

## 2004 INNOVATIONS AWARDS PROGRAM

1. **Program Name** – NORTH CAROLINA AGENCY SECURITY ASSESSMENT PROJECT
2. **Administering Agency:** North Carolina Office of Information Technology Services
3. **Contact Person (Name and Title):** Ann Garrett, Chief Information Security Officer
4. **Address:** 4101 Mail Service Center, Raleigh, NC 27699-4101
5. **Telephone Number:** 919-981-5130
6. **FAX Number:** 919-981-5043
7. **E-mail Address:** Ann.Garrett@ncmail.net
8. **Web site Address:** <http://www.its.state.nc.us/>
9. **Please provide a two-sentence description of the program.**

Concerned with unknown levels of information technology security across state government, the North Carolina State Chief Information Officer (State CIO) supported legislation in the North Carolina General Assembly to require an assessment of the information technology security posture of twenty seven (27) North Carolina executive branch agencies on the state's information security policy framework, which is based on ISO 17799 security standards. The legislature enacted a law that also requires that the assessment process recommend funding for enterprise wide security programs as well as for individual agencies to close the information technology security gaps.

10. **How long has this program been operational (month and year)? Note: the program must be between 9 months and 5 years old on May 1, 2004 to be considered.**

The program, mandated by the N.C. General Assembly in May 2003, began its operations in August 2003.

11. **Why was the program created? (What problem[s] or issue[s] was it designed to address?)**

The State CIO and the General Assembly were concerned that executive branch agencies were implementing information security in an uneven fashion and lacked an overall understanding of their information technology security needs. An assessment would identify and prioritize information technology security spending requirements at the enterprise level.

12. **Describe the specific activities and operations of the program in chronological order.**

May 2003:

- Legislation mandating a security assessment of each executive branch agency is passed.

- The State CIO, through the North Carolina Office of Information Technology Services (ITS) Information Security Office, issues a scope statement seeking proposals from vendors to lead the assessment effort.

August 2003:

- The ITS Information Security Office awards the lead assessment contract to Gartner
- The Information Security Office and Gartner organize a project management office.
- The Information Security Office issues a scope statement for additional vendors, with information security expertise, to perform individual agency assessments.

September 2003:

- Gartner develops an assessment tool to be used in the assessments based on the ten domains in ISO 17799.
- The Information Security Office establishes a schedule for individual agency assessments.
- The Information Security Office awards contracts to vendors who will conduct individual agency assessments.
- The project management office holds information session for agencies and vendors to explain the process and the timeline

October – November 2003

- First phase agency assessments begin – vendors collect data and interview key agency employees at ten agencies.
- Agency documentation is reviewed for compliance with state enterprise-wide security standards.
- Preliminary findings made by agency assessors.
- Data is analyzed by project management office for accuracy and consistency.
- Agency assessment report drafted for each agency assessed.
- Assessed agencies review and respond to their draft assessment.

December 2003 – February 2004

- Process outlined above performed on a second group of seven agencies.

February – April 2004

- Process outlined above performed on a third, and final, group of ten agencies.

April – May 2004

- Project management office, using data from agency assessors, identifies areas where agencies fail to meet the state information security framework, establishes priorities for enterprise information security funding, and estimates hardware and software costs for agencies to improve information technology security. The project management office also recommends information security staffing requirements for agencies.
- The project management office drafts a summary, final report with an overview of the findings for the General Assembly.

- The State CIO and the North Carolina Information Resource Management Commission approve the final report for General Assembly delivery on May 4, 2004.

May – July 2004

- The General Assembly addresses the findings in the report.

**13. Why is the program a new and creative approach or method?**

For each government agency, the program measures a broad range of information security mechanisms against a statewide, enterprise framework. It further provides a systematic approach to prioritizing and funding security for the agencies and identifies enterprise-wide security measures that can reduce the overall cost of providing information technology security. Finally, the program establishes a baseline for all agencies to be measured against in the future.

**14. What were the program's start-up costs? (Provide details about specific purchases for this program, staffing needs and other financial expenditures, as well as existing materials, technology and staff already in place.)**

The State CIO set aside \$2 million in fund reserves to perform the assessments and to develop a tool that can be used in future years.

**15. What are the program's annual operational costs?**

Annual operational costs for the first year, including the development of the tool, were \$1.8 million. Ongoing costs in future years are estimated to be approximately \$750,000 to \$1,000,000.

**16. How is the program funded?**

See response to Question 14.

**17. Did this program require the passage of legislation, executive order or regulations? If YES, please indicate the citation number.**

Yes, N.C.G.S. §147-33.82(e1) states:

The State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the standards in each agency and an assessment of each agency's security organization, network security architecture, and current expenditures for information technology security. The assessment shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment. Not later than May 4, 2004, the Information Resources Management Commission and the State Chief Information Officer shall submit a public report that summarizes the status of the assessment, including the available estimates of additional funding needed to bring agencies into compliance, to the Joint Legislative Commission on Governmental Operations and shall provide updated assessment information by January 15 of each subsequent year.

**18. What equipment, technology and software are used to operate and administer this program?**

The assessment tool, developed by Gartner, was custom created for the State CIO, without using proprietary software. Rather, the tool uses Microsoft Excel. Microsoft Access is used to perform the statistical analysis. The tool and other project documentation can be viewed at <http://www.its.state.nc.us/support/Security/SecurityAssessment.asp>

**19. To the best of your knowledge, did this program originate in your state? If YES, please indicate the innovator's name, present address, telephone number and e-mail address.**

To the best of our knowledge, this program is the only state-wide program of its kind. Other states are watching this project closely and have asked for assistance in setting up their own, similar assessments.

**20. Are you aware of similar programs in other states? If YES, which ones and how does this program differ?**

We are not aware of similar programs in other states.

**21. Has the program been fully implemented? If NO, what actions remain to be taken?**

YES: The legislation mandating the program requires annual security assessments of all agencies. ITS has developed a tool that agencies will be able to use in the future to reflect changes to their information technology security programs.

**22. Briefly evaluate (pro and con) the program's effectiveness in addressing the defined problem[s] or issue[s]. Provide tangible examples.**

The program has raised awareness of the importance of information technology security at all levels of government. The individual agency assessments are, in essence, detailed plans for future improvements, and the focus on enterprise-wide resolution of issues has reduced the funding requirements, creating economies of scale.

**23. How has the program grown and/or changed since its inception?**

The program is one of continuous improvement: the assessment tool is designed to be refined as time progresses, adjusting its questions as information technology security advances.

**24. What limitations or obstacles might other states expect to encounter if they attempt to adopt this program?**

It is critical to have a qualified statistician to normalize the data, so that each agency is reviewed fairly and even-handedly.

Most importantly, however, the program would be extremely difficult to manage if a state's information technology program is not centralized. North Carolina has a centralized system through the North Carolina Office of Information Technology Services. It further has enterprise-wide oversight through the North Carolina Information Resource Management Commission.

Finally, although North Carolina law protects information regarding information technology security matters from disclosure, the inadvertent release of the assessments to the public could expose agencies to breaches that exploit the vulnerabilities of their systems.

**Add space as appropriate to this form. When complete, return to:**

**CSG Innovations Awards 2004**  
**The Council of State Governments**  
**2760 Research Park Drive, P.O. Box 11910**  
**Lexington, KY 40578-1910**  
[innovations@csg.org](mailto:innovations@csg.org)

**DEADLINE: All original applications must be received by April 20, 2004, to be considered for an Innovations Award for 2004.**  
**ApplicationForm04.doc**