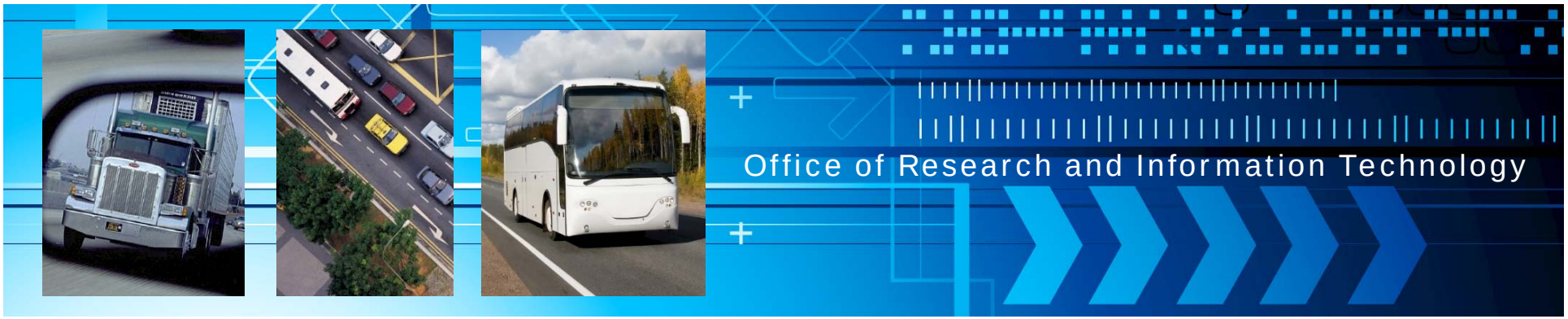
U.S. Department of Transportation
Federal Motor Carrier Safety Administration

Privacy in the Federal Government

Pam Gosier-Cox, FMCSA Privacy Officer ,
Federal Motor Carrier Safety Administration (FMCSA) ,
June 2012 ,



What is Personally Identifiable Information (PII)

- Information that directly or indirectly identifies an individual
- OMB Definition (from M-07-16): "…information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combine with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."
- - Examples include name, address, birthdate, SSN, biometric identifiers (e.g., photo, fingerprint)

When is PII Sensitive?

- Factors to consider when determining the sensitivity of PII
  - Use in combination with other data
  - Context of use

- Some PII is always sensitive, e.g.,
  - Social Security Number
  - Driver's license number
  - Alien (A-) number
  - Biometric identifiers
  - Financial and other account numbers
  - Medical information
  - Memberships
  - Education Records (including test results)

Why is it important to protect privacy?

Privacy is a core value of our society

Potential consequences for not adequately protecting privacy in the government include:

- Negative impact upon individuals whose PII is collected and used
  - Identity theft and other types of fraud
  - Embarrassment
- Reduced mission effectiveness for government organizations
  - Concerns over privacy have ended some government programs
- Loss of credibility, confidence, and trust in government organizations from covered individuals, the public, and stakeholders
- Large costs for government organizations for recovery from privacy incidents
  - Recovery costs per data breach incident average $4.8M

The requirement to protect privacy applies to ALL federal government agencies and contractors

What Can You Do?

- Be diligent in your work practices and diligent to mitigate threats
- This means using best practices in the use, distribution, use, storage, and disposal of information
- This means being leery of anyone requesting unauthorized access to information – who doesn't have a "need to know"
- Ensure recipients of privacy data have an approved need to know/access the data and have appropriate controls in place to protect PII.
- When privacy records are in hardcopy, store them in a locked file or cabinet.
- Restrict access so unauthorized personnel will not be able to view sensitive information displayed on monitors. Privacy information should not be displayed on public monitors or the appropriate controls should be in place to hide the privacy information with the use of special characters.
- Transporting, Mailing, Shipping of PII in electronic format must be encrypted. If an encryption key is required to decrypt, it must be sent in a separate mailing.

Key Privacy Legislation and Guidance for Federal Government Agencies

- Privacy Act of 1974
- E-Government Act of 2002
  - M-06-15, Safeguarding PII
  - M-06-16, Protection of Sensitive Info
  - M-06-19, Reporting PII Incidents
  - 9/20/06 Memo, Identity Theft Related Data Breach Notification Guidance
  - M-07-16, Safeguarding Against & Responding to PII Breach

Reporting Incidents Involving PII

- All suspected privacy related incidents must be reported to the FMCSA ISSO with 1 hour of discovering the incident.
  - Electronic or physical
  - Include suspected and confirmed breaches

  - To report incidents, please contact the FMCSA Information System Security Officer (ISSO) at (202) 493-0196 and the FMCSA Privacy Officer at (202) 366-3655. You will be asked to complete one of two incident reporting forms to accurately document your observations regarding the incident. This form should be submitted to FMCSASecurity@dot.gov.

Incident Reporting During Non-duty Hours

- If the incident occurs during non-duty hours, or the ISSO and Privacy Officer are unavailable, the incident should be reported directly to the Department of Transportation Cyber Security Management Center (CSMC) at 1-866-580-1852. The CSMC will then contact the FMCSA ISSO for further handling of the incident.

Final Thoughts

- Privacy is everyone's responsibility
- All contractors should be familiar with Federal, Department of Transportation, and FMCSA privacy policies, guidance and best practices
- When in doubt, contact the FMCSA Privacy Officer for questions or concern

Questions?