Title of Nomination: Information Security Remediation

Project/System Manager: Renée Bourget

Job Title: Information Security Analyst

Agency: NC Department of State Treasurer

Department: Information Technology

Address: 325 North Salisbury Street

City: Raleigh

State: NC

Zip: 27603-1385

Phone: 919-733-7528

Fax: 919-733-4322

Email: Renee.Bourget@treasurer.state.nc.us

Category: Security and Business Continuity

Person Nominating(if different from above): George Bakolia

Title: SCIO

Address: Office of Information Technology Services, PO Box 17209

City Raleigh

State: NC

Zip: 27609

Phone: 919-981-2680

Fax 919-981-2680

Email: george.bakolia@ncmail.net

Executive Summary:

In May 2001, "hackers" broke into state agency computer systems in North Carolina in less than 30 minutes. Fortunately, these "hackers" were consultants hired by the North Carolina Office of the State Auditor to perform an external security assessment and were not malicious attackers bent on disrupting the state's services. The consultants were able to observe work being performed, captured user ID's and passwords, and were even successful in altering government records. At the conclusion of this statewide security assessment, four mission critical agencies, including the North Carolina Department of State Treasurer (NCDST), volunteered to have a more comprehensive internal security assessment performed.

For the NCDST, the comprehensive security assessment provided a clear understanding that it badly needed a complete Information Security Program. To that end, the NCDST initiated the **"Information Security Remediation"** project. The project's goal was to establish a comprehensive security program, including layered security controls both technical and non-technical, in a very short timeframe (four months). NCDST wanted to develop momentum for a continuing process of identifying, assessing, and mitigating risk, so that the benefit of the initial effort would be long lasting.

The project leveraged a security framework established by the State Office of Information Technology Services (ITS) and, from there, addressed security risks in all areas of NCDST. The project included:

- Establishing a formal **Information Security Framework** with defined roles and responsibilities, including appointment of a dedicated Information Security Officer (ISO).
- Developing Information Security **Policies, Standards, and Procedures,** including an enterprise-wide review and approval process.
- Building a **Secure Network Architecture** with layered security and internal network zoning.
- Deploying an **Intrusion Detection System (IDS).**
- **Securing Host Computers** and actively managing vulnerabilities.
- Performing an **Application Architecture Security Assessment** to look closely for potential vulnerabilities in critical applications and the supporting architecture.
- Delivering formal **Security Awareness Training** to all 300 NCDST employees.
- Delivering **Secure Application Development Training** to all application development personnel.
- Creating an **Incident Response Process** that is coordinated with ITS and the State Bureau of Investigation.

The Security Remediation Project began October 2002, and ended February 2003, (as shown below) however, the program it established continues. NCDST now has a defined Security Strategy that will be managed by a dedicated ISO, on-going tactical projects to support the strategy, and will be doing continuous monitoring and improvement to keep up with the rapid change of technology.