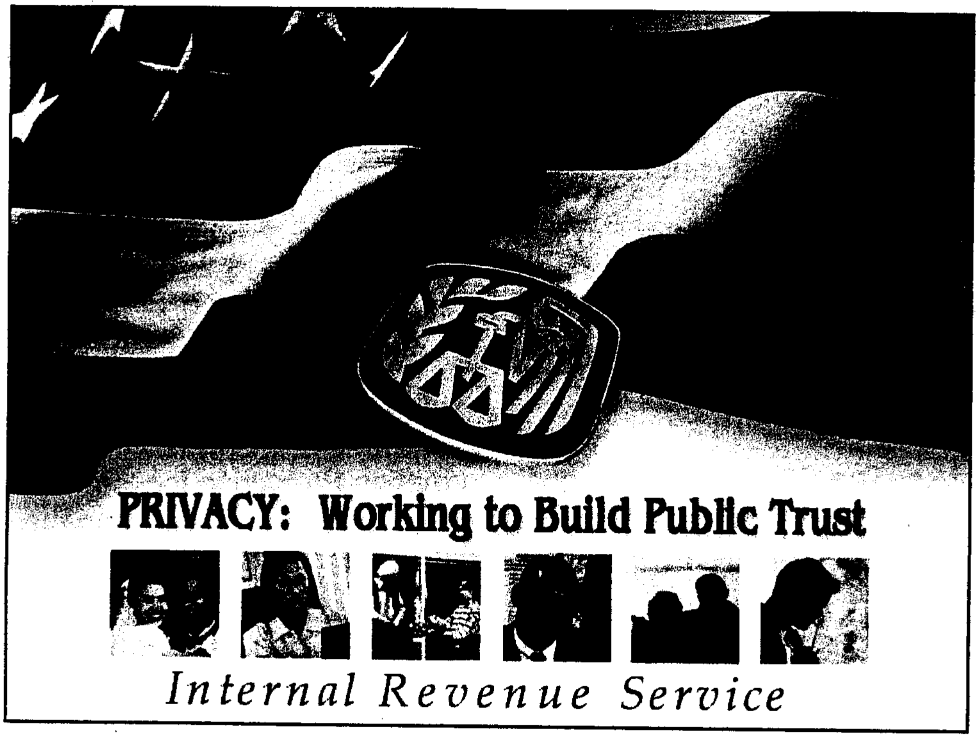
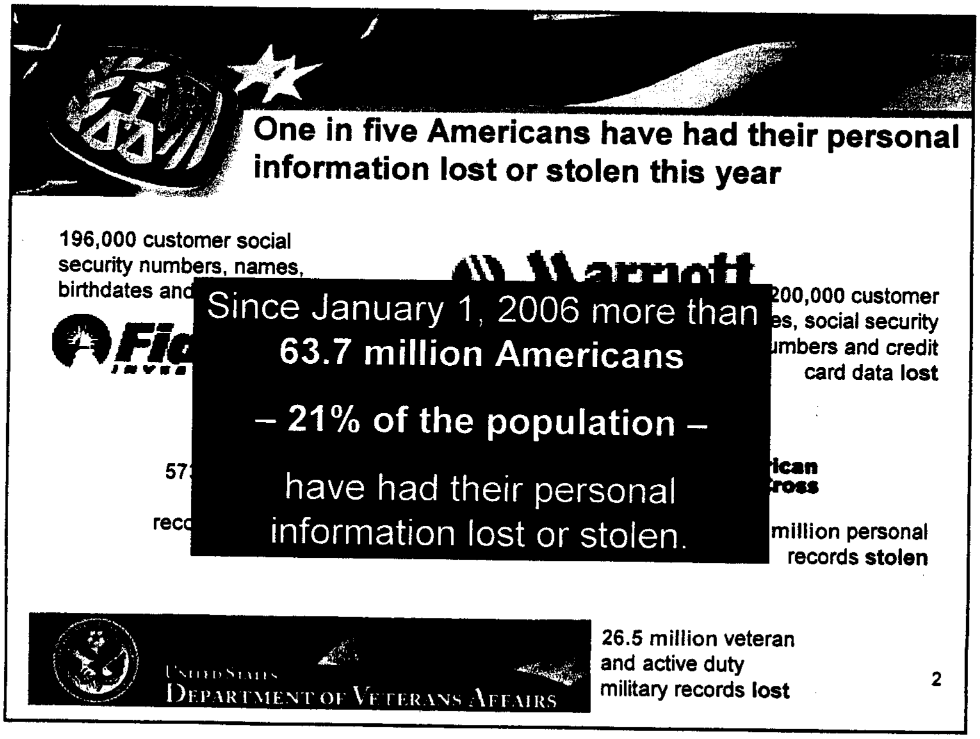


PRIVACY: Working to Build Public Trust

Internal Revenue Service



One in five Americans have had their personal information lost or stolen this year

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

200,000 customer
es, social security
umbers and credit
card data lost

57

rec

Since January 1, 2006 more than
63.7 million Americans

– 21% of the population –

have had their personal
information lost or stolen.

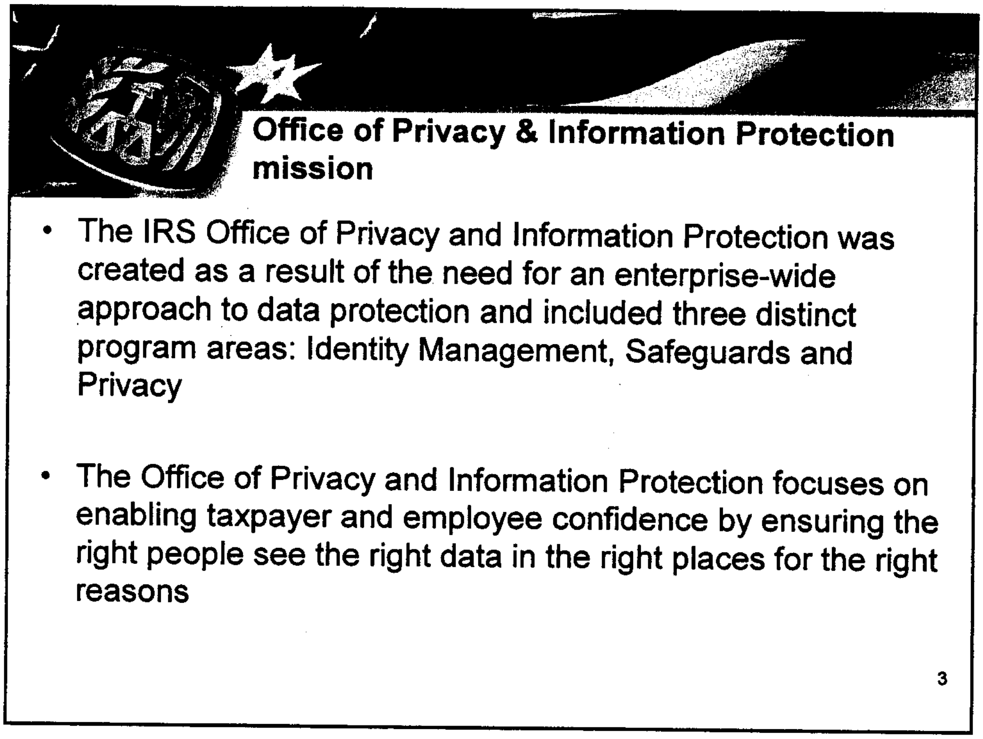
ican
ross

million personal
records stolen

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

26.5 million veteran
and active duty
military records lost

2

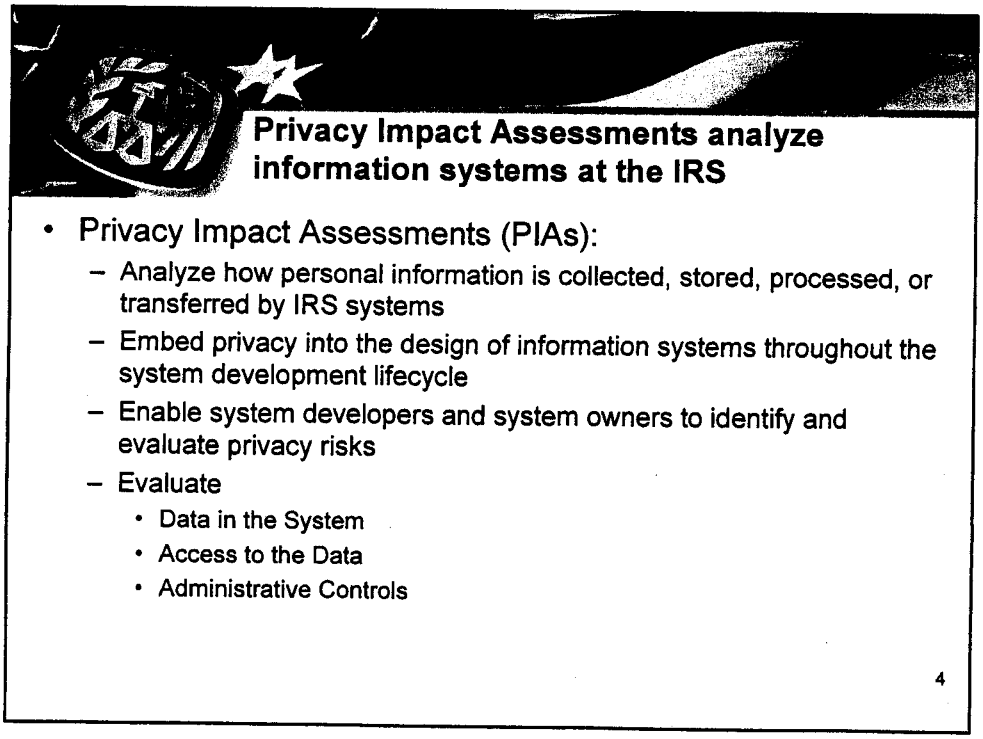


Office of Privacy & Information Protection mission

- The IRS Office of Privacy and Information Protection was created as a result of the need for an enterprise-wide approach to data protection and included three distinct program areas: Identity Management, Safeguards and Privacy

- The Office of Privacy and Information Protection focuses on enabling taxpayer and employee confidence by ensuring the right people see the right data in the right places for the right reasons

3



Privacy Impact Assessments analyze information systems at the IRS

- Privacy Impact Assessments (PIAs):
  - Analyze how personal information is collected, stored, processed, or transferred by IRS systems
  - Embed privacy into the design of information systems throughout the system development lifecycle
  - Enable system developers and system owners to identify and evaluate privacy risks
  - Evaluate
    - Data in the System
    - Access to the Data
    - Administrative Controls

4

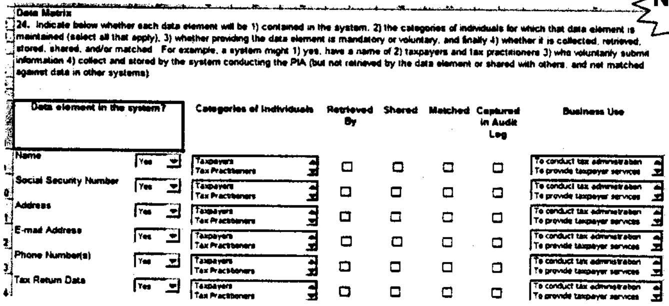
PIAs are a business enabler at the IRS

- PIAs are a mechanism to:
  - Ensure handling of personal information conforms to applicable legal, regulatory, and policy requirements regarding privacy
  - Determine the risks and effects of collecting, maintaining and disseminating personal information in an electronic information system
  - Examine and evaluate protections and alternative processes for handling personal information to mitigate potential privacy risks
  - Assure the public that the Agency is effectively managing its personal data
  - Ensure that system owners understand their obligations regarding personal data

Critical analysis is key to the PIA

- Key Points of Analysis include:
  - Audit trails
  - Identifying how, why, and from where data is collected
  - System interconnections and interfaces
  - Current SORN

New IRS PIA

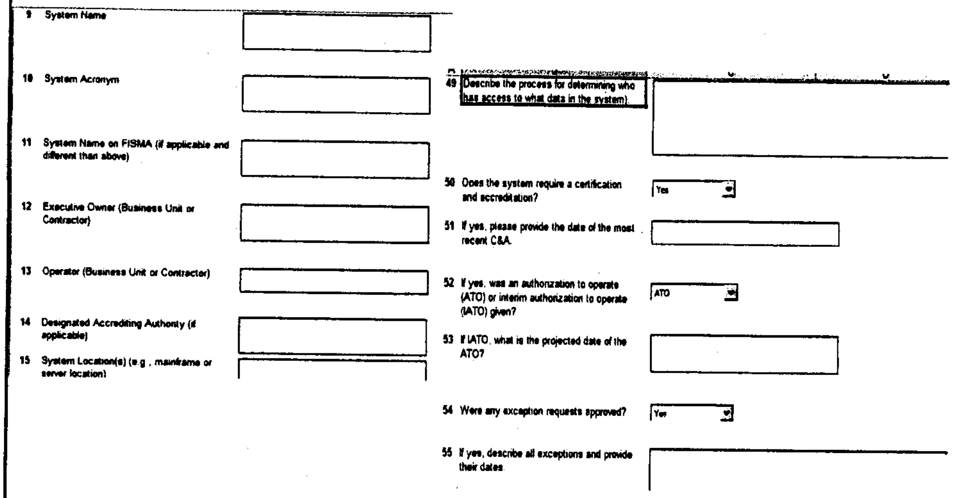


Data Matrix

24. Indicate below whether each data element will be 1) contained in the system, 2) the categories of individuals for which that data element is maintained (select all that apply), 3) whether providing the data element is mandatory or voluntary, and finally 4) whether it is collected, retrieved, stored, shared, and/or matched For example, a system might 1) yes, have a name of 2) taxpayers and tax practitioners 3) who voluntarily submit information 4) collect and stored by the system conducting the PIA (but not retrieved by the data element or shared with others, and not matched against data in other systems)

Data element in the system?		Categories of Individuals	Retrieved By	Shared	Matched	Captured in Audit Log	Business Use
Name	Yes	Taxpayers Tax Practitioners	□	□	□	□	To conduct tax administration To provide taxpayer services
Social Security Number	Yes	Taxpayers Tax Practitioners	□	□	□	□	To conduct tax administration To provide taxpayer services
Address	Yes	Taxpayers Tax Practitioners	□	□	□	□	To conduct tax administration To provide taxpayer services
E-mail Address	Yes	Taxpayers Tax Practitioners	□	□	□	□	To conduct tax administration To provide taxpayer services
Phone Number(s)	Yes	Taxpayers Tax Practitioners	□	□	□	□	To conduct tax administration To provide taxpayer services
Tax Return Data	Yes	Taxpayers Tax Practitioners	□	□	□	□	To conduct tax administration To provide taxpayer services

Analysis identifies privacy risks



9 System Name

10 System Acronym

11 System Name on FISMA (if applicable and different than above)

12 Executive Owner (Business Unit or Contractor)

13 Operator (Business Unit or Contractor)

14 Designated Accrediting Authority (if applicable)

15 System Location(s) (e.g , mainframe or server location)

49 Describe the process for determining who has access to what data in the system).

50 Does the system require a certification and accreditation? Yes

51 If yes, please provide the date of the most recent C&A.

52 If yes, was an authorization to operate (ATO) or interim authorization to operate (IATO) given? ATO

53 If IATO, what is the projected date of the ATO?

54 Were any exception requests approved? Yes

55 If yes, describe all exceptions and provide their dates.

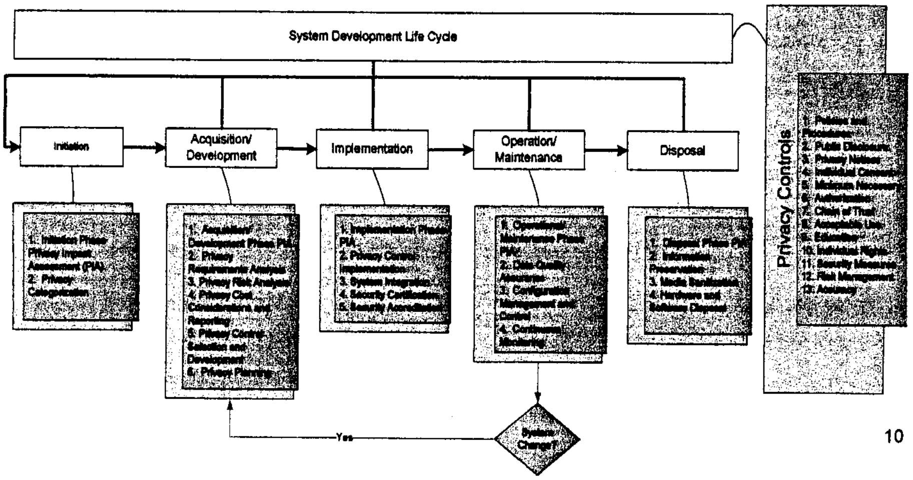
PIAs are driven by Federal mandates

- Section 208 of the E-Government Act of 2002, December 17, 2002 and Office of Management and Budget (OMB) Memorandum (M)-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003
  - **IMPACT = Encourage E-Gov by alleviating privacy concerns**
- OMB Circular No. A-11, Preparation, Submission, and Execution of the Budget, May 27, 2003
  - **IMPACT = PIA now basis for E-300 approvals**
- NIST SP 800-53 Rev. 1 Recommended Security Controls for Federal Information Systems, February 28, 2006
  - **IMPACT = PIA included in the Planning Control Family**
- Annual FISMA and Privacy Management Report and the President's Management Agenda
  - **IMPACT= PIA metrics are a requirement**

Multiple stakeholders have the responsibility of completing PIAs

- IRS Business Owners and System Owners:
  - Review their data collection to ensure that the minimum amount of relevant and necessary information is collected, used, and maintained
  - Work with the System Developers to complete the Privacy Impact Assessment
  - Answer what data is to be used, how the data is to be used, and who will use the data
- System Developers:
  - Work with the Business Owners to complete the Privacy Impact Assessment
  - Address whether the technical implementation of the Business Owners' requirements compromises personal privacy
- Office of Privacy:
  - Review the PIAs submitted by the Business Owner and System Developer
  - Work with the Business Owner and System Developer to develop design requirements that resolve risks identified by the PIA
  - Identify privacy risks
  - Assist in the development of privacy mitigation strategies

PIAs should be conducted throughout the system development lifecycle


System Development Life Cycle
Initiation
Acquisition/ Development
Implementation
Operation/ Maintenance
Disposal
1. Initiation Phase Privacy Impact Assessment (PIA)
2. Privacy Categorization
1. Acquisition/ Development Phase PIA
2. Privacy Requirements Analysis
3. Privacy Risk Analysis
4. Privacy Cost Considerations and Reporting
5. Privacy Control Selection and Development
6. Privacy Planning
1. Implementation Phase PIA
2. Privacy Control Implementation
3. System Integration
4. Security Certification
5. Security Accreditation
1. Operations/ Maintenance Phase PIA
2. Data Quality Assurance
3. Configuration Management and Control
4. Continuous Monitoring
1. Disposal Phase PIA
2. Information Preservation
3. Media Sanitization
4. Hardware and Software Disposal
Privacy Controls
1. Policies and Procedures
2. Public Disclosure
3. Privacy Notices
4. Individual Consent
5. Minimum Necessary
6. Authorization
7. Chain of Trust
8. Acceptable Use
9. Education
10. Individual Rights
11. Security Measures
12. Risk Management
13. Accuracy
System Change?
Yes

OMB M-03-22 specifies nine events that trigger the need for a PIA

Conversions - when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;

Significant Merging - when agencies adopt or alter business procesees so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;

New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

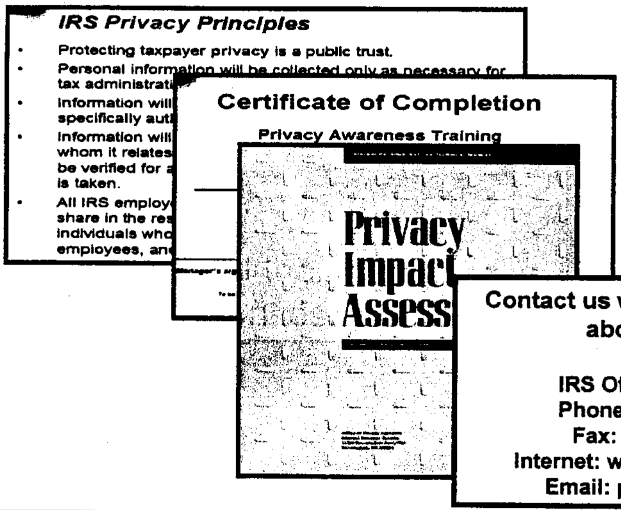
Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;

Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

Contact us for more information



IRS Privacy Principles

- Protecting taxpayer privacy is a public trust.
- Personal information will be collected only as necessary for tax administrati
- Information will specifically aut
- Information will whom it relates be verified for a is taken.
- All IRS employ share in the res individuals who employees, and

Certificate of Completion

Privacy Awareness Training

Contact us with your questions about Privacy

IRS Office of Privacy
Phone: 202-927-5170
Fax: 202-622-6785
Internet: www.irs.gov/privacy
Email: privacy@irs.gov