INDIANA UNIVERSITY

17d – Program Gap Analysis

Action Item Template Response

General Action Item Information

Action Item Number: 17d
Action Item Short Name: Information Security and Privacy Program
Dependencies with other EP Action Items: 17
Implementation leader (name & email): Tom Davis (tdavis@iu.edu)

I. DESCRIBE YOUR PLANS FOR IMPLEMENTING THIS ACTION.

A gap analysis will be performed while the program is being developed to identify information protection safeguards that need additional attention. This analysis will be based on well-established, industry-wide security and privacy principles and standards. Gaps identified, listed by program domain:

Risk assessment and treatment

- Risk assessment manager *(Priority: Medium)*
- Metrics and key indicators for self-assessment and decision-making
- SCADA security assessment

Policy

- Committee of Data Stewards (CDS) information governance policy and standards
- Information Security Policy and Standards

Organization

- Chief Privacy Officer *(Priority: Low)*

Asset Management

- Asset Tracking Product *(Priority: High)*

Human Resources

- Employee and contractor background checks
- See *Empowering People* Action 18 - Security and Privacy Awareness

Physical and Environmental

- Physical security of network wiring closets (10-year network master plan)

Communications and Operations Management

- Departmental firewalls (10-year network master plan)
- Enhanced capacity network intrusion detection systems (NIDS) (10-year network master plan)
- Cryptographically secure DNS (DNSSEC)
- IPv6 security plan
- Security event management/correlation system *(Priority: Low)*

Identity and Access Control

- Two-factor authentication *(Priority: Medium)*
- Network access control (NAC) *(Priority: Low)*

Information Systems Acquisition, Development, and Maintenance

- Whole-disk encryption product license (separate budget)
- Host-based intrusion detection systems (IDS)/intrusion prevention systems (IPS) *(Priority: Medium)*
- Host-based file integrity monitoring system *(Priority: Medium)*
- Data sanitization product *(Priority: High)*
- Patch management for operating systems and utilities (Shavlik renewal) *(Priority: High)*
- Patch management for third-party software *(Priority: High)*
- see *Empowering People* Action 19 - Data Storage and Protection

Business Continuity Management

- see *Empowering People* Action 20 - Business Continuity and Disaster Recovery

Compliance

- Review compliance responsibilities and adherence
- Data loss prevention product *(Priority: High)*
- Host-based sensitive data detection (Identity Finder renewal) *(Priority: High)*

II. WHAT ARE THE POLICY AND PRACTICE IMPLICATIONS OF YOUR PLANS?

Administrative, technical, and physical safeguards - including policies and standards - will be modified and/or established as the program is developed and implemented. Policies will be routed through the normal policy approval process.

III. IDENTIFY STAKEHOLDERS.

It must be reviewed by a number of groups at the university, including Internal Audit, Legal Counsel, Committee of Data Stewards, Data Managers, LSPs, campus CIOs, IUPUI technology deans, IUPUI Faculty Council technology subcommittee, IUB Faculty Council policy subcommittee, Research Compliance, and possibly others.