

**2005 Innovations Awards Program
APPLICATION**

Deadline: April 4, 2005

Be advised that CSG reserves the right 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

SC Information Sharing and Analysis Center (SC ISAC)

2. Administering Agency

South Carolina Budget and Control Board
Division of the State Chief Information Officer

3. Contact Person (Name and Title)

Larry Johnson, State CIO

4. Address

Division of the State Chief Information Officer
4430 Broad River Road
Columbia, South Carolina 29210

5. Telephone Number

(803)896-0400

6. FAX Number

(803)896-0091

7. E-mail Address

lajohns@cio.sc.gov

8. Web site Address

<http://www.Secure.SC.Gov>

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

The SC Information Sharing and Analysis Center (SC-ISAC) is a unique partnership designed to enhance coordination of investigation and intelligence information to detect, pre-empt, and prevent future cyber terrorist acts by combining resources, to include personnel, equipment, and information from the State Chief Information Officer (CIO), the South Carolina Law Enforcement Division (SLED), the United States Secret Services (USSS), the Multi-State ISAC, the US-CERT, and the Department of Homeland Security. The purpose of the SC-ISAC is, first, to assist members of the South Carolina government community in implementing proactive measures to reduce the risks of computer security incidents, and secondly, to assist that community in responding to such incidents when they occur.

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.

18 Months

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.

The complexity of computer and network infrastructures and the challenge of administration make it difficult to properly manage network security. Network and system administrators do not have sufficient staff resources and security practices in place to defend against and minimize damage due to hostile attacks by viruses, worms, politically motivated or terrorist attacks. As a result, there are a rising number of computer security incidents. In 1988, there were six incidents reported worldwide; in 2002, there were 82,094; and in 2003, there were 137,529 incidents reported according to Carnegie Mellon’s CERT/CC.

Previously the State had no coordinated effort to develop the skills needed to address these rising risks and the potential damages caused by these events. Each Agency or division is struggling to manage its own security events with limited resources and often untrained staff.

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

- Establish the South Carolina Information Sharing and Analysis Center (ISAC) to analyze and distribute information on security events, best practices, and awareness programs to federal, state, county, and local levels.
- Establish a State Computer Security Incident Response Team (SC CSIRT), creating a resource that can be leveraged across the State to limit damage and lessen the costs associated with the recovery from security events when they occur.
- Create a 24/7 Security Operations Center (SOC) to monitor and activate the CSIRT in the event of a security event. The centerpiece of the SOC will be a Security Information Management System (SIMS). By creating a central location for events to be recorded and monitored, the State will be the first with such a comprehensive view of the security posture of its network.

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

The South Carolina ISAC is one of the few cyber security efforts that encompass federal, state, county, local, and private resources. The approach uses the expert resources within each partner organization, leveraging what each does best. The team is strengthened by its involvement with the others, increasing the ability of the whole while not losing valuable time bringing the entire team up to expert level on every discipline. Along with this partnership, there will be state-of-the-art Security Information Management System (SIMS) deployed to monitor the state's network.

There will be sensors placed throughout the State's network giving real-time data to monitor and track security events acting as a tsunamis warning system. There be a central collection, monitoring, and analysis center, but each participating entity will be able to utilize the system to assess their own security posture or optionally have the CIO monitor their systems for them. Once an event has been identified, the CSIRT will be activated to assist the affected organization. The team is geographically distributed throughout the State which will shorten the response time and further reduce the cost of the incident. After triage has been completed, the South Carolina ISAC will sanitize the information and alert the community while ensuring all private information is stays confidential.

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.)

As a leader of technology in South Carolina government, the State CIO funded this program in order to assist the agencies with understanding the security issues and become better prepared to handle them. The CIO established three full-time positions to develop the basic groundwork; this included developing strategic plans, security policies and procedures, and establishing best practices. The Homeland Security Grant was used to fund many of the point products, training and tools needed for this effort. The South

Carolina CSIRT members are volunteer staff from the participating governmental entities. See item 18 for additional costs.

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

The only annual operating cost will be the 15% - 20% maintenance costs of the hardware and software purchased.

16. How is the program funded?

In the Department of Homeland Security (**DHS**) Grant 2004 Cycle, approximately \$481,000 was used to create and establish the South Carolina ISAC. The DHS Grant 2005 Cycle has just been awarded and will bring another \$420,000 to furthering the South Carolina ISAC efforts. A business model is being developed to offset the ongoing costs by providing additional services to the constituents participating in the partnership.

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

No. New legislation was passed to support this effort. The Homeland Security Bill which passed in 2002 required the State CIO to develop a Critical Information Technology Infrastructure Protection Plan (CITIPP). This was the heart of the push that led to this project. The proviso is Title 1 Administration of the Government Chapter 11, State Budget and Control Board Article 1, General Provisions, Section 1-11-435

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

- Forensic Server – Units (1) total cost \$10,000
used to support forensic activity to support ongoing security incidents.
- Network Sensors – Units (10) total cost \$140,000
sensors deployed to collect network activity to proactively alert network anomalies.
- Alert Communication Server – Units(1) total cost \$10,000
used to deploy alerts to different sector members
- PDA for Core CERT Team and Service for 13 months – Units (20) total cost \$16,500
on call units used for real time 24/7 notifications to response team
- Enterprise Sensor Servers (two) – Units (2) total cost \$20,000
needed to support in a High Availability (HA) environment the 24/7 sensors monitoring the state's critical infrastructure
- IDS Blade – Units (1) total cost \$19,750.00
Intrusion detection capabilities needed to monitor network at a hub of the state's network
- IDS appliance for adhoc mobile applications - Units(1) total cost \$8,750.00
Intrusion detection capabilities needed to monitor network at a hub of the state's network

- Syslog Server – Units (1) total cost \$4,995.00 used to support the logs generated by the IDS systems for further analysis
- Policy Manager Security – Units (1) total cost \$4,995.00 unit to enforce policy on the IDS
- IDS report server – Units (1) total cost \$4,995.00 server to generate detailed reports from IDS 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, as stated earlier, this program is a partnership emanating from the Homeland Security efforts in South Carolina. That partnership includes the State CIO, SLED, the Computer Crime Center, and the US Secret Service.

- Major Chip Johnson from the Computer Crime Center
 - Phone: (803)722-5868
 - Email : cjohnson@sled.sc.gov
- SAIC Neal Dolan from the US Secret Service.
 - Phone: (803)772-4015
 - Email : neal.dolan@uss.dhs.gov
- James MacDougall from the State CIO
 - Phone: (803)896-1660
 - Email : macdoug@cio.sc.gov

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

No.

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

No, there are two more phases yet to be implemented. The web site and email alert system which are the security awareness efforts of the South Carolina ISAC have been operational for a number of months. The next phases will be training and equipping the Computer Security Incident Response Team (CSIRT) and creating a statewide Security Incident Management System (SIMS) which will be the centerpiece of the Security Operations Center (SOC).

The CSIRT is made up of two major components, a private and a public side. Each team consists of approximately twenty to twenty-five security professionals from their respective constituents that will provide support in the event of a security incident. The teams have been meeting since last year and have been equipped with basic forensic tools. Beginning this month, each member will begin attending three weeks intense incident handling courses developed by the Carnegie Mellon University's Software Engineering Institute. Carnegie Mellon University, currently in partnership with the Department of Homeland Security, is running the US-CERT efforts.

The SOC portion of the ISAC will be manned twenty-four hours a day. Each participating Agency's infrastructure will be monitored from a command center within the SOC. Members of the CSIRT team will be able to identify and track security events using this system. It has built-in alert capabilities, remediation instructions, workflow, and trouble ticketing to assist the teams in handling any security event from initial discovery to fully archiving lessons learned. This system will be accessible from anywhere in the State by the members of the ISAC. It also has copious reporting capabilities to assist management in understanding the security posture of their respective environments.

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

As intruders use increasingly sophisticated attack tools, launch highly automated attacks that travel at Internet speed, and intentionally use attack techniques that make it difficult to understand the nature and source of the attacks, enterprise, real-time collaboration across response teams has become increasingly important. This collaboration will:

- support rapid and accurate diagnosis of a problem
- rapidly disseminate warnings of actual attacks across the community
- rapidly disseminate warnings of generic vulnerabilities across the community
- alert the enterprise community to suspicious activity and support collaborations that investigate and diagnose the activity
- provide information on mitigation and remediation strategies to combat attacks and threats
- minimize duplication of analysis effort across teams
- help leverage the technical knowledge that exists across the teams to limit damage and ensure continued operation of critical services

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

The program has grown to include more jurisdictions including programs from county sheriffs departments like Lexington County's Business Email Alert system and their secure internal communications forums for their RAPID group which is a criminal intelligence division. The sheer volume of interested personnel was not expected, but has been a welcomed problem. Changes have occurred as more and more people have joined the effort, things such as developing a center of excellence that would test and develop best practices and offer training to members of the ISAC.

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

Some of the bigger obstacles would be the territorial lines that are so prevalent in government. The whole issue of security concerns and making everyone feel comfortable opening up. Changing or building new processes in government that cut across

jurisdictional lines can be an obstacle, although this has gone much better than expected. Communication is the lynchpin to success.