PSIA Update

November 28, 2013

Jason Testart, IST

Current PSIA Format

A. Proposal (completed by project team)
B. Privacy Review (completed by Privacy Officer)
C. Security Review (completed by ISS)
D. Risk Mitigation documentation (completed by project team)
E. Verification Approval

Issues with current format

- Impossible to answer all questions, initially
- Unclear if entire document is appropriate for all projects
- No differentiation between build vs. buy
- How do we apply it to distributed systems? (e.g. Web Services/SOA architecture)
- What about additions?

PM Methodology

- Initiation
- High Level Planning
- Detailed Planning
- Execution
- Closure

SDLC

- Analysis & Requirements
- Design & Development
- Test
- Implementation
- Maintenance

New PSIA Format

- Work with PM and SDLC
- Needs sign-offs at different stages
- Encourage good systems documentation
- Checklist approach?
  - Less duplication
  - Helpful for other compliance requirements
  - Helpful for risk management

Goal

- Privacy/Security assessment should be able to be performed on project documentation
- So….
- PSIA should document questions that the docs need to answer

Proposed PSIA Process

Stage of Initiative	Privacy Action(s)	Security Action(s)	Sign-off?
Proposal/Business Case	Review/Assess	Review	Sponsor + Privacy
Solution Design (or "RFP Response")	Review/Assess	Review/Assess	Sponsor/Project Team + Privacy + Security
Development/Pre-production		Review/Assess	Project Team + Security
Implementation/Production	Review	Review	Sponsor + Project Team + Privacy + Security

Still Pondering…

- SOA model?
- Changes?