BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Privacy: A Business Enabler

25th Annual Government Financial Management Conference

Marcela Price Souaya

August 19, 2015

Agenda

- Common data related challenges for Federal agencies
- Compliance based risk mitigation strategies
  - Federal Information Security Management Act (FISMA) & Privacy Management
  - Privacy Act of 1974 & Computer Matching and Privacy Protection Act
  - Office of Management & Budget (OMB) Memoranda
  - National Institute of Standards & Technology (NIST)

Challenges & Key Principles of the Federal Government's Cybersecurity Strategy* include:

1. Protecting Data: Better protect data at rest and in transit.
2. Improving Situational Awareness: Improve indication and warning.
3. Increasing Cybersecurity Proficiency: Ensure a robust capacity to recruit and retain cybersecurity personnel.
4. Increase Awareness: improve overall risk awareness by all users.
5. Standardizing and Automating Processes: Decrease time needed to manage configurations and patch vulnerabilities.
6. Controlling, Containing, and Recovering from Incidents: Contain malware proliferation, privilege escalation, and lateral movement. Quickly identify and resolve events and incidents.
7. Strengthening Systems Lifecycle Security: Increase inherent security of platforms by buying more secure systems and retiring legacy systems in a timely manner.
8. Reducing Attack Surfaces: Decrease complexity and number of things defenders need to protect.

**SOURCE - OMB FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity, 12 JUN 2015*

Compliance Matrix

#	Principles of the Federal Government's Cybersecurity Strategy	FISMA & Privacy Mgmt	Privacy Act & CMPPA	OMB	NIST
1	Protecting Data		X		
2	Improving Situational Awareness			X	
3	Increasing Cybersecurity Proficiency			X	
4	Increase Awareness	X	X	X	X
5	Standardizing and Automating Processes			X	X
6	Controlling, Containing, and Recovering from Incidents	X		X	
7	Strengthening Systems Lifecycle Security	X	X		X
8	Reducing Attack Surfaces	X	X		X

Questions?

Contact Information

Primary Contact
Marcela Price Souaya
Do Not Pay (DNP) Senior Privacy Analyst
202-504-3525
marcela.souaya@fiscal.treasury.gov

Secondary Contact
Omazi Boykin
DNP Privacy Analyst
202-504-3686
omazi.boykin@fiscal.treasury.gov

Do Not Pay Business Center Support
donotpay@stls.frb.org
1-855-837-4391

www.donotpay.treas.gov

Sign up for our mailing list to receive updates on new functionality and data sources or to schedule a demo.
http://www.donotpay.treas.gov/MailingList.htm

Resources

- **OMB Memoranda**
  - M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices
  - M-10-23, Guidance for Agency Use of Third-Party Websites and Applications
  - M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
  - M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- **NIST Special Publication (SP)**
  - 800-53 Rev. 4, Appendix J of Security Controls for Federal Information Systems and Organizations
  - NIST IR 8062, Privacy Risk Management for Federal Information Systems