



**Internal
Revenue
Service**

Information Protection of IRS Data used by State Agencies

March 8, 2007

*Presentation to the Federation
Tax Administrators Computer
Security Officer Conference*



Nearly one in four Americans had their personal information lost or stolen in 2006

196,000 customer social security numbers, names, birthdates and addresses **lost**



200,000 customer names, social security numbers and credit card data **lost**

135,000 employees and patients



1 million personal records **stolen**



26.5 million veteran and active duty military records **lost**



Nearly one in four Americans had their personal information lost or stolen in 2006

196,000 customer social security numbers, names, birthdates and addresses lost



200,000 customer s, social security mbers and credit card data lost



In 2006 more than **75.1 million Americans**

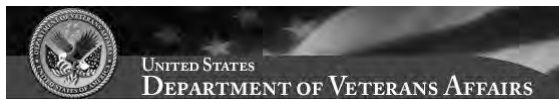
– 25% of the population –

have had their personal information lost or stolen.

135,000 employ and patients

can oss

million personal records stolen



26.5 million veteran and active duty military records lost

3



Identity Theft is easier than you may think

- ▶ Thieves get information from businesses or other institutions by:
 - Stealing records while they are on the job
 - Bribing employees with access to records
 - Hacking
- ▶ Steal personal mail
- ▶ Complete a change of address form to divert mail to another location
- ▶ Rummage through trash – “dumpster diving”
- ▶ Get credit reports by posing as someone who has a legal right
- ▶ Steal personal information found on a cell phone

4

Personally Identifiable Information (PII) includes the personal data of taxpayers as well as employees, contractors, and visitors to the IRS

- ▶ Personally identifiable information (PII) is generally defined as any data which can potentially be used to identify, locate, or contact an individual, or potentially reveal the activities, characteristics, or other details about a person
- ▶ Examples of PII include:
 - Federal Tax Information (FTI)
 - Names
 - Home address
 - Home telephone numbers
 - Social Security Numbers
 - Date of birth
 - Biometric (height, weight, eye color, fingerprints, etc.)
 - Financial or bank account information
 - Driver's license number



5

Technology advances put us all at risk of misuse or loss of personal information

Share data with external organizations

Support a mobile workforce

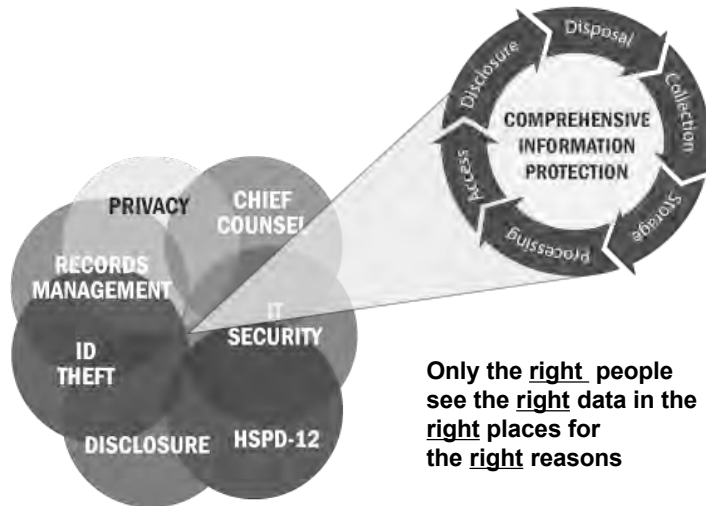
- Increased electronic transactions
- Increasing use of laptops
- Use of portable storage devices
- Internet (Phishing and other social engineering)
- E-mail
- Cell phones
- PDAs

We must implement mechanisms to identify and mitigate security risks.

6



Our goal is to build public trust through our programs and practices



7



In response to data breaches across the government, the Office of Management and Budget (OMB) issued several memoranda on safeguarding PII

OMB M-06-15 May 22, 2006	OMB M-06-16 June 23, 2006	OMB M-06-19 July 12, 2006	OMB M-06-20 July 17, 2006
<ul style="list-style-type: none"> Restates Privacy Act Requirements Conduct Policy and Process Review Weaknesses identified must be included in agency Plan of Action and Milestones (POA&M) Remind Employees of Responsibilities for Safeguarding PII, the rules for acquiring and using such information, and the penalties for violating these rules 	<ul style="list-style-type: none"> Requires agencies to perform a technology assessment to ensure appropriate safeguards are in place, including: <ul style="list-style-type: none"> Encryption standards Allow remote access only with two-factor authentication Use a "time-out" function for remote access and mobile devices; Log all computer-readable data extracts and time parameters System Review (NIST Checklist) 	<ul style="list-style-type: none"> Revises current reporting requirements to require agencies to report all (electronic and physical form) incidents involving personally identifiable information (PII) to US-CERT within one hour of discovery (both suspected and confirmed breaches) Privacy and Security Funding Reminder 	<ul style="list-style-type: none"> Identifies additional FISMA reporting instructions for privacy Results from the OMB M-06-15 review of policies and procedures for protecting PII must be included as an appendix Privacy updates must be submitted quarterly with the security updates to the President's Management Agenda scorecard

<http://www.whitehouse.gov/omb/memoranda/2006.html>

8



The President's Identity Theft Task Force made several recommendations for responding to a data breach

▶ Key recommendations:

- **Identify a core response group (CRG)** to be convened upon identification of a potential data breach. CRG should include agency senior leadership such as the CIO, General Counsel, Chief Privacy Officer, and TIGTA.
- **Develop risk-based analysis** to determine whether the incident being examined has the potential for identity theft.
- **Implement a response plan** to identify mitigation measures (e.g. credit monitoring) and notify affected individuals of the incident.

9



IRS' Office of Privacy & Information Protection works to protect and safeguard information

Privacy

- ▶ Gather only the taxpayer and employee data necessary
- ▶ Conduct Privacy Impact Assessments
- ▶ Identify, analyze and mitigate privacy risks

Safeguards

- ▶ Guarantees protection of federal tax returns and return information (FTI)
- ▶ Publication 1075 Safeguarding taxpayer information
- ▶ Oversee compliance and creating protection awareness
- ▶ Conduct on-site evaluations of those agencies and report on compliance

Incident Response

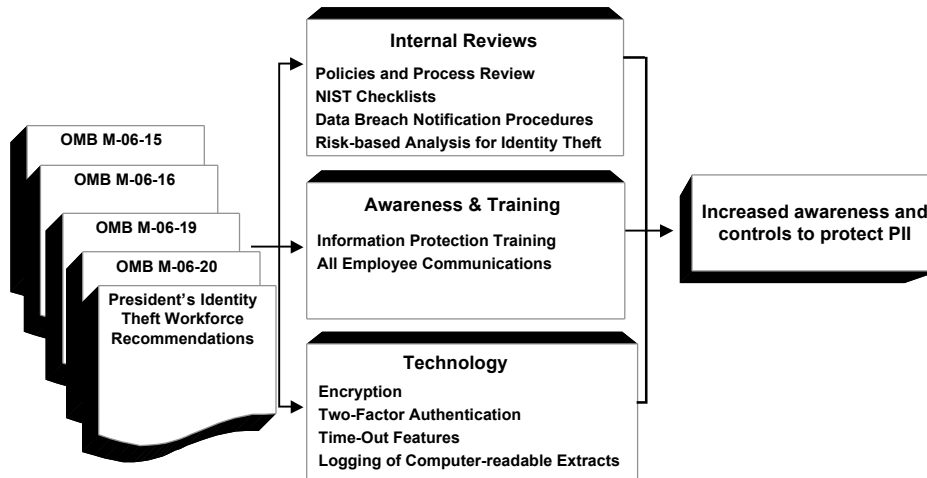
- ▶ Core Response Group (CRG)
- ▶ Risk-based analysis
- ▶ Response plan



10



Within the IRS, we are implementing a three-pronged approach to protect information



11



IRS conducted a review of internal policies and processes in place to prevent the intentional or negligent misuse of, or unauthorized access to, PII

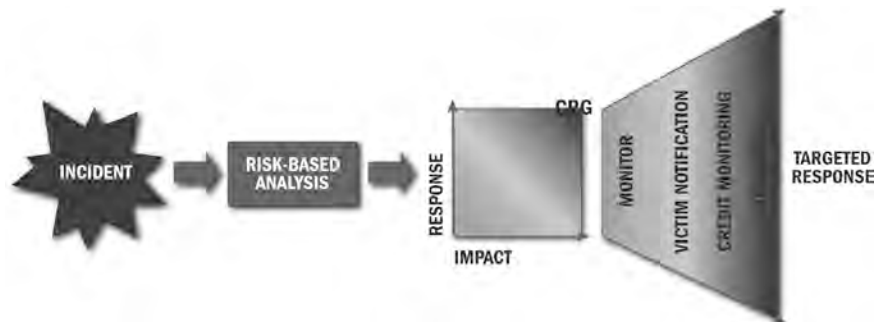
- ▶ We focused on the following:
 - Who has access to what
 - Training in the use of technical tools to safeguard PII (e.g. encryption)
 - Increasing employee awareness of Rules of Behavior
 - Securing equipment
 - Incident notification procedures
 - Remote employee policies and technologies
 - Internal Privacy Advisory Board
 - Updating IRM to reflect all privacy requirements, processes and role of Senior Agency Official for Privacy

12



The IRS is implementing an incident response process

- ▶ Established servicewide PII Incident Management Program within MA&SS
- ▶ Developed draft PII Incident Management policies and procedures
- ▶ Currently assessing incidents involving PII



13



IRS developed and delivered mandatory information protection training to clearly explain employee responsibilities

- ▶ This mandatory training for all employees is a unified module that demonstrates the interconnectedness between IT Security, Unauthorized Access (UNAX), Disclosure and Privacy domains
 - The mandatory Information Protection training meets MA&SS multiple training mandates, including protecting personally identifiable information
 - The mandatory Information Protection training was successfully administered and is available to state organizations for their internal use



14



The IRS uses strategic communications to remind employees of their obligation to protect PII at work and at home

- ▶ Using multiple internal IRS communication channels:
 - *IRS Headlines* and *IRS Web News Articles*
 - Online document repository
 - Memorandums and e-mail from Senior Officials
 - Developed Security Response wallet card containing contact information in the event of a privacy or security breach
 - Developed FAQs for all employees who work with PII
 - Created an internal website with all data protection information
 - Job Aides (encryption)

15



The IRS is using technology solutions to protect and prevent PII or other sensitive information from being accessed even if lost or stolen

- ▶ All IRS laptops now have full disk encryption
- ▶ We are implementing encrypted electronic transmission technologies
- ▶ OMB technical requirements in the area of two-factor authentication, time-out functions, and computer readable extracts are being assessed
 - The IRS currently uses multi-factor authentication through its ERAP VPN solution
 - Time-out capabilities are in place and will be validated to ensure remote access and mobile devices require user re-authentication after 30 minutes of inactivity
 - Formal processes and procedures will be validated/implemented to ensure sensitive data extracts are erased within 90 days



16



How to Contact Us

- ▶ Barbra Symonds, Director, Office of Privacy & Information Protection
- ▶ Marla Somerville, Assistant to the Director, Office of Privacy & Information Protection
- ▶ Richard Phillips, Deputy Director, Office of Privacy
- ▶ Catherine Campbell, Acting Deputy Director, Safeguards
- ▶ Ellen Pieklo, Senior Operations Advisor, Office of Privacy & Information Protection

- ▶ Mailing address
 - Director, Office of Privacy and Information Protection
 - Internal Revenue Service, OS:MA:PIP
 - 1111 Constitution Avenue, N.W., IR-7050
 - Washington D.C. 20224

- ▶ Telephone: 202-927-5170
- ▶ Safeguards email address: safeguardreports@irs.gov
- ▶ Privacy email address: privacy@irs.gov
- ▶ Tactical advisory group – security subcommittee members

17