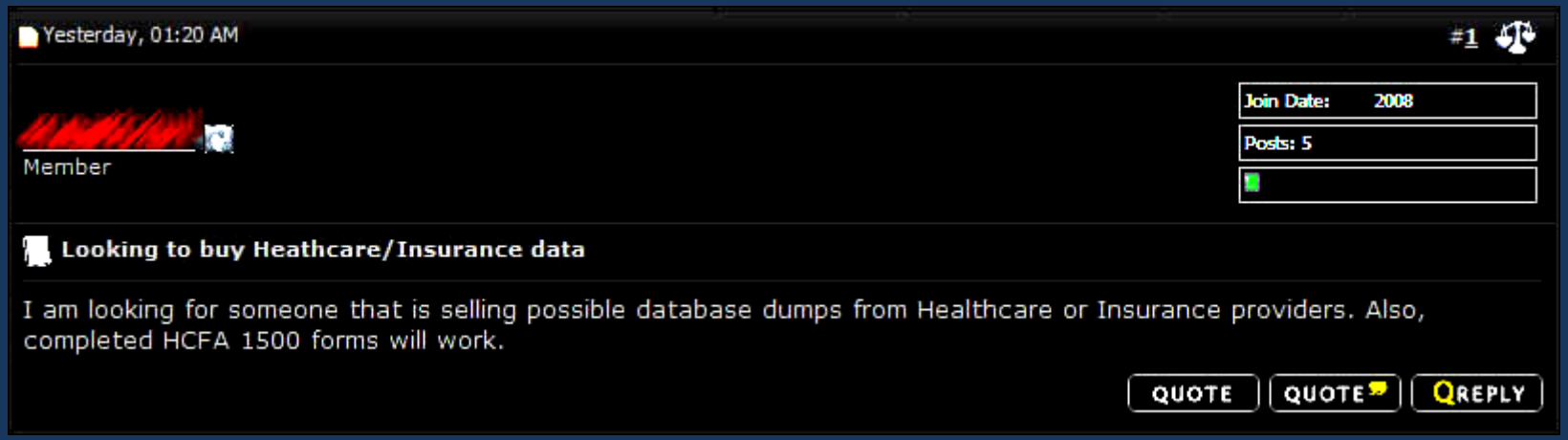
- Curious – don’t let the way we’ve always done things be a barrier
- Humble – we can improve on what we’re already doing
- Think beyond compliance

Opening Activity

- Turn to someone sitting near you who you don't know well.
  - Introduce yourself
  - Answer these questions:
    - Why did I come to this conference?
    - In order for to leave the conference thinking it was wildly successful, I will _____.

Who wants our Data Anyway?

Who wants our Data?



Why Do Security?

- Confidentiality
- Integrity
  - Health Care is a multi-trillion dollar business, representing more than 16% of our economy
  - Lives are at stake!
- Availability
  - Lives are at Stake

CMS Statistics

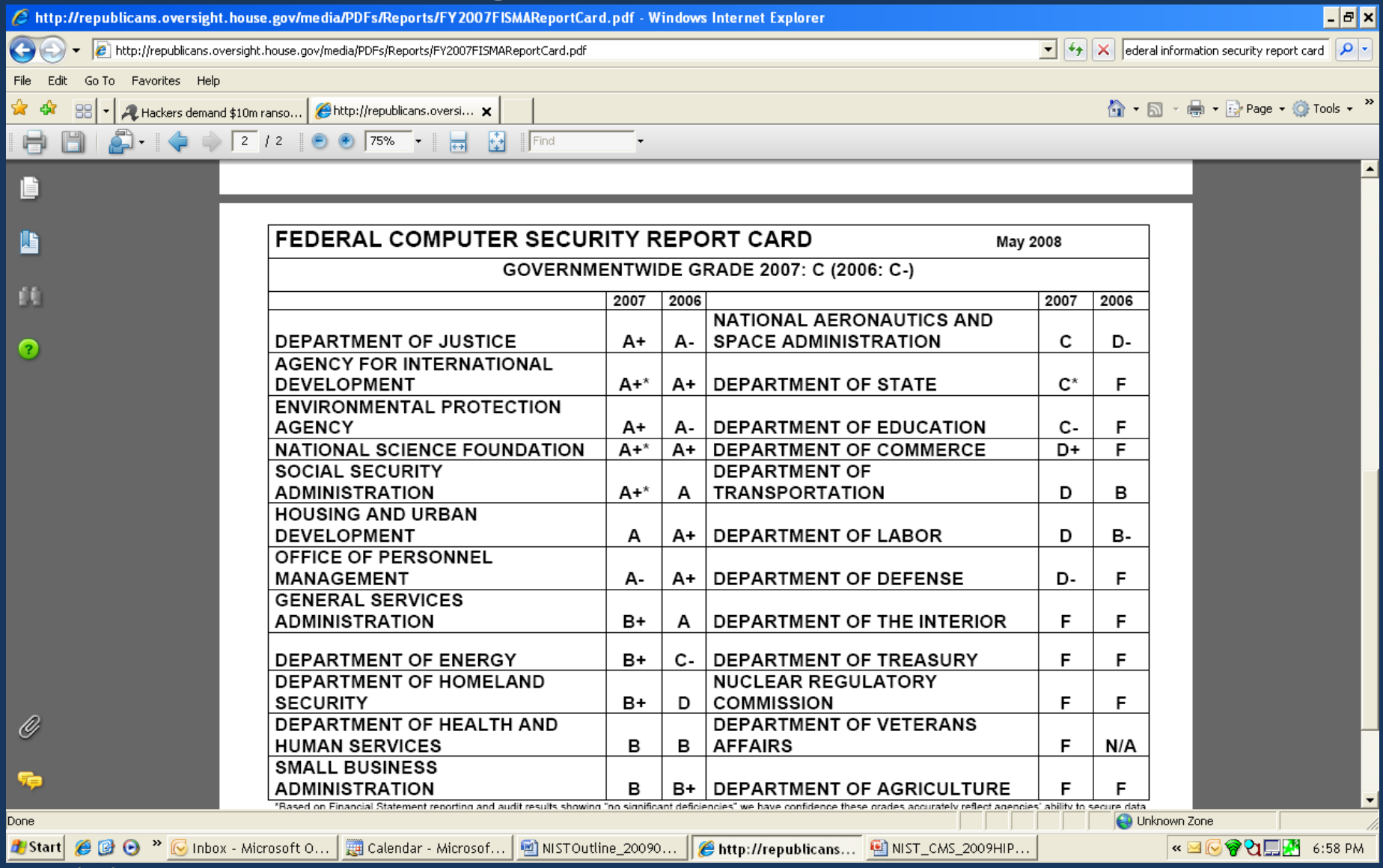
- More than 90 Million Covered Lives
- $1.3 Billion – *PER DAY!*
- 1.2 Billion Medicare FFS claims annually
- 1.2 Billion Medicare Prescription Drug Events
- 2.5 Billion Medicaid Claims Data Events
- ***15 million eligibility inquiries per week***

FISMA in a Nutshell

- The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner. The National Institute of Standards and Technology (NIST) outlines nine steps toward compliance with FISMA:

1. Categorize the information to be protected
2. Select minimum baseline controls
3. Refine controls using a risk assessment procedure
4. Document the controls in the system security plan
5. Implement security controls in appropriate information systems
6. Assess the effectiveness of the security controls once they have been implemented
7. Determine agency-level risk to the mission or business case
8. Authorize the information system for processing
9. Monitor the security controls on a continuous basis

Do Federal Agencies Care about FISMA?



FEDERAL COMPUTER SECURITY REPORT CARD May 2008

GOVERNMENTWIDE GRADE 2007: C (2006: C-)

	2007	2006		2007	2006
DEPARTMENT OF JUSTICE	A+	A-	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	C	D-
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+*	A+	DEPARTMENT OF STATE	C*	F
ENVIRONMENTAL PROTECTION AGENCY	A+	A-	DEPARTMENT OF EDUCATION	C-	F
NATIONAL SCIENCE FOUNDATION	A+*	A+	DEPARTMENT OF COMMERCE	D+	F
SOCIAL SECURITY ADMINISTRATION	A+*	A	DEPARTMENT OF TRANSPORTATION	D	B
HOUSING AND URBAN DEVELOPMENT	A	A+	DEPARTMENT OF LABOR	D	B-
OFFICE OF PERSONNEL MANAGEMENT	A-	A+	DEPARTMENT OF DEFENSE	D-	F
GENERAL SERVICES ADMINISTRATION	B+	A	DEPARTMENT OF THE INTERIOR	F	F
DEPARTMENT OF ENERGY	B+	C-	DEPARTMENT OF TREASURY	F	F
DEPARTMENT OF HOMELAND SECURITY	B+	D	NUCLEAR REGULATORY COMMISSION	F	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	B	DEPARTMENT OF VETERANS AFFAIRS	F	N/A
SMALL BUSINESS ADMINISTRATION	B	B+	DEPARTMENT OF AGRICULTURE	F	F

*Based on Financial Statement reporting and audit results showing "no significant deficiencies" we have confidence these grades accurately reflect agencies' ability to secure data

Interoperable Health Information Technology DEMANDS Accessibility

FISMA's risk-based approach is not incompatible with accessibility.

CMS Information Security Program

- Policies and Standards
- Certification & Accreditation
- Security Technical Architecture
- Training & Awareness

http://www.cms.hhs.gov/InformationSecurity/

Thought Question

- Can protected health information be both accessible and secure?
  - Decisions regarding the balance are made every day, but within the framework of the information security program policies & standards

ENDING IN ACTION

- With the same partner you talked to at the beginning of my session, spend the next 3-4 minutes responding to these questions:
  - Is FISMA an unreasonable bar for any organization that values information security?
  - What are the information security barriers that will hold us back from achieving the vision of a nationwide, interoperable EHR for most Americans by 2014?