



## THE 50 STATES

November 2001

*The hole that Sept. 11 tore into the heart of our nation was an especially deep wound for state governments. New York, Pennsylvania and Virginia bore the direct brunt of the terrorists' blows, but state employees from Maine to Hawaii shared their grief, fear and sorrow as our nation's freedom and prosperity were challenged.*

*GCN/State & Local reporters asked officials in each state what special security measures their state took to protect government data in the wake of Sept. 11. Most states listed security at the top of their IT agenda long before September. For others, it was a wake-up call to tighten data security procedures.*

*State officials also talked about how technology helped them cope with disaster. New York officials, for instance, relied on geographic information systems to pinpoint state offices in Manhattan. Lacking a LAN, District of Columbia officials improvised an instant messaging system on the day of the attack to communicate quickly and quietly with agency employees.*

*A motto from Revolutionary War days said it best: United we stand; divided we fall. Several state officials reported that they felt a new spirit of cooperation between agencies, reminiscent of the year 2000 rollover. Turf battles were largely forgotten; state, local and federal agencies worked together to keep citizens calm, safe and sound. These strong, united states are then free to rally round another motto: Don't tread on me.*

### ALABAMA

**LET'S GO TO THE PHONES.** As a part of activating the emergency operations center, officials at the Emergency Management Agency stayed connected with local administrators through an 800-MHz statewide communication system, which includes two-way radio, text and numeric paging capabilities. The handsets from Motorola Inc. allow officials to contact all local emergency coordinators at once as well as the National Guard.

### ALASKA

**TURN UP THE VOLUME.** Alaska reported a heavier than normal caller volume following the terrorist attacks of Sept. 11. General Communications Inc. of Anchorage, which provides telecommunications and Internet services to the state government, that same morning began to monitor all incoming and outgoing Internet and telephone communications over the company's fiber-optic and satellite networks.

### ARIZONA

**INTELLIGENT COMMUNICATIONS.** Officials at the Emergency Management Division use Microsoft Access to log, track and communicate about activities between the emergency operations center and the intelligence center during events. Once a lead is called into the emergency center, workers enter the information into the database, which is then relayed to a collections manager in the intelligence center, who assigns investigators to the matter.

### ARKANSAS

**READY TO ROLL.** "Long before Sept. 11, hackers and crackers were a problem," said David Huddleston, manager of the Emergency Management Department's information systems management division. Division staff back up data daily, store copies of everything off site and run mirrored servers.

### CALIFORNIA

**SECURITY TOOLBOX.** Before the attacks of Sept. 11, tools were already in place to enhance security in the

state's Information Technology Department, said Kiran Kernellu, IT Department spokeswoman.

California officials used unspecified "hardware and software devices" to detect, record and repel damaging network traffic, Kernellu said. After the attack, IT Department officials put the state's systems administrators and security specialists on heightened alert.

#### COLORADO

**INCREASED SCRUTINY.** After September's attacks, Colorado put into effect plans that had already been set up to increase IT security in the state, said CIO Bob Feingold. The plans were activated and overseen by the Colorado Bureau of Investigation and Public Safety Department.

"But we've always examined our networking infrastructure for viruses and hacking attempts," he said. "That's been going on long before these terrorist incidents."

#### CONNECTICUT

**ALWAYS AVAILABLE.** The Statewide Emergency Telecommunications Office relied on its recently upgraded 911 system to keep track of emergency situations around the state. The system uses Palladium 9-1-1 System software from Lucent Technologies of Murray Hill, N.J., to record and track emergency calls and vehicles, and provide computer-aided dispatching.

#### DELAWARE

**SPARKLING SYSTEM.** Officials at the Emergency Management Agency rely on EIS/GEM Version 8.2 from Essential Technologies Inc. of Rockville, Md., to log, track and communicate among the three sections of their 28,000-square-foot emergency operations center.

#### DISTRICT OF COLUMBIA

**IM CONNECTED.** The Emergency Management Agency has no LAN. On the day of the attack, Andrew Jackson, chief of the operations center, set up an instant messaging system through Yahoo! Inc. of Sunnyvale, Calif., so agency coordinators could communicate quickly and keep the noise level to a minimum.

#### FLORIDA

**SIGN AWAY.** In the aftermath of disasters, the Emergency Management Division expedited recovery payments to counties for residents through digital signatures. The state-developed Process Automation and Paperless Routing System uses public-key infrastructure software from Entrust Inc. of Plano, Texas, to allow county officials to use digital signature certificates to represent their authority when signing documents.

#### GEORGIA

**THE RIGHT ROUTE.** The Emergency Management Office uses Lotus Notes 4.6 to route and record requests for assistance to agencies and partner volunteer groups. The agency that receives the request keeps a running log of how the program handles requests and then compiles and prints situation reports.

#### HAWAII

**ALOHA OY.** Hawaii took a big hit in lost tourist dollars after Sept. 11. "The hotel occupancy rate dropped drastically," said Charlie Tarnay, head of the Information and Communication Services Division's systems security section. But the state's IT officials were prepared. The IT staff already had a computer backup procedure in place, Tarnay said. The department also uses a series of magnetic security cards to control access to secured areas.

#### IDAHO

**ROAD TO RECOVERY.** Less than a month before the attacks of Sept. 11, Idaho's IT Resource Management Council approved a policy that requires each agency to submit a business recovery plan each year as part of its overall IT plan.

#### ILLINOIS

**READY FOR NEXT TIME?** The Emergency Management Agency encouraged local officials to take stock of their disaster response capabilities by using the Illinois Local Capabilities Assessment for Readiness. The

Microsoft Excel tool, available at [www.STATE.il.us/iema/news.htm#sitrep](http://www.STATE.il.us/iema/news.htm#sitrep), helps emergency response agencies identify strengths and weaknesses in 13 functional areas, so the agencies can develop improvement plans.

#### INDIANA

**EXECUTIVE DECISIONS.** To manage the aftermath of September's attacks, Emergency Management Agency officials used Tracsys software from Applied Computer Systems Inc. of Los Alamos, N.M. The program, which runs under Sun Microsystems Solaris, lets supervisors log, forward and track requests for information or assistance.

#### IOWA

**INTEGRATION NOW.** CIO Richard Varn said the attacks have given new urgency to state projects to integrate criminal justice systems. At the same time, state officials will press the federal government to improve the security of systems that generate identity documents such as passports, which can be easily counterfeited, he said.

#### KANSAS

**Y2K UPDATED.** Kansas CIO Don Heiman called for an update on the state's disaster recovery plans created for the year 2000 rollover. The Kansas IT Office is "joined at the hip" with the state's attorney general and emergency management officials, Heiman said.

#### KENTUCKY

**STILL WATCHFUL.** The Governor's Office for Technology has scaled back by about 50 percent its additional security measures instituted on Sept. 11, said acting security director Mark McChesney. In the immediate aftermath of the attack, officials ordered Kentucky State Police officers to guard the state data center and stepped up network monitoring.

#### LOUISIANA

**ON DETAIL.** "For the past nine months we've been looking at security in a lot more detail," said Allen Doescher, assistant commissioner of the Administration Division. Division officials are assessing physical security, network security and the possibility of establishing a state-level security office.

#### MAINE

**GRAPHICALLY INCLINED.** In the first few hours after the attacks, Emergency Management Office workers mapped the state's highly vulnerable areas and critical facilities using the agency's geographic information system. A state technician used ArcView GIS 3.2 from Environmental Systems Research Institute of Redlands, Calif., to plot the data and help identify critical infrastructure.

---

## THE 50 STATES: Maryland to Wyoming

#### MARYLAND

**GETTING THE WORD OUT.** State emergency operations center workers contacted 30 state, federal and nongovernmental agency representatives in less than 20 minutes to staff the center using an automatic dialing system from Dialogic Corp. of Parsippany, N.J. The system calls the emergency workers at home, at the office and via pagers.

#### MASSACHUSETTS

**VIDEO STARS.** Officials at the Emergency Management Agency conferred with officials at the main command center at Logan International Airport using videoconferencing. The Trinicom 5100 Plus System from Sony Corporation of America of New York, runs over an Integrated Services Digital Network line.

#### MICHIGAN

**BACK TO THE FUTURE.** Officials in Michigan have been "dusting off their Y2K books," said CIO George Boersma, referring to planning documents prepared for the year 2000 date rollover. "They are an excellent resource for what to do" in a disaster situation, he added.

## MINNESOTA

**IS IT TRULY SECURE?** Minnesota agencies reviewing their security systems after the attacks expressed renewed interest in network tools provided through the Administration Department's Technology Office, commissioner David Fisher said. The office uses TruSecure risk management software from TruSecure Corp. of Herndon, Va.

## MISSISSIPPI

**READY AS PLANNED.** The Mississippi Emergency Management Agency activated its EM/2000 system from Specialized Disaster Systems International Inc. of Lake Ozark, Mo. The software includes a Lotus database management system running on a Domino server from IBM Corp., with data about the emergency response resources of the state's 82 counties.

## MISSOURI

**HARD RISKS, TOO.** Officials activated the state's emergency operations center in Jefferson City on a full-scale, 24-hour basis for three days after the attacks. Center personnel used SoftRisk emergency management software from SoftRisk Technologies Ltd. of Toronto to track incident reports.

## MONTANA

**PATCH WORK.** Montana has become vigilant about computer viruses, said Mike Boyer, chief of the computing technology services bureau. "We're very diligently trying to keep people 'patched' with the most current virus protection," Boyer said.

## NEBRASKA

**perimeter patrol.** Nebraska's data security plans didn't really change after Sept. 11, said CIO Steve Schafer. Last month the state held a meeting with agencies to discuss the security of Nebraska's networks, focusing on firewalls and what Schafer called "perimeter security"—keeping the network secure from outside attacks.

## NEVADA

**ON THE RADIO.** On the day after the attacks, Emergency Management Division officials set up two radio communications networks—an 800-MHz and a high-band amateur. Officials used the ACU-1000 Intelligent Interconnect System from JPS Communications Inc. of Raleigh, N.C., to link all the systems so officials at the highway patrol, transportation department and fire division could communicate on either network.

## NEW HAMPSHIRE

**FIRST TIME'S A CHARM.** The Emergency Operations Center used its new event logging system in a true emergency situation for the first time. The center's computer specialists created the Web system using Microsoft's Active Server Pages.

## NEW JERSEY

**MEDIA RELIEF.** The State Police Web site lists all state residents who were reported missing to local and township police departments in the wake of the attacks. The police received more than 100 calls daily from media outlets before they put the list online and trimmed the number of calls to fewer than 10 in two days.

## NEW MEXICO

**BORDER PATROL.** As a border state, New Mexico has some special security concerns. "We did some asking 'What if?'" said Orlando Romero, Public Safety Department CIO. The department had been installing a virtual private network, but the events of Sept. 11 caused Romero and his team to step up the process, he said.

## NEW YORK

**DISSEMINATE, COORDINATE AND ALLEVIATE.** Computer specialists at the State Technology Office used geographic information systems software to give other state officials information on where every state office in Manhattan was located. The computerized map information also was used to coordinate transporting emergency generators by the Transportation Department from state offices around the city to the disaster site.

## NORTH CAROLINA

**WELL EQUIPPED.** The state Emergency Management Office, most of the county emergency offices, many of the state's vehicles, seven weather service stations and 20 statewide radio stations relied on satellite phones to communicate during the crisis. Officials use phones made by Hitachi America Ltd. of Brisbane, Calif., Motorola Inc. and Sony Corporation of America of New York.

#### NORTH DAKOTA

**V IS FOR VIGILANCE.** North Dakota is staying the course in terms of security, said Dan Sipes, associate director of administrative services for the IT Department. "We're just trying to be a little more vigilant," Sipes said. "We're pushing harder on finalizing our security policy framework and other initiatives we already had on the plate."

#### OHIO

**NO DOLL HERE.** The Emergency Management Agency uses a video projection system to transmit data from paper, white boards or maps to five 16-foot screens so employees all over the center can view the images simultaneously. The EV-8000AF from Elmo Manufacturer Corp. of Plainview, N.Y., also can display information through a video switch or slides.

#### OKLAHOMA

**WEATHERING THE STORM.** While the emergency operations center went on 24-hour alert after the attacks on New York and Washington, D.C., state officials did not see a direct impact on their region. The center's main function, however, is to warn residents and local officials about weather hazards.

#### OREGON

**SECURE SERVICE.** Security tops Oregon's IT agenda, said CIO John Lattimer. Oregon is getting ready to launch a new state portal, which may include security features such as public-key infrastructure and digital certificates.

#### PENNSYLVANIA

**FIRST ON THE SCENE.** When the hijacked United Airlines plane crashed in Somerset County, state police sent their Mobile Command Post almost immediately. The command post is a motor-home-size vehicle outfitted with cellular phone and radio communications equipment, as well as five IBM ThinkPad notebooks running Microsoft Windows NT. Officials secured Internet access and the use of state and national law enforcement databases through telephone lines and 56K modems.

Troopers also used notebooks from IBM and Toshiba Corp. of Tokyo with grid mapping software to document the location of evidence.

#### RHODE ISLAND

**STAYING LOW-TECH.** Having had no serious emergency since the hurricane of 1954, officials don't use specialized software but run the emergency operations center using WordPerfect from Corel Corp. and Microsoft Office applications such as PowerPoint. Center employees log major events using Corel's QuattroPro and use a poster printer for paper up to 36 inches wide.

#### SOUTH CAROLINA

**COORDINATED EFFORT.** The University of South Carolina provided the Emergency Management Office with software to allow state agencies and counties to request assistance and track those requests during emergencies. The system runs over a secure intranet and can be accessed through the office's LAN or remotely via the Web.

#### SOUTH DAKOTA

**SONET SURVIVOR.** South Dakota backs up all state information systems at a site in the Colorado hills, CIO Otto Doll said. The state's Synchronous Optical Network is tough enough to survive "cuts in fiber, blackouts, all that sort of thing," Doll said.

#### TENNESSEE

**WHERE'S THE GAP?** In the days after the Sept. 11 attacks, Office of Information Resources staff members

reassessed the information security capabilities and physical security aspects of the state's data and telecommunications centers. Information systems chief Vic Mangrum said officials performed a "gap analysis" to find security weaknesses.

#### TEXAS

**DON'T MESS WITH TEXAS.** Texas officials noticed a lot more intrusive network activity in the weeks following the Sept. 11 attacks. "We've had more intrusions, more perimeter violations and more viruses," CIO Carolyn Purcell said. Fortunately the state performed a security analysis of its systems last year and took corrective measures then, Purcell said.

#### UTAH

**SON OF Y2K.** Utah's disaster recovery plan hasn't changed since Sept. 11, according to CIO Phillip Windley. The state has adopted some new measures to protect government data but Windley did not provide details. The year 2000 rollover laid the foundation for the state's new emergency measures. "Some of what we have and use is clearly a product of Y2K planning," he said.

#### VERMONT

**HELP LIST.** Within hours after the attack, the Emergency Management Office constructed a database of volunteer resources, such as manpower and equipment that residents wanted to donate to the rescue effort. Items entered into the Microsoft Access database were grouped by similar resources.

#### VIRGINIA

**NO TIME FOR SLEEP.** Officials from Arlington County, Va.'s, Technology Services Department were on call 24 hours a day after the attack on the Pentagon. Staff members supported rescue workers' and federal officials' technology needs by setting up a field office of the emergency operations center with networked computers and printers and e-mail access.

#### WASHINGTON

**FIGHTING CYBERTHREATS.** Washington has been "heavy into disaster recovery plans" since 1990 or so, said Mike Curtright, assistant director of the computer services division in the Information Services Department. After Sept. 11, the department took stricter measures about verifying the identities of people who enter the data center, he said.

#### WEST VIRGINIA

**ON THE CUSP.** The Emergency Services Office is training employees on a new Web system to handle all communications and event logging.

The office is installing E Team software from eteam.com of Canoga Park, Calif., and linking it to ArcView and ArcInfo from Environmental Systems Research Institute of Redlands, Calif., to map the state's critical infrastructure.

#### WISCONSIN

**TASK AT HAND.** State IT officials from the new Electronic Government Department and the Administration Department will serve on the terrorism preparedness task force formed by Gov. Scott McCallum. The task force will review the terrorism readiness of the state's IT infrastructure, among other functions.

#### WYOMING

**CARRYING A TORCH.** The Olympic Games, long an attraction for terrorists, are coming February to Salt Lake City, which is only about 40 miles from Wyoming's border. "That's one reason we're dusting off some of our plans from the year 2000 rollover," said Bob Bezek, coordinator of the Wyoming Emergency Management Agency.