

2005 INNOVATIONS AWARDS PROGRAM

APPLICATION

Deadline: April 4, 2005

Be advised that CSG reserves the right to use or publish in other CSG products and services the information that you provide in this Innovations Awards Program Application. If you object to CSG potentially using or publishing the information contained in this application in other CSG products and services, please advise us in a separate attachment to your program's application.

1. Program Name

Garden State Network Enterprise Intrusion Detection Project

2. Administering Agency

New Jersey Office of Information Technology

3. Contact Person (Name and Title)

Anna Thomas, Chief of Strategic Development and Digital Communications

4. Address

300 Riverview Plaza
Trenton, NJ 08625

5. Telephone Number

609-633-9032

6. FAX Number

609-633-8888

7. E-mail Address

anna.thomas@oit.state.nj.us

8. Web site Address

<http://www.nj.gov/it>

9. Please provide a two-sentence description of the program.

The state of New Jersey has partnered with the U.S. Army Communications-Electronics Command Research, Development, and Engineering Center (CERDEC) to research and analyze the state's networks for the development of an intrusion detection system to thwart cyber-terrorists. The Cooperative Research and Development Agreement (CRADA) between New Jersey and CERDEC defined the operations and architecture needed to deploy an intrusion detection and response program for the state's executive branch, including host-based intrusion detection systems, network-based intrusion detection systems, and security information management systems.

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, 2005 to be considered.**

The cooperative research and development agreement was signed on March 28, 2003.

11. Why was the program created? What problem[s] or issue[s] was it designed to address? **Indicate how the program applies to the “change driver” that you listed above.**

OIT was very excited to begin this innovative working arrangement that allowed the state of New Jersey to take advantage of the extensive experience and expertise of the U.S. Army in developing mechanisms to protect critical, confidential data.

With more and more people using state government online services, the need to protect our infrastructure has never been more vital. More than one million citizens access our Web site each month to get information and conduct business with the state. They have completed more than \$1 billion dollars in transactions using state of New Jersey online services.

If any of these systems are attacked, damaged, or destroyed, OIT must be prepared to bring them back online quickly. Technology is the driving force behind most state services. They could not be delivered without the state’s computer systems.

In recent years, the way business is done has dramatically changed in both government and the commercial sector. Take retail, for example. People expect to be able to buy anything online, from shoes, to books and DVDs, to cars, or even a house. They expect to do so securely and privately.

They bring those same expectations when they are doing business with government. They want to be able to apply for tax rebates, or register their car online, or access all kinds of information and services, in a private, secure, customer friendly environment.

A comprehensive intrusion detection program is a key component in our homeland security plans to protect our IT infrastructure from cyber-terrorism. However, OIT recognized that there are a number of technical and operational challenges associated with the implementation of an effective enterprise-wide intrusion detection and response capability.

Choosing an effective IDS from the myriad of vendors to fit an organization’s needs is difficult. Once in place, inherent incompatibility of intrusion detection products from different vendors makes it difficult to centrally manage and monitor possible incidents. The traffic from multiple distributed IDS is often too large and riddled with unneeded information to get a comprehensive whole picture. Event data flowing from disparate IDS products need to be correlated and reduced to provide a means to determine incidents effectively so that a proper reaction can occur.

To properly manage risk, an organization must have a complete incidence response capability that can react to threats as they arise across the entire enterprise. CERDEC has the experience and knowledge to assist OIT in making those proper decisions.

12. Describe the specific activities and operations of the program in chronological order. The project began with the creation of a project plan. The plan set a schedule and milestones, allowing for weekly status reports and action item tracking.

The second step was the definition of requirements. A network survey and critical asset survey was conducted to gather information on the current state of the Garden State Network, New Jersey's wide area network. Data, such as network topology, line speeds, number of hosts, firewall placement, and network traffic statistics, are essential to the proper design of an intrusion detection solution. The surveys were then analyzed to define the requirements.

After extensive research of IDS products, the CERDEC team conducted an evaluation of the major candidates according to their ability to meet the network requirements.

Next, a concept of operations was created to outline processes, procedures, staffing, and job functions for the operations and management of the IDS program.

Finally, the CERDEC team designed a technical architecture including IDS placement, data transmission plans, SIM integration, and Security Operations Center components.

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

The program is CERDEC's first research partnership with a state government. CERDEC offers non-federal partners access to a wide range of expertise in many disciplines. This technical expertise is leveraged to meet state of New Jersey information technology and infrastructure objectives.

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 total cost of the project from project plan creation to IDS Architecture creation was \$229,000. These funds were used to reimburse CERDEC for costs incurred during the course of the project. The cost was minimal as OIT was able to leverage so much of CERDEC existing knowledge and products, as was the purpose of the CRADA.

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

OIT has not yet selected a vendor for the IDS. The implementation of the system will include a substantial upfront cost and then maintenance and licensing costs going forward.

16. How is the program funded?

The Office of Information Technology used funds from its budget to cover the \$229,000 start up costs. OIT is seeking federal homeland security grant funding for the implementation of the IDS.

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

The Cooperative Research and Development Agreement was authorized and encouraged by the Federal Technology Transfer Act of 1986 (P.L. 99-502) and implemented by Executive Order 12591 (April 10, 1987). Congress, in enacting the law, found that federal laboratory developments should be made accessible to private industry and state and local governments to improve the economic, environmental, and social well-being of the United States by stimulating use of federally-funded technology developments. The Act gives each federal agency the authority to enter into CRADAs with state governments to provide personnel, services, property, facilities, equipment, or other resources.

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

The technical components of the program include host-based intrusion detection systems, network-based intrusion detection systems, and security information management systems.

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.

Yes.

Charles S. Dawson, Chief Information Officer/Chief Technology Officer
NJ Office of Information Technology
300 Riverview Plaza
Trenton, NJ 08625

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

No. To the best of our knowledge, the CRADA is a first-of-its-kind partnership between the U.S. Army and a state government for the development of an enterprise intrusion detection system.

21. Has the program been fully implemented? If NO, what actions remain to be taken?
The IDS implementation is the remaining step.

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

The CRADA has been an incredibly cost effective solution for the NJ Office of Information Technology. Through the efforts of the CERDEC team, OIT has gained policies, procedures, and network documentation that did not previously exist. The architecture document sets forth a path to an IDS solution that avoids many of the shortcomings of a quick fix, vendor-installed solution.

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

Due to the close ties developed between OIT and CERDEC through the CRADA, we were able to establish an outstanding working relationship for the future. In Fall 2004,

the Office of Information Technology created the multi-state, multi-city Partnership on Secure Information Infrastructure Technologies or POSIIT. The POSIIT partnership builds upon and leverages the results of the CRADA.

The POSIIT partners are a consortium of state and municipal governments, CERDEC, Monmouth University, and the National Association of State Chief Information Officers (NASCIO). The state government partners are Connecticut, Delaware, Kansas, Michigan, Missouri, Nevada, New Jersey, Pennsylvania, and Rhode Island. The city government partners are Camden (NJ), Las Vegas, Philadelphia, and Providence. The New Jersey Office of Information Technology will provide leadership for the state/city partners.

POSIIT's proposed project will harness best practices to deliver a multifaceted solution. The centerpiece of our solution is a dashboard with a unique, correlated view of cross-network attacks and vulnerability aggregation. The dashboard will be well tested through an interactive simulation and a Vulnerability Assessment Program (VAP) that will speed the training and preparation of member organizations. The pilot will also incorporate a set of tools and reports as part of a robust cyber security strategy.

The POSIIT team applied for grant money from the Homeland Security Advanced Research Projects Agency. The proposal was deemed "selectable" by the HSARPA and OIT will be promoting the project at the NASCIO D.C. Fly-In this May.

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

OIT has been limited in its ability to swiftly implement the IDS architecture due to budgetary difficulties. Other states may face obstacles in gathering the requirements in the survey stage depending on how their network is managed. A state with many separate agency infrastructures may face difficulties. New Jersey is fortunate that its Garden State Network is gateway to all departmental online service offerings.

Add space as appropriate to this form. Return to:

CSG Innovations Awards 2005

The Council of State Governments

2760 Research Park Drive, P.O. Box 11910

Lexington, KY 40578-1910

innovations@csg.org