WELCOME TO PRIVACY IMPACT ASSESSMENT TRAINING

SALLIE MILAM, WV'S CHIEF PRIVACY OFFICER

JUNE 15, 2015

WHAT DO YOU WANT TO GET OUT OF THIS TRAINING?

FOR THE NEXT 30 MINUTES OR SO . . .

- What is Privacy?
- WV State Privacy Program
- Defining Personally Identifiable Information
- Privacy Principles
- Why Privacy is so important

WHAT IS PRIVACY?

- "The rights and obligations of individuals and organizations with respect to the collection, use, disclosure and disposal of personal information." Generally Accepted Privacy Principles.

- Executive Order No. 6-06
- State Privacy Office
- Privacy Management Team
- Privacy Policies
- Education & Training

The WV Privacy Program applies to the Governor’s Office and all departments (including agencies, boards, and commissions) within the Executive Branch of the West Virginia State Government.


GOVT

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (PII)?

All information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes Protected Health Information (PHI). PII is contained in public and non-public records.

EXAMPLES OF PII

- First Name (Or Initial)
- Last Name (Current Or Former)
- Geographical Address
- Electronic Address (E-mail Address)
- Cell Number
- Telephone Number /Fax Number (Place Of Residence)
- Social Security Number
- Birth Date
- Birth, Adoption or Death Certificate
- Medical, Disability or Employment Records
- Credit/Debit Card Number
- Financial Records (Loan Accounts, Payment History, Consumer Reports)
- Check/Savings/Other Financial Account Numbers
- Mother's Maiden Name
- Biometric Identifiers
- Driver Identification Numbers
- Criminal records & history
- Salary Information
- Computer Information

PRIVACY PRINCIPLES

- The Privacy Program is based upon these six **Privacy Principles**, consistent with law and policy.
- Compliance is required for all Executive Branch Departments.
- Program is annually audited against AICPA's Generally Accepted Privacy Principles.
- Additional information on the Privacy Principles can be obtained on the West Virginia State Privacy Office website: http://www.privacy.wv.gov/Pages/default.aspx

PRIVACY & SECURITY INTERRELATIONSHIP

- The PMT works in collaboration with the Governor's Executive Branch Information Security Team (GEIST). Privacy and Security go together.
- Without good security, you won't have privacy. Security is an essential part of the equation; it's the other side of the coin.


PRIVACY


SECURITY

WHY PROTECT PRIVACY?

Public Trust

- Citizens have no option to shop around – they are required to provide personal information to government.
- We have an obligation to protect the information entrusted to us.

WHY PROTECT PRIVACY?

Federal Law(s):

- Privacy Act of 1974
  - Section 7 (5 U.S.C. § 552a)

WHY PROTECT PRIVACY?

State Law(s)s:

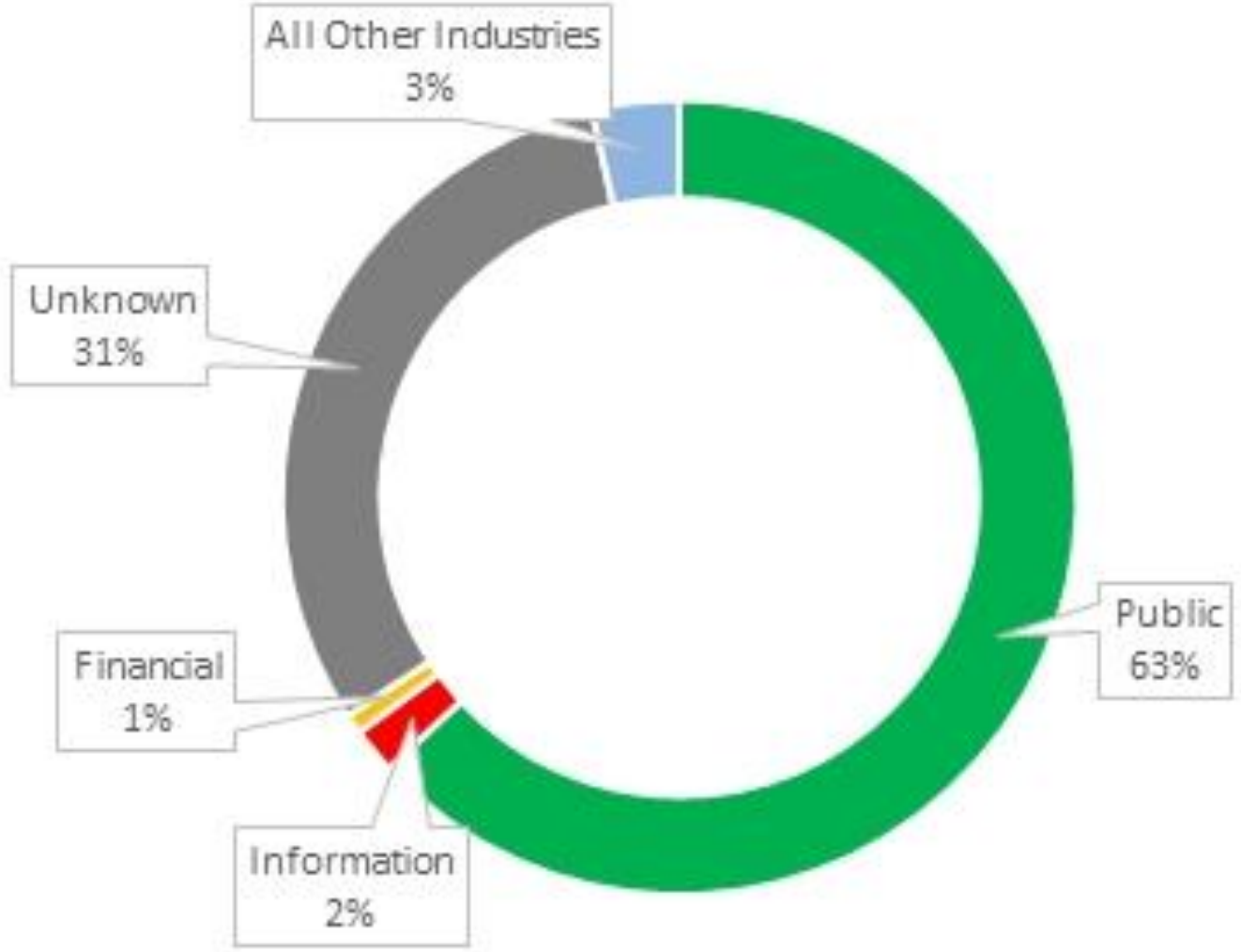
- Records Management & Preservation of Essential Records Act
  - Applies to state government
  - Exempts SSN from FOIA
  - Prohibits release to non-governmental entities, unless authorized by law

WHY PROTECT PRIVACY?

State Law(s):

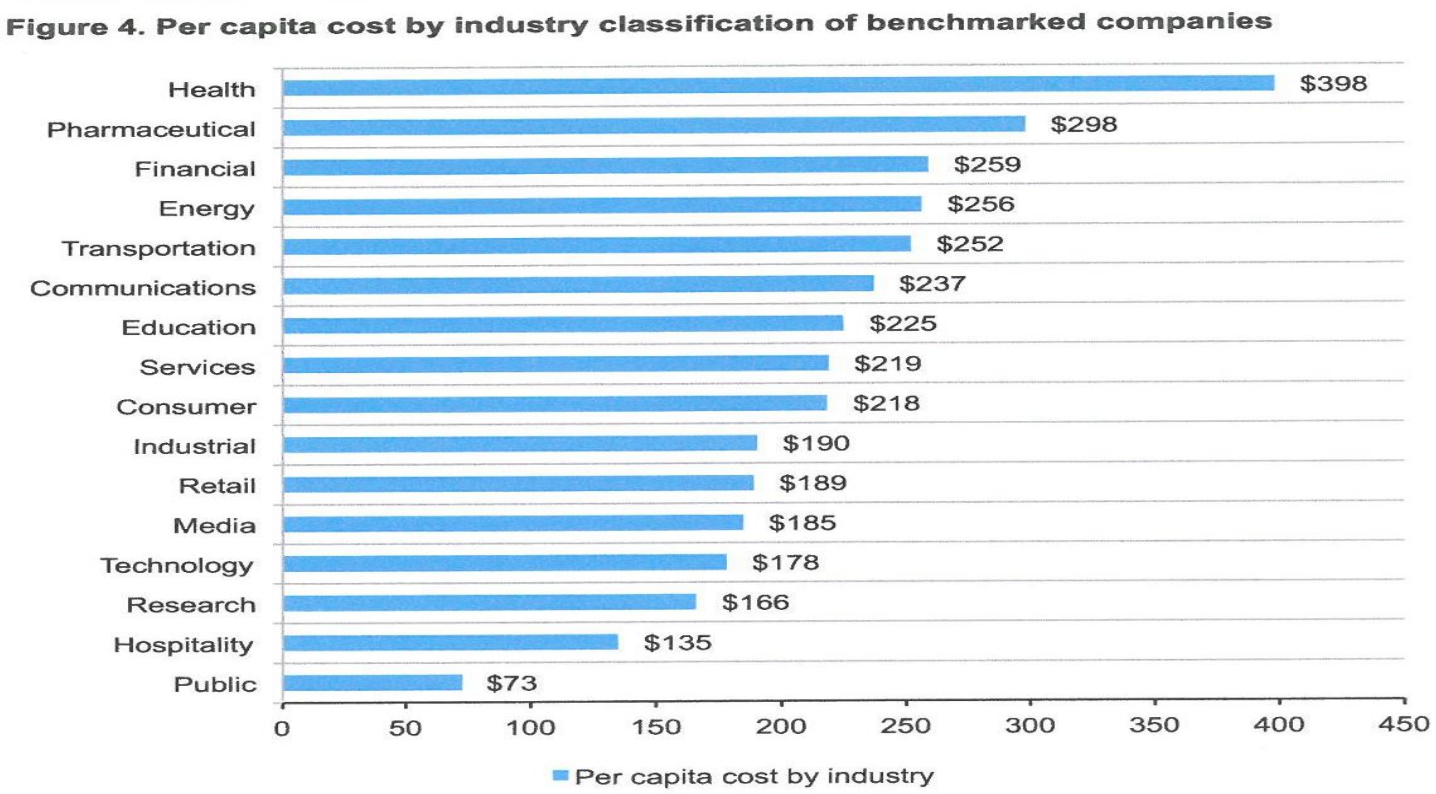
- Breach of Security of Consumer Information Act (W. Va. Code § 46A-2A-10)
  - Individuals must be notified of an incident where:
  - Computerized data elements include a WV resident's first name or initial and last name, linked to the individual's:
  - SSN, DLN, state-issued ID card number, financial account number, credit card or debit card number (including any required security code, access code or password)
  - And, the data is unencrypted or unredacted, and was or is reasonably believed to have been accessed and acquired by an unauthorized person,
  - And, the incident causes or it is reasonably believed that it has caused or will cause identity theft or other fraud.

Total Data Breach Incidents



Data Source: Verizon 2015 Data Breach Investigations Report

2015 COST OF DATA BREACH STUDY: UNITED STATES, PONEMON INSTITUTE MAY 2015



WHERE IS YOUR RISK?

Privacy Risk Management

- Privacy Self-Assessment and Audit
- Analysis of incident experience
- Privacy Impact Assessment

EVERYONE'S ROLE & RESPONSIBILITY

As a member of the WV State government workforce, you are responsible for following privacy policies and procedures. Privacy policies and procedures require you to:

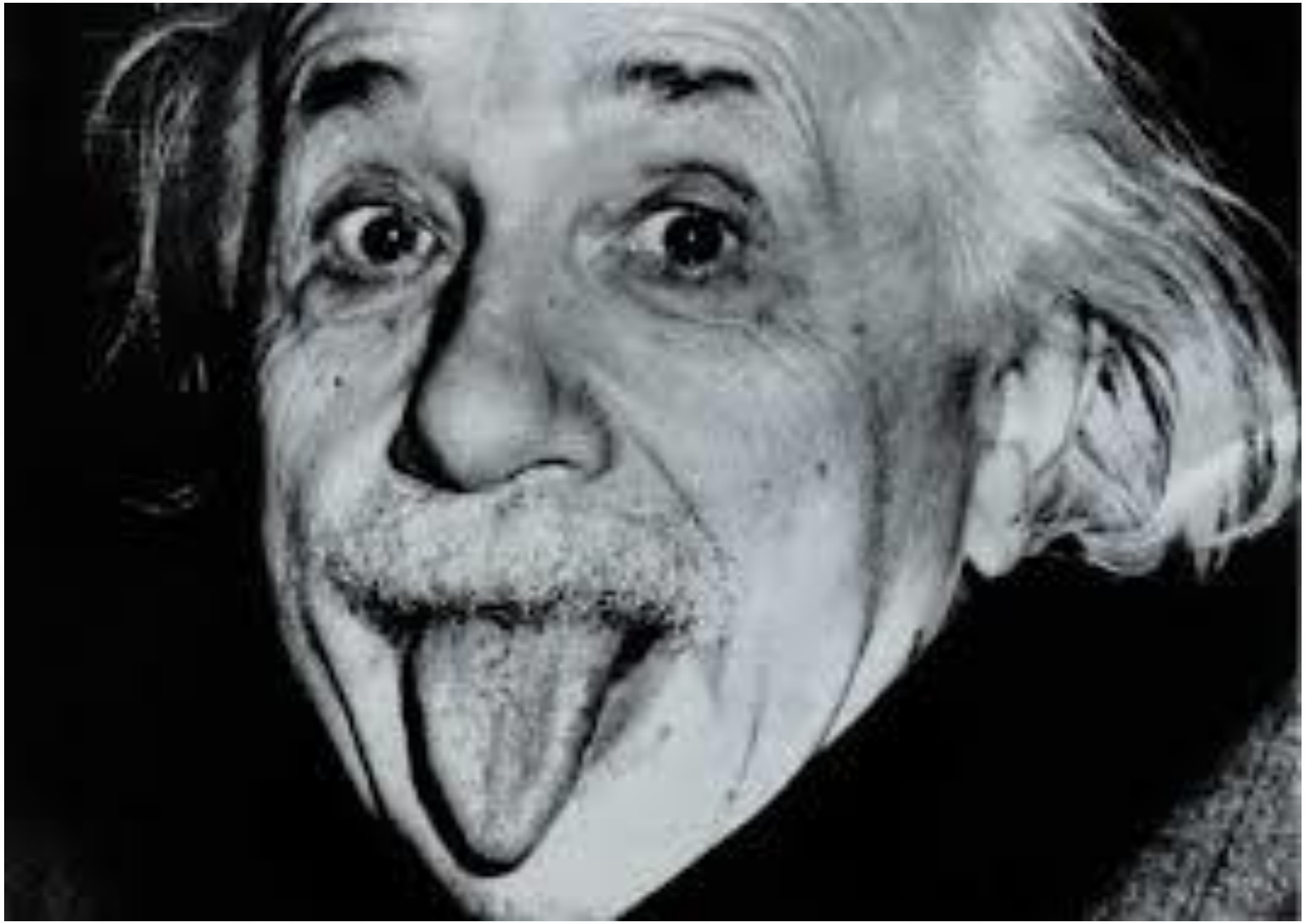
- Collect, access, use, and disclose personal information only for reasons that are for a legitimate job function, support the mission of WV State Government, and are allowed by law.
- The Notice policy makes you respect privacy as it is your agency's written promise to individuals that you will respect their privacy.
- Safeguard personal information in your possession, whether it be in paper or electronic format.
- Properly dispose of documents containing PII.
- Report suspected privacy violations or incidents.

Complete appropriate training and education regarding Privacy laws, regulations, policies, standards, and procedures governing the handling of PII.

Sign an appropriate Confidentiality Agreement upon hire and as otherwise required by laws, policy or procedure.

YOUR ROLE & RESPONSIBILITY AS LEADER

- Privacy Management Team members, Department/Agency Privacy Officers, Security Information Officers, Compliance/Risk Managers, and Department Managers/Business Operational Managers have enhanced responsibility.
- A Privacy Impact Assessment helps organizations assess potential privacy implications of a project, initiative, joint venture, development, office move, installation or upgrade of current systems.



QUIZ ANSWERS

1. How many records were lost or stolen every second of last year (2014)?
   B: 32/second or 1,023,108,267/year.
2. How much will be spent in 2015 globally on cybersecurity? D: $80+B
3. Where does most theft involving incidents occur? C: Victim's work area, at 55% of incidents
4. What percentage of recipients now open phishing messages? C: 23%. 11% click on attachments. Numbers show that with just 10 emails, there is a greater than 90% chance that at least one person will be hacked.

QUIZ ANSWERS CONTINUED

5. Who is responsible for training a vendor's workforce? A: Vendors themselves. By contract, vendors shall be responsible for providing appropriate training to their workforce. A Department can always elect to supplement the vendor's training, but this is not required or expected.

6. Is consumer consent required for a department's marketing activities? A: Yes. A Department may only conduct consumer marketing activities if it has obtained an appropriate consent from the consumer.

QUIZ ANSWERS CONTINUED

7. Who is responsible for investigating a consumer's privacy complaint? C: Each Department shall provide a means to investigate privacy complaints from individuals and ensure that individuals are aware of how to file a complaint with the Department concerning the content of their PII.

8. May Departments collect as much PII as they want? B: No. Departments shall limit the collection, and disclosure of personally identifiable information (PII) to their legal authority. Additionally, Departments should only collect or disclose those elements of PII that are reasonably needed to accomplish a legitimate Departmental objective, except where law or public policy directs otherwise.

QUIZ ANSWERS CONTINUED

9. Where a Department collects PII directly from an individual, it shall have a privacy notice. Which is not a required element of a privacy notice?

E: Types of privacy workforce training. Underlined language is the correct component. This privacy notice shall contain (at minimum): a description of the information collected by the Department, the source(s) of that information if not from the individuals themselves, a statement regarding the purposes for the PII collection, how the PII will be used, types of entities to whom the PII may be disclosed, the individual's rights and choices (if any), where the information is maintained. The notice will also provide a statement that the PII will be appropriately secured.

QUIZ ANSWERS CONTINUED

10. Departments must comply with whose security policies? D: Office of Technology

DID YOU LEARN WHAT YOU WANTED? OR SOMETHING ELSE?

RESOURCES

- **WV State Privacy Office Website - http://www.privacy.wv.gov**
  - Privacy Requirements
  - Privacy Policies/Procedures
  - Privacy Tips
  - Other Resources
- **BRIM - Cyber Insurance - http://www.brim.wv.gov**
- **WV Office of Technology - http://www.technology.wv.gov**
  - Security Policies & Procedures
  - Incident Response Reporting Portal

WEST VIRGINIA
STATE PRIVACY OFFICE

Sallie Milam, Chief Privacy Officer

Terri Barrett, Deputy Chief Privacy Officer

Sue Haga, Privacy Secretary

West Virginia
OFFICE OF TECHNOLOGY

GALE GIVEN

Chief Technology Officer
West Virginia Office of Technology