2003 NASCIO Recognition Awards

NOMINATION FORM

Title of Nomination:	Enterprise Business Continuity Planning
Project/System Manager:	Mike Russo
Job Title:	Chief Information Security Officer
Agency:	State Technology Office
Department:	Office of Information Security
Address:	4030 Esplanade Way
City:	Tallahassee
State:	Florida
Zip:	32399-09050
Phone:	850 414-0157
Fax:	850 922-5162
Email:	mike.russo@myflorida.com

Category for judging: **9 – State IT Management Initiatives**

Person nominating **(if different than above):**	Jennifer Faul
Job Title:	Awards Coordinator
Address:	4030 Esplanade Way
City:	Tallahassee
State:	Florida
Zip:	32399
Phone:	850-410-0853
Fax:	850-922-5162
Email:	jennifer.faul@myflorida.com

ONE-PAGE EXECUTIVE SUMMARY

The State of Florida expanded their concept of Enterprise Business Continuity Planning with new breadth and depth of programs this year. Today the Florida state agencies and the citizens they serve depend heavily on access to electronic information, so when disaster strikes the computer network, it strikes the heart of state government. A disaster that weakens the foundation can spread quickly to bigger problems. Florida has historically been well prepared for disasters relating to hurricanes and floods; it now prepares itself for incidents caused by computer viruses and cyber-terrorism that can have the same if not greater impact than a natural disaster. The State Technology Office’s enterprise business continuity and disaster recovery program approaches the problem on two fronts. First, to have all agencies prepared to recovery from any disaster and second to address computer incidents swiftly and directly with the best resources available.

Computer Security Incident Response Teams Help Protect Florida’s Cyber Systems:

Newly formed Computer Security Incident Response Teams (CSIRT), made up of teams of employees from each state agency, were organized and received critical training on responding to computer security incidents. The training was provided by Carnegie Mellon University. These teams were created at the direction of Governor Jeb Bush as part of the Florida Infrastructure Protection Center.

"The creation of Computer Security Incident Response Teams within each of our state agencies is a key step to ensuring the safety and security of the cyber infrastructure within state government," Governor Jeb Bush said. "I am proud to report that Florida is the first state in the nation to create these teams enterprise wide."

Statewide Program for all Agencies Information Technology Disaster Recovery plans:

A statewide Continuity of Operations (COOP) program started in 2002 requiring all state agencies to review and complete a comprehensive disaster preparedness plan. To assist agencies with the development of the Vital Records and Databases Element, the Division of Emergency Management (DEM) and the State Technology Office (STO) Office of Information Security have partnered to assure an efficient and effective assessment and approval process for the Information Technology Disaster Recovery Plans (ITDRP).

Business continuity planning has always been “good business” and keeping services operating for the citizens of the State of Florida has always been of highest importance. Now, through newly developed COOP processes guidelines and new Enterprise Information Technology Disaster Recovery processes, guides and templates the state information technology officers have formed a closer partnership with the emergency coordinators to develop better COOP plans.

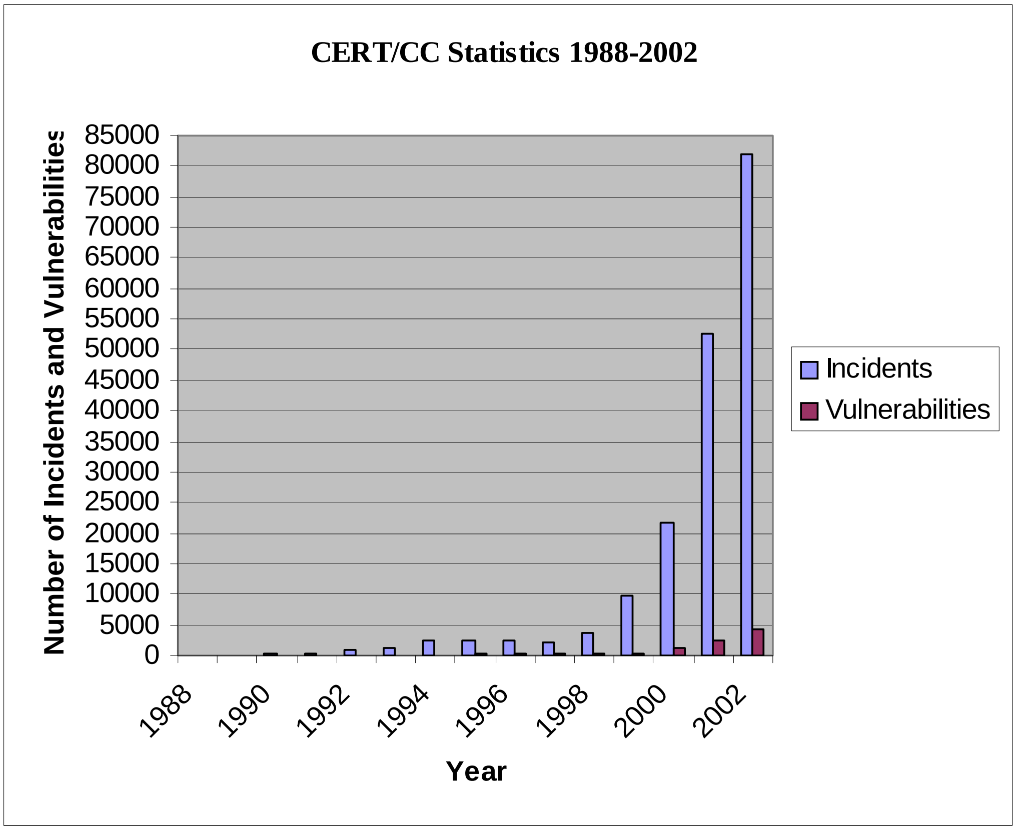
Written Justification

a) Description of project, including length of time in operation.

Computer Security Incident Response Teams Help Protect Florida’s Cyber Systems:

During the past year, Florida has worked hard to respond to the threat of terrorism, and as a result, the state is a safer place to live. One area that required additional attention is cyber security. Carnegie Mellon University's Computer Emergency Response Team (CERT) reports that in 2002 there were 82,094 reported cyber incidents — a 56 percent increase over the incidents reported for 2001.

Network Security Incidents 1988-2002



In order to counter the threat of cyber crime, the new program was put in place to ensure every system within each state agency is secure. This means not only to protect our systems from unlawful intrusion, but to react quickly to any potential failure or attack. To that end, the Legislature has created the Florida Infrastructure Protection Center (FIPC) within the Florida Department of Law Enforcement (FDLE).

The mission of the FIPC is to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a partnership between FDLE and the State Technology Office (STO). It is part of a broader initiative to secure all computer systems within Florida. During the past two years, great effort has been put forth by each state agency to shore up their networks and ensure their information and systems are protected. To learn more about the FIPC, please visit http://www.fdle.state.fl.us/Fc3/fipc.htm.

As you know, cyber security efforts are never complete. To keep the state networks and systems safe, we must be continuously dedicated to upgrading and testing those systems. Being prepared to respond to cyber incidents within every agency is critical. To ensure such preparation, Governor Jeb Bush directed the formal creation of **Computer Security Incident Response Teams (CSIRTs)** within each state agency.

CSIRTs are teams of employees within each agency that provide services and support for responding to computer security incidents. An incident could be caused by cyber terrorism, or by something as simple as a power outage. The CSIRT will protect, detect, analyze, and respond to an incident, thus limiting the damage done and lowering the cost of recovery. When computer security incidents occur, it will be critical for every agency to have an effective way to respond. Having a formally trained CSIRT will ensure a timely and efficient resolution.

The creation of this CSIRT formalized what many agencies already have in place. Each agency's CSIRT included current members of the agency's IT staff, human resources, legal counsel, and the Inspector General's office. Since most security incidents originate from internal sources, this team of experts will ensure an effective and correct response.

The FIPC contracted with Carnegie Mellon University's CERT to bring premier training to the state of Florida. This training was the first step in forming the new teams. The initial set of training occurred in early 2003. Each team received critical training for responding to computer security incidents. For more information on this training, please refer to the Carnegie Mellon website at http://www.cert.org/csirts/. .

Statewide Program for all Agencies Information Technology Disaster Recovery plans:

The Continuity of Operations (COOP) Implementation Guidance was issued September 9, 2002 by the Division of Emergency Management to provide instructions to the Executive Branch of the State of Florida to develop and implement disaster preparedness plans in accordance with the Florida Statues, Chapter 252.365: *Emergency coordination officers; disaster-preparedness plans*. One of the essential elements being reviewed in this guidance is the protection and recovery of Vital Records and Databases. The Division of Emergency Management (DEM) and the State Technology Office (STO) have partnered to assist the agencies in the planning and review of the essential elements.

This new program included:

1. **Best Practices IT Disaster Recovery Planning Guidance and Planning Template**

   The STO prepared a standard guidance document and planning template based on "Best Practice" IT Disaster Preparedness Planning (ITDRP) in Word format and several planning spreadsheets in Excel format. These templates are generic in nature and can easily be imported in automated planning tools such as Strohl Systems LDRPS or Sungard's PreCovery tool.

   The CIOs now have available to them a new ITDRP Guidance document as a reference guide of accepted practice areas for developing new ITDRPs.

2. Review of IT Disaster Recovery portion of COOP

The Division of Emergency Management and the State Technology Office teamed together to review the Information Technology portion of each agency's COOP. The two organizations shared common resources and information to make these reviews beneficial for the agencies success. The STO worked closely with each agency to review the agency's IT DRP plans in conjunction with the approval of the agency's overall COOP.

3. Alternate Site Capabilities

The State Technology Office led a multi-agency working team in developing an "Invitation to Negotiate" to provide updated pricing for alternate sites to recovery their critical processing needs. The goal was to consolidate their requirements and get the best process for these types of services.

b) Significance to the improvement of the operation of government.

The Florida Infrastructure Protection Center (FIPC) works to prevent, react and recover from acts of terrorism, sabotage, cyber crime and natural disasters. The creation of the CSIRTs will bolster the FIPC's current cyber security efforts.

The CSIRT will protect, detect, analyze and respond to a cyber incident, making for a more efficient and effective response within state agencies. The CSIRTs report cyber activity to the State Technology Office (STO), which will be responsible for escalating any potential criminal violations to the Florida Department of Law Enforcement.

Not all incidents can be prevented that is why the second program to create a near-term analysis of the state's IT Disaster Recovery Plans further ensures that state leaders fulfill their responsibility to protect critical state operations.

c) Benefits realized by service recipients, taxpayers, agency or state.

The creation of the CSIRT within each state agency takes Florida a giant step ahead in being prepared to protect the cyber infrastructure of the state agencies. The teams are now in place to continuously ensure that the very systems needed to provide services to the citizens of Florida will be operational.

The state is now working on creating 1 Enterprise IT Disaster Preparedness Plan versus 59 plus individual plans. Prior to the passing any additional legislation, 8 of the largest agencies combined their efforts to work to acquire alternate site capabilities for their mission critical functions. Rather than doing this as individual efforts they collaborated and did it with one set of resources and avoided 7 redundant sets of resources.

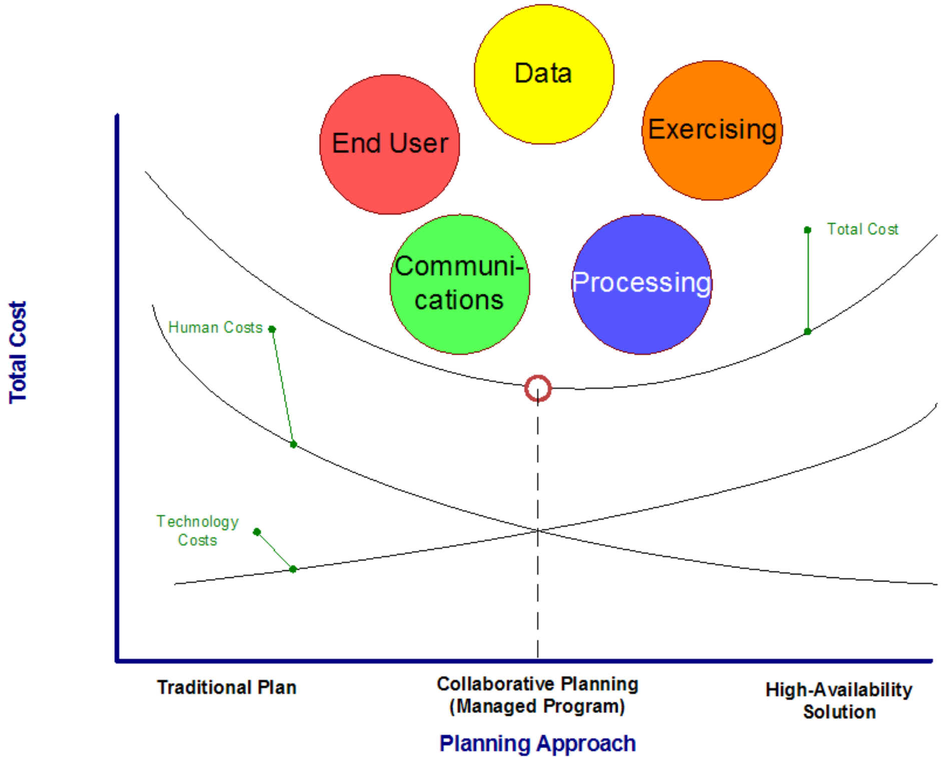
Prior to the Enterprise approach the Recovery Objectives were unknown. Of the agencies already included in the assurance objectives went from 30% known to 100%.

d) Return on investment, short-term/long-term payback (include summary calculations). Projects must exhibit measurable operational benefit.

- Recovery Objective's assurance increased to 100% versus previous level of 30%

- Saved over 2,400 labor hours of purchasing and administrative expense by creating 1 request for alternate sites versus 8 individual requests.
- Projected savings are to save over 20% in the Total Cost of Contracts for alternate site capabilities and emergency communication fees by taking an enterprise approach. (Refer to the following chart used as an aid to evaluate the optimum solution for each individual agency alternate site solution).

Charts, graphs, samples



The above chart was used as an aid to find the most cost effective solution for each agency’s IT Disaster Recovery Plan. Before throwing people or technology at the solution, each agency needed to understand how they would provide services to their end user, where their data would be restored, how they planned to exercise their program, how much emergency communications would cost, and how much processing power they really needed for their mission critical functions. By understanding the Total Cost of their program each agency was able to work toward their most optimal solution.