| Agency | Project | FY2005-06 | FY2006-07 |
|---|---|---|---|
| DAS - CIO | Security Audits | $ 50,000 | $ 50,000 |

**SUMMARY OF REQUEST** (Executive Summary from the Proposal)

The purpose of this project is to engage a qualified firm to conduct annual security audits / assessments of the information technology infrastructure for state government. Topics of interest include network security, wireless security, application security, and security policies and procedures. The exact scope of each security assessment will focus on one or more of these areas. The Security Work Group will help set priorities and define the scope of work for each assessment.

The NITC security policies (Information Security Management Policy) provide guidance for establishing effective security programs. One requirement is to conduct regular security audits. The Network Security Policy states, "An audit of network security should be conducted annually."

The HIPAA (Health Insurance Portability and Accountability Act) proposed rule for Security and Electronic Signature Standards (45 CFR Part 142) imposes a comprehensive set of security requirements for "covered entities" that "electronically maintain or transmit any health information relating to an individual." The regulations pertaining to "Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability" includes a requirement for "Security Testing." Given the breadth of HIPAA requirements and the potential penalties for violators, state government requires an independent evaluation of compliance efforts.

Guidelines pertaining to federal Bioterrorism Preparedness and Response grants require "regular independent validataion and verification of Internet security, vulnerability assessment, and security and continuity of operations…" (Critical Capacity #13, Focus Area E – Health Alert Network / Communications and Information Technology).

The National Strategy to Secure Cyberspace recommends that state and local governments "establish IT security programs … including awareness, audits, and standards."

In 2003, the Office of the CIO engaged Omnitech Corporation to conduct an external perimeter security sweep of the state's network. The initial evaluation took place during April to June of 2003. This included an automated vulnerability scan and testing of devices exposed to the Internet. In March 2004, Omnitect conducted a second vulnerability scan of the state's network.

**FUNDING SUMMARY**

The budget request is for $50,000 per year in cash fund authority. The source of cash fund will be the Information Technology Infrastructure Fund. Effort will be made to identify additional funding sources.

**PROJECT SCORE**

| Section | Reviewer 1 | Reviewer 2 | Reviewer 3 | **Mean** | Maximum Possible |
|---|---|---|---|---|---|
| III: Goals, Objectives, and Projected Outcomes | 12 | 14 | 14 | 13.3 | 15 |
| IV: Project Justification / Business Case | 23 | 24 | 24 | 23.7 | 25 |
| V: Technical Impact | 18 | 19 | 19 | 18.7 | 20 |
| IV: Preliminary Plan for Implementation | 7 | 10 | 9 | 8.7 | 10 |
| VII: Risk Assessment | 8 | 9 | 9 | 8.7 | 10 |
| VIII: Financial Analysis and Budget | 17 | 19 | 20 | 18.7 | 20 |
| | | | **TOTAL** | **92** | 100 |

**REVIEWER COMMENTS**

| Section | Strengths | Weaknesses |
|---|---|---|
| III: Goals, Objectives, and Projected Outcomes | - Very good list of goals, objectives, etc. I recommend this be expanded to include a risk-assessment of any identified vulnerabilities. We'd then not only know what might happen if something is not fixed but we'd also know the odds of it happening at all.<br>- Clear and concise. | - While this contains a clear statement of benefit to the state agencies, isn't there also a case to be made for the "protection" and confidence of the "citizenry" who also directly and indirectly benefit? |
| IV: Project Justification / Business Case | - We just need to make sure that we get what we pay for in this area (i.e. security assessments) | - Item 5 - might it build a better case if you noted that this a foundation step toward building a security program? What's proposed would be more efficient than individual activities, more comprehensive and objective, and provide a better roadmap for the state. |
| V: Technical Impact | - This project can, conceivably, have a major technical impact on other projects if installed features and functionality prove to contain major security flaws. Accordingly, this project can have a very long arm into all aspects of information technology. | - In Item 8 - "Project will help with implementing security policies" should be "will provide strategic and tactical inputs for inclusion in framing security policies"? |
| VI: Preliminary Plan for Implementation | - I appreciate the thoroughness of the Preliminary Implementation Plan although I personally would like to see a more aggressive schedule. | - Item 10. Given the urgency, importance and statute issues with this project, why wait until Nov 2005 to start? |
| VII: Risk Assessment | | - Item 14 - to get "buy-in" should some form on educational awareness and implication to the stakeholders (business and I/T) be part of risk mitigation? Point is to get them to become the partners in the process. |
| VIII: Financial Analysis and Budget | | |