



In this week's NGA Homeland Security News:

- [Homeland Security: News From the States](#)
- [Counterterrorism News](#)
- [Additional News](#)

If you would like to ask a question of the NGA or your peers in other states or post a best practice in this newsletter, please e-mail Will Ware at wware@nga.org.

(This is a subscriber's forum. This list is set up to allow only the administrators to post messages.)

NGA Resources

[NGA Homeland Security Home](#)

[NGA Home Page](#)

[NGA Center for Best Practices](#)

[About the Governors](#)

[NGA Policy Positions](#)

[NGA Press Releases](#)

[NGA Reports Online](#)

Contacts

[Chris Logan](#)

202-624-5379

[Will Ware](#)

202-624-5311

Homeland Security: News from the States

Homeland security stories from news sources around the country for the week ending November 6, 2009.

[Electronic Prescription Data Helps Track H1N1](#)

Rhode Island health officials are using prescription data collected by pharmacies to accurately determine the number of H1N1 cases in their state. The state receives prescription data through an e-prescriptions network. By quantifying the number of Tamiflu and other anti-viral prescriptions in the state, health officials can use the data to:

- Detect outbreaks of flu by zip code and community, including by age groups;
- Monitor discrepancies between outbreak data from the *Sentinel* symptom-tracking system used by doctors, and prescription-based data; and
- Offer a more detailed view of the outbreak than doctor reporting systems, as systems such as *Sentinel* offer only a statewide composite from 25 reporting doctors.

Combined with *Sentinel* and emergency room reporting of influenza-like illness, the prescription data will offer a more complete picture of the outbreak in the state.

[Digital Health Records Made Available for Use in Emergencies](#)

First responders and Emergency Medical Technicians (EMTs) in Indianapolis now have access to digital medical records at the scene of an incident, through a new digital record system developed in Indiana. The system gives EMTs real-time access to a patients' medical record, showing emergency responders pre-existing conditions of a victim, treatments, allergies and current medications, among other data, to provide personalized care at the scene rather than waiting to begin specific procedures at the emergency room.

Florida County Issues Handheld Fingerprint Scanners to Police

Sarasota County has deployed 14 portable fingerprint scanning systems that provide quick positive identification of individuals by searching state, local and FBI databases. Unlike most fingerprint systems that can take hours and must be performed at the jail, this new system provides positive identification in the field in a matter of seconds. Positive identification of individuals is critically important for the safety of law enforcement officers. Once an individual's criminal history is revealed officers can make better informed decisions that can increase their safety. Officers in Sarasota, Florida, have already identified several individuals providing false names using the scanners. The scanners cost \$4,100 each and were purchased using the county's drug forfeiture funds.

Kansas and Oklahoma Conduct Joint Drill on Foot and Mouth

Kansas and Oklahoma have conducted a joint drill aimed at protecting the nation's food supply in the event of an outbreak of foot and mouth disease. The drill also helped evaluate each state's plans for a stop movement order. The exercise focused on an outbreak of foot and mouth in another state that forced officials to declare an emergency and halt the movement of livestock. During the exercise, state and local authorities set up roadblocks and pulled livestock vehicles aside to question drivers about their loads and destinations. In the event of an actual outbreak, officials would stop livestock haulers and require them to return to their point of origin and wait for inspection. Representatives from Colorado, Iowa and Nebraska also monitored the drill.

Delaware Hosts Cyber Security Exercise

The Delaware Department of Technology and Information in collaboration with the Delaware Department of Safety and Homeland Security, the Delaware Emergency Management Agency and the Delaware State Police hosted a cyber security exercise that gathered 200 representatives from federal and state governments. The exercise titled "Cyber Siege" featured a scenario where network and system administrators had to defend against a real time attack on systems and networks. State managers and public information officers practiced implementing emergency procedures and the release of information to the public. Delaware is one of four states participating in the United States Cyber Challenge pilot program.

Counterterrorism News

Intelligence Community Concerned about Smaller Scale Attacks

U.S. intelligence officials are concerned that extremist groups tied to al Qaeda are planning small-scale attacks in the United States that would be more difficult to detect, thus more likely to succeed. Recent purported disruptions in Denver and Chicago have reinforced the intelligence community's concerns. In both instances, the defendants have been long-term U.S. residents with substantial ties to their respective communities. Defendants in both cases also attended training events with al Qaeda affiliates in the Pakistani tribal regions, similar to the planners of the Madrid train bombings of 2004 and the London subway attacks in 2005. Compared to many previous arrests since 2001, the men arrested in Denver and Chicago were more security conscious, better organized and better trained. A number of other arrests involved young men eager for battle, but lacking the skills to carry out effective attacks.

Additional News

NGA Webinar Highlights H1N1 Vaccination Challenges and Successes

The NGA Center recently hosted a webinar titled: *H1N1: Assessing State Vaccination*

Efforts, which captured the current state of the H1N1 vaccination program from the federal, state and local perspectives. The webinar contains guidance from the US Department of Health and Human Services on the recent emergency declaration by President Obama as well as explanations for seeking reimbursement for public health emergencies in the state under 1135 Medicare and Medicaid waivers. In addition, Massachusetts and South Carolina health officials presented state examples of pandemic preparedness and current strategies to meet the vaccine demand from the public. The Fairfax County Medical Reserve Corps also presented their lessons learned from a mass vaccination clinic in Virginia, from logistical challenges to the management of volunteers during a public health response.

Report: Telecommuting May Overwhelm Internet During a Pandemic

Should a pandemic influenza require workers and students to stay at home to avoid the spread of a virus, the telecommuting workforce might overwhelm current Internet capacity, according to a GAO report. Demand on Internet services would shift from company and academic servers to workers using their personal computers from home, putting excessive demands on the Internet infrastructure that services personal residences. Additionally, critical systems might be threatened as essential personnel needed to maintain infrastructure might not be in the workplace for weeks or months. While the shift from corporate servers to personal computer use is anticipated in the event of a massive telecommuting effort, the GAO indicates that there is little planning or preparation by federal authorities to manage the demand, as there is no clear authority to act since much of the Internet infrastructure is privately owned.

Study Finds Students Personal Information Is Vulnerable

While examining data systems created to track student progress, a new [study](#) conducted by Fordham University found that states often collect more information about students than necessary and fail to enact the proper measures to protect their privacy. The findings conclude that states fail to protect student's privacy due to the lack of tightened protocols for purging records after students graduate. The study recommends that states:

- Enhance protocols to keep data anonymous, with special provisions for those in local schools who need to know more;
- State reasons for collecting data and dispose what is unnecessary; and
- Appoint officers to oversee compliance with state and federal privacy laws.

DHS Launches Web Site for Sharing Recovery Ideas

The U.S. Department of Homeland Security has launched a new website, DisasterRecoveryGroup.gov that allows state, local, and federal officials to submit ideas on how to manage long-term disaster recovery. The site acts as a tool for the newly formed Long-Term Disaster Recovery Working Group, co-chaired by Housing and Urban Development Secretary Shaun Donovan and Homeland Security Secretary Janet Napolitano. Through this working group, Secretaries Donovan and Napolitano plan to develop a National Disaster Recovery Framework aimed at providing detailed operation guidance to recovery organizations under existing authorities.