

**NASCIO Recognition Awards 2004**  
**Tennessee's 2003 Cyber Security & Business Continuity Project**

**Executive Summary**

With strong leadership support, Tennessee's Cyber Security and Business Continuity Project moved from talk to action this year.

The Cyber Security and Business Continuity Project is a full spectrum approach to protecting the State of Tennessee's infrastructure, communications, and computing power for assured business continuity. The program is meeting the challenge put forth by the State's IT Steering Committee (ISC), a joint Executive, Legislative, and Judicial committee, to improve both network security and the ability of state government to function in and through disasters or cyber attacks.

Over the past year, Tennessee has focused effort and resources to assure that our citizens can contact their government 24 hours per day for vital services. The value of the program to government continuity was proven in the first-ever printing of a payroll check under disaster conditions and in the coordinated response of the State and contractor teams in maintaining vital services when a devastating tornado struck Jackson, Tennessee's fifth largest city. The program is built on several tenets:

- **Strong Policy** - The ISC approved an ironclad security policy to assure the reliability, integrity, availability and confidentiality of the operations of government. This policy, known as Policy 13, protects networks and data concerning the citizens, ensures the privacy of protected health information mandated by federal law, and endorses establishment and enforcement of standards down to the desktop configuration level. Further, it promotes efficiencies to ensure the existing rate structures provide sufficient capacity to implement the policy. A Security Task Force was created to address the day-to-day implementation of the policy.
- **Education** – A comprehensive on line Cyber Academy was created to provide training for employees to receive a “network driver’s license” and continued training for employees and the general public. This Public-Private sharing is available to all our citizens.
- **Prioritized List of Requirements** – A continually refreshed list of cyber requirements is maintained by the security team to channel available resources to the most urgent needs. Addressing the requirements in incremental pieces of one-time and recurring funding allowed funding from grants, as well as internal sources.
- **Visible Symbol** – The State built a Network Operations and Security Center (NOSC) from the ground up. It functions as the Cyber Command Post of the State. The NOSC not only assures that attention is given to each issue, through the use of “stop light” type maps and digital dashboards, it also provides a visible symbol that IT leaders, Legislators, State executives and citizens can readily understand.
- **Disaster Exercises** – Tennessee has increased emphasis on disaster recovery planning and exercises. With increased Agency participation the State conducted expanded exercises. For the first time the State added printing to our capabilities as well as non-mainframe application recovery.

Cognizant that delays in applications such as driver's license or Children's Services are a source of frustration, and can be life threatening, the State maintains constant internal and external views of the service provided. A Children's Services caseworker relies on immediate information when entering a home situation. The approach and outcome for a child can be different on a first call at an address, as opposed to a repeated incident. The external view of interfaces assures that the State always sees and reacts to the citizen's view of government services. The internal view gives us that same constant visibility from the employee perspective. The Cyber Security and Business Continuity Project is assuring vital services are available and citizens can rely on a reliable interface to their government.

## NASCIO Recognition Awards 2004 Tennessee's 2003 Cyber Security & Business Continuity Project

The State of Tennessee's enterprise-caliber security program, led by the Office for Information Resources (OIR), has certainly moved from talk to action, with an aggressive list of accomplishments. There is nothing like a supportive leadership environment, a record-setting year of worldwide cyber-terrorism, two tornadoes and another two lightning strikes within a year to keep an organization's focus on cyber security and business continuity. This nomination encompasses initiatives beginning with a statewide assessment, formation of a rigorous Security Task Force, deployment of a first-class statewide Network Operations and Security Center (NOSC), and an online Cyber Academy that has been shared with private and public sectors. More importantly, the State met the challenge put forth by the state IT Steering Committee (ISC), a joint Executive, Legislative, and Judicial committee, and state leaders to improve support for disaster recovery funding and testing, business recovery and resumption, contingency planning, homeland security, bio-terrorism prevention, and health alerts.

### a) Description of project including length of time in operation

The depth of this project is shown in multiple segments below, each with descriptions and associated timeframes. In 2002, OIR wrapped up a statewide analysis that resulted in a gap assessment and a set of recommendations for future action. Action began immediately. The first IT Security Task Force (STF) was formed, with a group that takes this business seriously enough to have a monthly two-hour agenda which addresses: anti-virus statistics; stripped attachments; incident analysis, including valuation of lost productivity per incident (useful toward cyber Return on Investment (ROI) decisions); and a wide array of current issues, such as policies for wireless devices, cyber audit findings, Spam blocking, and patch management. In late 2002, the state's Chief Network Security Officer (CNSO) position was established to lead day-to-day implementation of STF direction.

**Policy Development.** The State formed a small but effective OIR Cyber Policy team – not only to guide the statewide rollout of a Policy-Procedures-Checklist-Audit program approved by the ISC, but also to ensure a classic checks-and-balances relationship with the critical OIR Operations and Infrastructure team. For even stronger checks and balances, the Policy and Quality Assurance team is the only group that can, in conjunction with the CNSO, resolve and close a security incident. And this can only after a post mortem with the full Operations team. This team gained agency and ISC approval for a far-reaching Cyber Security policy, as well as an Acceptable Use Policy (AUP) with teeth.

### Cyber Academy

In order to keep the friendliest possible face on AUP and other aspects of the new program, OIR's Policy team built a comprehensive online Cyber Academy as a training tool before employees can receive a "network drivers license." Cyber Academy is also available to the general public free-of-charge at [www.state.tn.us/finance/oir/ca/](http://www.state.tn.us/finance/oir/ca/) (please try this link). Tennessee feels this is a meaningful and genuine national model of the President's challenge for state governments to create public/private Sector sharing within the context of "The National Strategy to Secure Cyberspace," signed by President Bush in February 2003. Tennessee has now offered the Academy to all NASCIO Security Committee members, the Federal Homeland Security CIO, and in multiple states in the Speaker's Bureau and state/regional forums.

Every IT team wishes their state leaders had the backbone and vision to support a comprehensive policy to secure state networks and ensure their availability for daily interaction among government entities and citizens. Tennessee's leaders have exhibited this kind of commitment. From mid-2002 until fall-2003, the State's IT community campaigned hard; and in turn Tennessee's leaders supported the ironclad ISC security Policy 13. The State continues to carry the message that while our networks are strong our future security in response to the increasing threats is only as strong as the weakest link.

The State fostered a wide understanding that protecting all PC's from attack begins with a current operating system, supported with security upgrades and anti-virus software patched to the current level. As part of a public cyber security initiative "No PC Left Behind," the State succeeded, after a yearlong effort, in funding the replacement of 5,000 aging PCs and associated software (see Tennessee's associated article "PC Replacements a Bitter Pill You Must Swallow," TechTarget.com

[http://searchcio.techtarget.com/originalContent/0,289142,sid19\\_gci951655,00.html](http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci951655,00.html)).

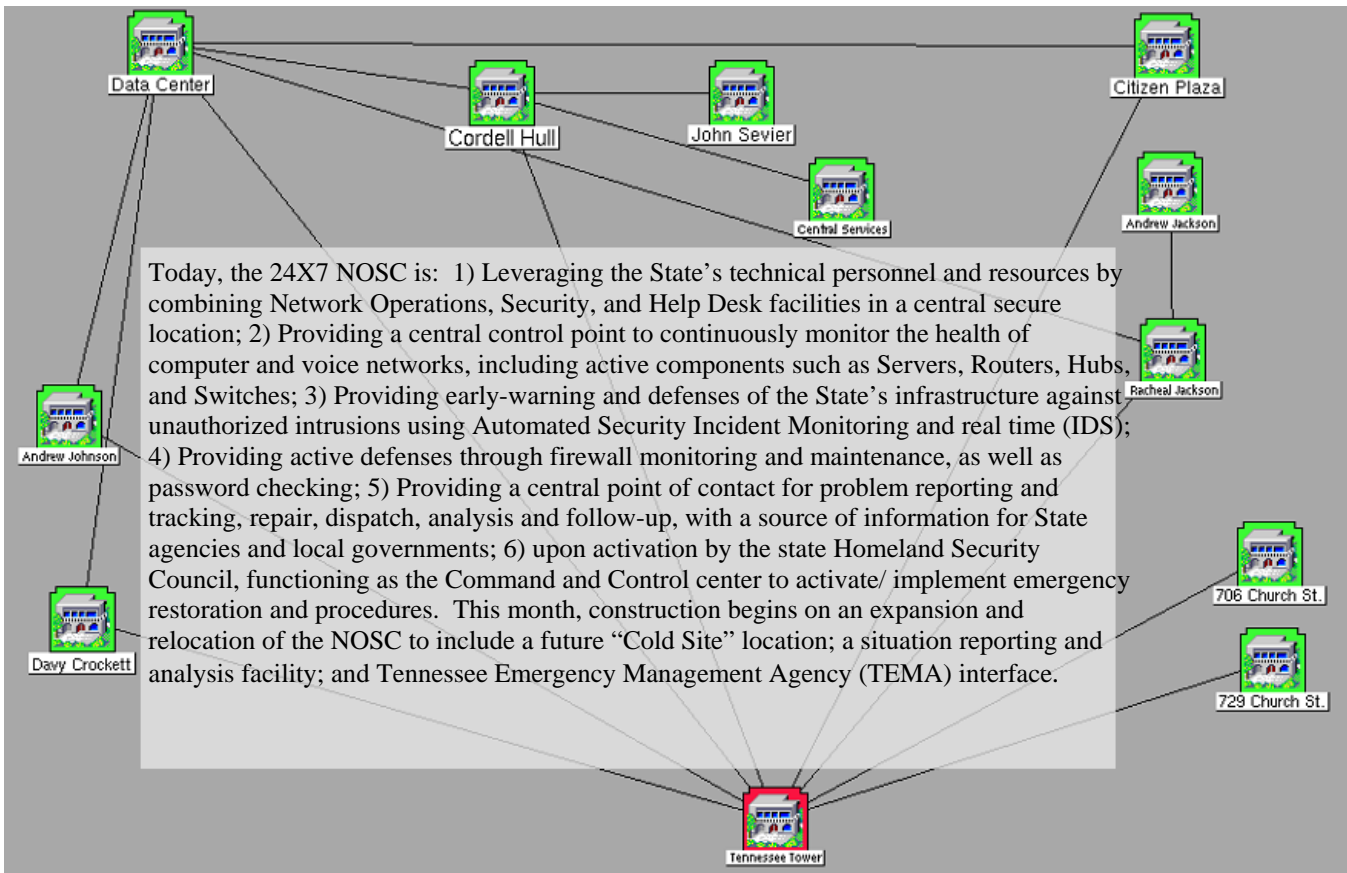
**Creation of a Prioritized List of Cyber Requirements.** We all know that if we need funding, our "elevator speech" must be ready. In 2003-4 the State developed a prioritized, top ten list of needs. By continuing to show compelling needs, the State has already funded the first six and modified the list again to keep added requests on the horizon. These future initiatives will further strengthen the State network in keeping with other enterprise-class state government networks of this caliber, and are prioritized in order of their merit, urgency, and necessity. Examples include: Intrusion Detection Systems, devices to secure the Nashville MAN (Metropolitan Area Network ) and regional data centers, 24X7 Network Security Monitoring, Workstation and Server Patch Management, AAA Authentication VPN, Network Forensic System, URL (Content) Filtering, Workstation Scanning, Independent Security Posture Assessment and Audit, and Workstation and Server Intrusion Prevention.

These requirements and initiatives were carefully defined in hopes of Federal cyber security funding, yet in full recognition that there is an important difference between one-time grant funding versus the reality of recurring support costs. So, the breakdown includes hardware, software and personnel resources, and funding shortfalls associated with each initiative. Exact detail on equipment types, vulnerabilities addressed and progress are protected as confidential information by Tennessee statute TCA 10-7-504. (This statutory remediation is another example, which was shared during US Congressional testimony, of how states can protect cyber interests.) The State has secured Buhrn Grants, grants from the Attorney General's office, and has used OIR internal funds.



**Just Do IT – Tennessee Builds a NOSC to Fight a Trojan Horse.** Sometimes leaders need to take a risk and push the train out of the station. The State built a visible symbol of our commitment to cyber security and erected a first-class Network Operations and Security Center (NOSC). The components include a "Command and Control" center with highly specialized staff work stations, which feature monitoring systems interfaced with large screen technology and Remedy Help Desk, and HP OpenView which tracks network security and E-Commerce WEB sites. Monitoring of State websites is accomplished on a Dashboard with Speedometers for Availability, Response Time, and Service Levels. A 'click' on a Speedometer provides in depth information about all, or individual, WEB sites for varying time frames. As implementation nears completion, the Center views 2,000 devices in 1,100 locations throughout the State of Tennessee.

A specialized feature for the state's Remedy Help Desk software was created to focus visibility on cyber-security incidents for agency IS Directors, and to allow tracking until closure. This feature also creates an "evidence quality" chain-of-custody for potential law enforcement use.



**Improve Awareness.** With the intense cyber incidents of 2003-4, OIR built an instant notification portal on the State's Intranet that would serve as a "layman friendly" translation of the real threat coming from the latest worm and recommend specific actions agencies should take. Now, a 24 X 7 capability exists for rapid-fire evaluation, with professionally rendered web posting of threats sent as e-mail to agencies, linking to the new Home Page devoted to Security Resources. Quality external links exist to CIRT, SANS and others. The leadership team of OIR hosted over 10 different statewide security protection conference calls with nearly all of the 46 state agencies, with SWAT team approaches to sharing IT staff to cover large incidents. Additional contract resources have been made available to small agencies at affordable vendor rates. An online listing of the status of virus protection and threats is available. This provides a ready source for statewide reference to fight potential infections.



The NOSC network management tools now enable it to serve effectively as a shared trouble documentation system, which allows agencies and the central OIR staff to collaborate on problems for quick resolution. The dashboards allow troubleshooters to "drill down" for more detail of each security issue for over 200 network equipment devices. Staff have been retrained and augmented with an emphasis on security and business continuity. At every seat in the NOSC, immediate references are built-in to indicate whom to notify in agencies, in the event warranty and repair coverage is needed.

The OIR Ops team built a communication and Action Plan to reduce the vulnerability to

attacks and intrusions. The State began with a dozen Intrusion Detection System (IDS) probes in 2002 and

shared the story of more than 6-700,000 daily hack attempts or sophisticated trace-routes. But knowing that IDS is ultimately just a blur on the windshield of cyber protection, serious analysis efforts began in mid-2003 by a select cyber architectural standards team to pulse the leading edge among affordable Network Prevention.

**Disaster Recovery/Business Continuity.** As another part of the effort, Tennessee improved Disaster Recover (DR) and Business Continuity, with an emphasis on added testing and documentation of DR plans. Building upon an inventory of 797 system applications that had already been rated as “Fatal, Critical, Marginal, or Manageable,” OIR challenged agencies to test more systems than the previous year. The State made a media event around the offsite printing of a payroll check for our state Commissioner of Finance – in the first-ever offsite-printed output for a 32-year-old payroll system. Our decisions for staffing in this area reflected genuine interest in improvement, and in early 2003 the State added experience in worldwide help desk, Intel and UNIX servers, DR and cold site testing. To expand Agency support and non-mainframe disaster efforts, in late 2003 the state committed another new full-time position with focused expertise in DR development and execution.

The State increased emphasis on semi-annual DR exercises. In the most effective DR and Business Continuity exercise ever in Tennessee’s history, 16 agencies participated in around-the-clock simulations. At kick-off, the technical and operations team retrieved backup tapes from the State’s secure offsite storage and dispatched to our recovery facility. In less than 24 hours, a new full mainframe and limited Unix environment was established. Customer agencies accessed data remotely, running vital programs to demonstrate that disaster plans and procedures worked. To address a shortcoming in previous planning, printing backup was added for the first time. The actual printing and delivery of a payroll check proved the State could maintain this vital government function (Tennessee prints 250,000 unemployment, 271,000 Child Welfare checks monthly).

## **b) Significance to the improvement of the operation of government**

The State’s Wide Area Network (WAN) interconnects Federal, State, county, and municipal users in over 1,400 locations statewide and Internet egress points located at the major hub sites across the State of Tennessee. The total number of users on the network is currently approximately 38,000 (including 8,000 Metropolitan Area Network [MAN] users), approximately 2,500 dial-up users, and 2,500 VPN users with Internet connections. The WAN is still growing at 20% per year - it includes a downtown campus fiber MAN at 12 state office buildings and the State’s Data Center. The OIR WAN Section supports 60 Tennessee Board of Regents locations across the state (colleges, universities, and technology centers), in addition to all state agencies on the WAN, and network systems and security services (security planning, consulting, firewall deployment, intrusion detection, access control lists, data transmission encryption, DNS, DHCP, network security monitoring, etc.)

Cognizant that delays in applications such as driver’s license or Children’s Services are a source of frustration, and can be life threatening, the State maintains constant internal and external views of the service provided. The external view our NOSC maintains of Web interfaces assures that the State always see and react to the citizen’s view of government services. The internal/intranet view gives us that same constant visibility from the employee perspective. The quantifiable evidence of application and website or network performance translates into more effective troubleshooting and a more reliable citizen interface.

The need for a broad spectrum of communications within the State of Tennessee’s WAN structure, with government agencies outside the WAN, and with citizens via the internet and web access creates a large and complex overall network structure. The overall WAN, MAN, LAN, Internet, web access structure is vulnerable to attacks and intrusions from numerous sources. The impact of attacks are now minimized even if targeted at a specific time or specific agency, server, network, or workstation. Other attacks that take over portions of the State of Tennessee’s networks for malicious or criminal purposes, or impair network effectiveness, have been reduced.

During an actual disaster and several major situations the DR processes and procedures proved the value of planning and exercise with customer/Agency involvement. Last spring a Tornado hit Jackson, the sixth largest city in Tennessee, and the disaster planning and procedures proved effective for both restoration of service, vendor coordination, and keeping government agencies and citizens involved and informed

### c) Benefits realized by service recipients, taxpayers, agency or State of Tennessee

A major benefit is the peace-of-mind created because Tennessee knows that service to citizens will be restored quickly in a disaster. The impact of a citizen not receiving a child care check, or a highway patrolmen not being able to instantly check criminal activity of a vehicle's occupant before approaching it, or of Children's Services not being able to access a case file related to a potentially life-threatening complaint can be devastating—the solution priceless.

Daily, our citizens benefit from the NOSC support of networks, websites, and intranet interfaces. The NOSC has greatly reduced downtime on the State's network by addressing issues before they are problems, through more effective triage of problems, and faster dispatch of the right crew to address any problem, network, equipment, or security issue. Constant website monitoring assures citizens can reach their government 24 X 7.

From the security view, over the past twelve months, incidents representing a loss of \$380,000 taxpayer dollars have been documented. A significantly greater amount has been avoided. In addition, the State confirmed annual savings through avoiding labor and overtime for security patches, by committing to replace outdated PCs and operating systems that are not capable of "push technology." Perhaps the greatest benefit realized is that staffing time lost decreased year-to-year.

### d) Return on investment, short-term/long-term

The investment of a year's disaster preparation is returned in less than 20 minutes of lost productivity from Tennessee's employees during a disaster. ROI is best addressed from a cost avoidance or loss avoidance perspective. The project allows Tennessee to provide essential services with minimum disruption during a limited disaster and most importantly to rapidly restore service when most needed, after a disaster. The investment in exercises is minimal. The state only pays \$13,000 per month or \$156,000 for a mainframe subscription, and \$8,000 per month or \$96,000 per year for the UNIX subscription annually in support of the exercises. Our offsite storage for the backup media costs are \$72,000 per year. Hot-site usage in case of a disaster is \$17,000 daily and cold-site occupancy costs only \$4,600 per day (after 6 consecutive months). Travel expenses for personnel and lodging are \$10,000 for each of our two trips to hot-sites are included the total investment. Thus the cost is \$344,000 per year to have the capability available and tested plus \$17,000 per day of use in an actual disaster.

The return for this investment is calculated from a number of components. First from a pure employee cost basis with the 40,000 plus employees of the State of Tennessee and their hourly wages, an hour of lost productivity is valued at \$750,000. With its emphasis on continuity and exercises, the longest that the State of Tennessee could imagine being down would be 36 hours as we implemented the continuity plan in a major disaster. Given the timing of the disaster that 36-hour period would include at most 15 work hours (Tennessee employee business day is 7.5 hours) for the average employee. By contrast, places like the Pentagon were still struggling to reestablish full continuity 5 days after the 11 September attack. A rough calculation based on recovery would show savings of over \$19,000,000 in a real emergency (3.5 days less at 7.5 hours per day and an economic impact of \$750,000 per hour). The return becomes much higher when one considers the interest which could be lost from not properly investing or managing funds during an extended outage.

The chart is based on the following assumptions:

1. Lost productivity costs \$5,625,000 per day ( $\$750,000/\text{hr} \times 7.5 \text{ hour day}$ )
2. In a disaster, productivity drops 100% on days 1, 2, & 3.
3. In a disaster, productivity drops 50% on day 4 and 25% on days 5-7.

