Name of Proposal: University-wide Information Technology Security Infrastructure

Academic Division/Area: Provost / Information Technology Services

Priority # 1

Overview – URI has a number of security products and practices in place to protect its Information Technology services. However, a consistent Security Infrastructure needs to be fully deployed throughout the University. Policies that are currently in draft form need to be finalized, approved and implemented with the cooperation of all Information Technology Service areas, including services delivered by our colleges and administrative areas.

ITS Security has been identified as a key component of the IT Strategic Plan. ITS Security is critical as URI will be the custodian of data that has or will have both FERPA and HIPAA requirements.

1. A. Please briefly describe the process and timeline as to how these new funding priorities were developed or derived?

IT Security is a changing, challenging and threatening field with hazards emanating from across the globe. To keep pace in this cyber-war, the infrastructure requests are designed to meet the current and projected threats that will be posed to the University.

B. What processes or incentives have been considered to encourage reallocation from within the division/unit?

ITS continues to provide Security support but requires additional funding in order to accomplish these strategic initiatives.

1. Please identify what is being requested, associated costs, possibility of alternative (partial) funding source(s) and/or any match funding, and the rationale for each requested item. Use as much space as needed. Please indicate also any possibility of alternative or match funding.

ITS is requesting $260,000 to purchase a series of hardware and software systems to improve the Information Technology Security Infrastructure at URI.

The steps will include the following:
- Develop an Information Security Program
  - Centralized depository of documented policies and procedures Business Continuity Plan
2. **Risk Management Assessments**
   - Implement Vulnerability Assessment and Remediation Program
   - Patch Management System for Operating Systems and Applications
   - Security Configuration Controls and Management
   - Vulnerability Management for Security Compliance
   - End-Point Protection Management
     - Manage multiple 3rd Party security clients

URI must have a solid Security Infrastructure to protect the University and respond to the increase in cyber threats and regulations. A breach or intrusion on the URI data and infrastructure would result in loss of computer facilities, imposition of fines and probably most importantly, the loss of reputation.

*This proposal is a companion to the Single Directory Structure proposal since the implementation of an ITS Security Infrastructure is facilitated by a single authoritative directory.*

2. **Is this request strategic and how does the request support or relate to URI’s Strategic Academic Plan?**

Yes, this strategic request supports both the Academic and IT Strategic Plans by positioning technology services, both ITS and outside ITS to help grow the University’s Global presence (Goal 3, Academic Plan) while continuing to meet the increasing challenges of security the University’s intellectual property.

3. **How does the request provide additional benefit to URI? (Enrollment, student services, condition of campus, fundraising/development, public relations, etc.)**

In all categories listed above, the University must be able to deliver a solid security infrastructure which creates a safe-computing environment.

4. **Please provide any data (including benchmark data) relative to the request OR a statement as to why no benchmark data is available.**

Assessing IT security risk is often an indicator of health information security practices. In 2016, 68% of peer institutions have had an IT security risk assessment completed. URI has not conducted an IT security risk assessment.

Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources.

Attackers have access to the same information and can take advantage of gaps between the
appearance of new knowledge and remediation. For example, when researchers report new vulnerabilities, a race starts among all parties, including: attackers (to “weaponize”, deploy an attack, exploit); vendors (to develop, deploy patches or signatures and updates), and defenders (to assess risk, regression-test patches, install).

Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, and sometimes-uncertain side effects.

5. Please complete and enclose the cost summary excel document from the Budget Office.