NASCIO
Representing Chief Information
Officers of the States

NASCIO Staff Contact:
Drew Leatherby
Issues Coordinator
dleatherby@AMRms.com

Pandemic Planning and Response for State IT: Where's My Staff?

Without the flow of electronic information, government comes to a standstill. When a state's data systems and communication networks are disrupted, the problem can be serious and the impact far-reaching. The consequences can be much more than an inconvenience. Serious disruptions to a state's IT systems can lead to public distrust, chaos, fear and potential loss of life. Traditionally, IT disruptions are planned for based on anticipated disasters both natural and manmade that can physically damage facilities and equipment. **However, we live in a time that holds the potential for a pandemic outbreak in your city, state or possibly the nation. What would you do as state chief information officer (CIO) if one day your staff did not come to the office because of a pandemic outbreak?**

Physical disasters that shut down mission critical applications are typically covered under a state's disaster recovery and business continuity (DR/BC) plan. Under these plans, physical assets can be replaced, and information protected, using various backup and business resumption practices. However, if one day you find your offices empty – your systems running unattended

due to a pandemic scare – are you prepared to act? **CIOs have an obligation to ensure that IT services continue in the event of a pandemic outbreak, and planning for such a scenario has become essential.** It's not a matter of if a pandemic is going to strike, it's just a matter of when, and how far-reaching the problem will be. **The good news is that there are simple steps that state CIOs can follow to prepare for such a disaster.**

Pandemic Planning 101

The primary focus of this brief is on how to maintain critical operations during a pandemic outbreak. Pandemics are unique in that they affect an organization's workforce as opposed to its physical infrastructure, and therefore require a radically different approach for recovery efforts. Planning in response to a pandemic event should include an incident management component involving an incident command response and identifying those key members and players necessary for a comprehensive solution to the plans that are developed. The impact of a pandemic on the state IT organization goes beyond just

Pandemic Planning and Response for State IT: Where's My Staff?

1

the people, process and technology aspects. On a larger scale, the CIO must understand the impact to the logistics of suppliers outside of the state IT organization who may also be experiencing a high rate of employee absenteeism.

Experts agree that a pandemic event will likely occur in the next ten years and undoubtedly will result in a high rate of employee absenteeism. Most states' IT organizations are simply not prepared to address the infrastructure and procedural issues that will emerge as a result. Whether caused by pan-flu, plague, smallpox, anthrax, West Nile Virus, TB or other epidemic, state IT leaders need to make sure their DR/BC plans are designed to deal with such a contingency. Consciousness is being raised on several fronts, but state IT – for the most part – hasn't taken the necessary steps to implement and test plans and processes to cope with such an outbreak.

The Role of the State CIO in Pandemic Preparedness and Response

In many states there is a dependency on IT to "figure it out," if a problem is technology related. The state CIO is generally expected to introduce innovation within the state enterprise and prepare for all contingencies. When systems are down and every aspect of state business is affected, the buck may stop at the CIO's desk. However, there are simple steps that CIOs can follow to ensure that their IT infrastructure is protected under any scenario. One major difference in a pandemic crisis versus an unforeseen disaster is that there is an element of nature that may provide the luxury of time. The CIO can start to respond and escalate a response, but identifying the critical triggers and executing successfully on those must be in the state's overall DR/BC plan. CIOs need to identify critical staff and business functions that their state enterprises cannot function without. The critical business functions and critical staff tiering for a

pandemic may be completely different from that for a physical disaster. Unlike other DR/BC situations, in the case of a pandemic, the critical staff list should include for example, those operating the facility's chiller rooms and other general maintenance functions. Finally, prepare for making decisions in an environment of uncertainty. ***During a crisis the CIO may not have all the information necessary, but will be required to make immediate decisions.***

Communication

Educate state IT staff on basic preparedness for themselves and their families – Prepare and distribute pandemic preparation resources to every member of the IT staff, with information on what individual employees and their families can do to avoid or minimize exposure. Work with state public health agencies for basic survival information, and build a packet of information tailored to state IT staff.

Educate state IT staff, lawmakers, appointed officials, human resources and budget officials – Craft an education and awareness program for state IT staff, lawmakers and budget officials to ensure all parties are on the same page with regards to the pandemic preparedness plan and the need for such a plan. Prepare key talking points that outline the rationale for pandemic planning. **Establish metrics for costs of not having a plan:** How much will it cost the state if certain critical business functions go down? Costs could stem from ERP issues on the payment side; citizen service issues (what it would do to the DMV for license renewals); and impacts on eligibility verifications for social services. How long can the state afford to be down? How much will this cost the state? How long can the state be without a core business function?

Communication and cross-boundary collaboration – A CIO can build a portfolio of remote access solutions to meet business needs from ultra-secure systems

to fairly simplistic, low bandwidth constrained systems. Yet that will not be useful if the state's workers aren't properly trained to use the technology. Also, CIOs need to build critical partnerships with other agencies and branches of government. **Think outside the box:** CIOs can partner with anyone to share IT resources; including universities, local government, lottery corporations, local companies and leased facilities with redundant capabilities.

Classify and cross-train workers – State IT organizations often struggle with getting other business units to classify workers in terms of criticality, and further breaking down their assigned roles and providing cross-training so, in the event of a crisis, critical employees are equipped to change roles or function in multiple roles. In most other events, the CIO is able to designate who responds. Yet, with pandemics, the CIO has no control over who is sick.

Intergovernmental communications and coordination plan – Develop a plan to communicate and coordinate efforts with state, local and federal government officials. Systems critical for other state, local and federal programs and services may need to be temporarily shut down during a pandemic event to safeguard the state's IT enterprise. Local jurisdictions are the point-of-service for many state transactions, including benefits distribution and child support payments, and alternate channels of service delivery may need to be identified and temporarily established. *Make sure jurisdictional authority is clearly established and articulated to avoid internal conflicts during a crisis.*

Identify indirect factors and implications – CIOs should also identify indirect factors and implications related to a pandemic disaster (e.g. loss of staff to public utilities and other infrastructure). The CIO should take leadership on this, and begin pressing other state entities to make sure that they're addressing these indirect issues.

Pandemic preparedness coordinating committees – Gather representatives from all applicable lines of business and critical service industries necessary for continuity of IT operations. Keep the dialogue open with state business partners and periodically convene briefings for them on the state's DR/BC plans.

Communicate to rank and file employees – Explain there is a pandemic plan and the reasons behind its establishment. Clearly articulate employee roles during a pandemic incident and identify members of a possible crisis management team. Also, compile a list of employee office, home and mobile phone numbers, and other relevant contact information.

Establish a media crisis communications protocol – A crisis communications protocol should be part of a state's IT DR/BC plan. Designate a primary media spokesperson with additional, single point-of-contact communications officers as back-ups. *Articulate who can speak to whom under different conditions, as well as who should not speak with the press.*

State summits – Several states have developed educational state-wide summits as part of their pandemic influenza preparation. Typically U.S. Department of Health and Human Services and other federal, state, local, tribal, not-for-profit, and private sector officials convene to discuss current and future pandemic readiness plans. These summits are statewide opportunities to share planning efforts among the various partners as states continue their work to prepare for this threat. Summits may include elements such as Webcasts.

Planning

CIOs must have a DR/BC plan that addresses the unique problem associated with a pandemic event – This plan should include: **(1)** A focus on capabilities that are needed in any crisis situation; **(2)** Identification of functional requirements; **(3)** Planning based on the different severity levels of a pandemic event – see Centers for Disease Control

and Prevention (CDC) Pandemic Severity Index <http://www.cdc.gov/od/oc/media/pdf/MitigationSlides.pdf>; **(4)** Service level requirements for business continuity; **(5)** Revisions and updates – having critical partners review the plan; and **(6)** Storing hard and digital copies of the plan in several locations for security.

Ask and answer the following questions – **(1)** What are the top business functions and essential services without which the state enterprise can not operate? **Tier business functions and essential services into recovery categories based on level of importance and allowable downtime**. **(2)** How can disruption to an agency's or department's operations be reduced?

Conduct contingency planning in case of absent personnel – This could involve cross-training of essential personnel who can be lent out to other agencies in case of loss of service. Also, **mutual aid agreements** with other public/private entities such as state universities for "skilled volunteers" can be put in place. Make sure contractors and volunteers have approved access to facilities during a crisis.
Approach enterprise backup as a shared service: Other agencies may have the capability for excess redundancy.

Review and suggest revisions to state personnel policies that offer flexibility – During a pandemic crisis, state IT employees may be asked to work under conditions not traditionally covered under current state policy. State CIOs should meet with state personnel officials, employee unions and associations to discuss flexible policies that can be temporarily implemented during a pandemic crisis. In this manner, decisions made by the CIO concerning who stays on site, who goes home, and issues about pay, leave, and state liabilities can be adequately addressed ahead of a potential crisis.

Review state and federal regulatory requirements regarding business processes and IT service levels – During a pandemic crisis, state IT organizations may find that mandatory service delivery associated with state and federal programs is temporarily disrupted and service level agreements are not being met. Federal programmatic funding may require certain service performance levels that cannot be met during a pandemic. In such a situation, the CIO may need to seek waivers from the federal government, or temporarily seek service freezes because of IT operational concerns. ***Investigate the process and options for seeking relief ahead of the crisis!***

Build cross-boundary relationships with emergency and health agencies – CIOs should build relationships with state-wide, agency and local emergency management and health department personnel. A CIO should know and communicate with his or her emergency management counterparts before a crisis. Also, consider forging multi-state relationships with other state CIO counterparts to prepare for multi-state events, partnering with those in the region. Consider developing a cross-boundary DR/BC plan or strategy, as many agencies and jurisdictions have their own plans.

Conduct testing activities – CIOs should conduct periodic state-wide training exercises and drills to test pandemic DR/BC plans. These drills should be pre-scheduled and conducted on a regular basis and should include all aspects of on-site and remote access procedures. Conduct a **gap analysis** following each exercise.

Prepare for limited or zero access to your facilities – Even though personnel may be theoretically available during a crisis, the structural environment in which IT systems are located may be where a pandemic exposure level is rising. If the area is quarantined and access is prohibited, there exists a serious problem. CIOs must look at how they would manage the situation as it is beginning to build. If a facility becomes contaminated or is in a quarantine zone, state health officials are probably not going to allow access. It may be possible to seal the area off and gain approval for controlled access of critical

personnel. Thus, be sure to coordinate with state health departments in advance. Make them aware that they may not be able to access critical health files if the state's primary computing facilities are non-operational.

Prepare to treat state IT facilities as disaster areas and go into full DR/BC mode – If access is denied to critical state data facilities and the result is a failure from the technology side, the state CIO must be prepared to enter into full DR/BC mode. Due to a potential lack of access, a CIO may be in the position to declare a full-scale disaster.

The Supply Chain

Consider outside entities that provide supplies and support – There are many organizations such as fuel distributors, wholesalers and grocery stores which would all be facing a similar problem as state government in a pandemic situation. Other potentially critical support elements to consider are contractors, vendors and sites that they provide. CIOs also need to examine services that provide basic necessities, such as the power grid that supplies power to state IT facilities. The power grid itself is not subject to infection; however, the massive number of people it requires to keep operating would be just as susceptible to a pandemic outbreak as anyone else.

Review state contracting instruments and laws – Set up emergency standby services and hardware contracts and have contracts in place for products and services that may be needed in the event of a declared pandemic emergency. Create a contract template so that a contract can be developed with just one or two hours work time. CIOs must be sure essential IT procurement staff are part of the DR/BC plan and are aware of their roles in executing pre-positioned contracts in the event of a disaster. Provide emergency contact information ahead of time. *CIOs should also develop "Emergency Purchasing Guidelines" for agencies and have emergency response legislation in place.*

Execute emergency standby services and hardware contracts – *If necessary*, execute pre-placed contracts for products and services needed during the crisis. The Governor may have to temporarily suspend some of the state's procurement laws and execute emergency purchasing guidelines for agencies. Also, consider identifying back-up providers for products and services as some suppliers may suspend deliveries during a pandemic.

Technology

Shutdown non-essential services – This will free up resources for other critical services. Identify critical business applications and essential services and then tier them into recovery categories based on level of importance and allowable downtime. Tier III applications would be shut down first. Critical services should be classified for internal customers versus external customers. Also, limit use of rich media and streaming media applications to conserve bandwidth.

Protect current systems – Mechanisms include uninterruptible power supply (UPS), for example, and back-up generators with standby contracts for diesel fuel. Use priority and back-up fuel suppliers that also have back-up generators to operate their pumps in the event of a widely spread power outage.

Remote access from other facilities – If the business processes and capabilities are established on the front end, the state IT environment can be remotely supported, as long as the systems do not fail. With the likelihood of operating without back-up tapes, a CIO's willingness to operate without those back-ups will determine how long operations continue in that mode versus declaring an actual disaster. Such a declaration will involve going to either an internal back-up source or an outsourced vendor to begin the recovery process. Without a process in place, a CIO may be forced to declare a disaster even though IT systems are intact. Virtualization and use of redundant data centers in

remote locations may minimize this risk.

Tele-working – The tactical use of tele-working for critical staff may resolve many on-site accessibility problems. However, there is still a pervasive culture in state government where some may be leery of letting staff work from home for fear of creating an environment where staff starts requesting to work from home on a regular basis. Working with state personnel offices to educate them on the critical need for tele-working procedures to be in place may avoid future conflict and personnel issues.

Priority IP access for critical employees – The Government Emergency Telecommunications Service (GETS), which allows critical government officials to gain priority accesses to voice line communications, has been extended to cell phone service allowing users to drive a priority connection through the PBX phone systems. CIOs should explore a similar data service that is sponsored by either the National Communication System (NCS) <www.ncs.gov> or another federal agency that would allow critical IT staff to register their local IP address to allow them to gain priority access through the IP networks.

Alternative communications methods – Should a pandemic develop, that doesn't necessarily mean the Internet will fail. However, absenteeism over a period of time among the maintenance staff of Internet providers may lead to issues that cause the Internet's infrastructure to fail. **This could greatly affect tele-working technologies and VPN access for critical staff and increase the need for remote access technologies that do not depend on PBX phone systems and Internet access.** Alternative communications methods require pre-planning. A CIO can not afford to explore such methods for the first time as the problem is unfolding. **Mobile communication centers** also can be utilized in the event that traditional telecommunications and IP systems are down.

Leverage technology and think outside the box – In a disaster situation a state's

Geographic Information Systems (GIS) can be utilized to monitor power outages and system availability. For emergency communications, the state's Web portal can be converted to an emergency management portal. Exploit existing interactive video conferencing sites and services. Also, Web 2.0 technologies such as Weblogs, Wikis and RSS feeds can be utilized for emergency communications.

CIO Considerations – Preparing for the Worse Case Scenario

State CIOs, as much as possible, should not focus on the multi-state, geo-political aspects of a pandemic incident, but instead focus on "**how does this directly affect my IT enterprise operations**," and take immediate steps to keep the state's essential IT business functions operating. CIOs should rely on federal, state and local emergency management and health officials to handle the wider "big picture" issues of disrupted commerce, the general health and well-being of the populace, and control and protection of a panicked populace.

If an isolationist self-sustainable "**Shelter in Place**" strategy must be implemented, then the state CIO should consider planning for emergency operations center class control rooms, complete with self-contained air filtration systems, on-site fuel supplies for power generation, food stores and internal health care and vaccines for essential employees.

With states already consolidating data assets in hardened, centralized facilities with secondary back-up centers, taking these additional steps may not be thinking too far outside the box, especially considering the bleak projections and implications for a natural or man-made pandemic incident occurring in the near future.

A final important concern of CIO pandemic planning centers on what could be very real and profound implications for essential IT and facilities maintenance staff. To

maintain critical computing operations that support the state's first responder community, essential IT and facilities maintenance staff may require insulation both physically and emotionally from the possible horrors occurring outside the data facility doors. It may not be too far-fetched to consider providing critical IT staff psychological training to cope with isolation from families, and the worse case scenario that their loved ones and com-munities my be experiencing untold stress from loss of life and social upheaval.

Use this Brief in conjunction with NASCIO's Disaster Recovery Tool-kit

NASCIO's **Disaster Recovery Working Group** has developed a series of products on disaster recovery and business conti-nuity including the working group's publi-cation, "*IT Disaster Recovery and Business Continuity Tool-kit: Planning for the Next Disaster*," designed to assist state CIOs and their staff in IT disaster recovery and business continuity planning; and NASCIO's DVD on disaster recovery, **"*Government at Risk: Protecting Your IT Infrastructure.*"** These products, along with this issue brief on pandemic pre-paredness, will serve as resources for state CIOs and other state leaders to not only better position themselves to cope with an IT crisis, but also to help make the busi-ness case for disaster recovery and busi-ness continuity activities in their states.

Appendix 1. Additional Resources

State Government Resources

State Pandemic Influenza Summits (ASHTO):
<http://www.astho.org/pubs/StateSummitReport.pdf>

PandemicFlu.gov – State Pandemic Preparedness Plans:
<http://www.pandemicflu.gov/plan/states/stateplans.html>

State and Local Pandemic Influenza Planning Checklist: Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC):
<http://www.pandemicflu.gov/plan/pdf/checklist.pdf>

Alabama Pandemic Flu Preparedness Website:
<http://www.halek12.org/PCF/Families/AlaPanFluEPK/index.html>

Arizona Department of Administration (ADOA) Pandemic Preparedness Planning Website:
<http://www.hr.state.az.us/Homepagelinks/News_030907.htm>

Arizona State Agency Influenza Pandemic Preparedness Checklist:
<http://www.azdhs.gov/pandemicflu/pdf/az_government_agency_checklist.pdf>

Arizona Influenza Pandemic Response Plan (ADHS):
<http://www.azdhs.gov/pandemicflu/>

Arkansas Department of Health and Human Services (DHHS) Influenza Pandemic Response Plan:
<http://www.healthyarkansas.com/pandemic_influenza/pandemic_influenza_plan.pdf>

California Department of Health Services (CDHS) Pandemic Flu Website:
<http://www.dhs.ca.gov/ps/dcdc/izgroup/diseases/pandemic_flu.htm>

California Department of Health Services (CDHS) Pandemic Influenza Preparedness and Response Plan:
<http://www.dhs.ca.gov/ps/dcdc/izgroup/pdf/pandemic.pdf>

California's Pandemic Influenza Preparedness Efforts:
<http://bepreparedcalifornia.ca.gov/EPO/BeInformed/Flu/PandemicFlu/CalifPanFluPrepEfforts.htm>

Colorado Department of Public Health and Environment Emergency Preparedness and Response Pandemic Influenza Planning Webpage:
<http://www.cdphe.state.co.us/bt/panflu.html>

Connecticut Department of Public Health (CDPH) Pandemic Influenza Preparedness Plan:
<http://www.dph.state.ct.us/BCH/flu/dph_pandraft%20.pdf>

Connecticut Department of Public Health (CDPH) Pandemic Influenza Summit:
<http://www.dph.state.ct.us/avian/summit.htm>

Delaware Department of Health and Social Services, Division of Public Health, Pandemic Flu Website:
<http://www.dhss.delaware.gov/dph/pandemicflu.html>

Delaware Department of Health and Social Services, Division of Public Health, Pandemic Influenza Plan:
<http://www.dhss.delaware.gov/dhss/dph/files/depanfluplan.pdf>

Florida Department of Health (DOH) Pandemic Influenza Website:
<http://www.doh.state.fl.us/rw_Bulletins/panfluplanindex.html>

Florida Department of Health (DOH), Action Plan for Pandemic Influenza Florida, March 2004:
<http://www.doh.state.fl.us/disease_ctrl/epi/htopics/flu/Pandemicdraft8.pdf>

Florida CIO Council, Pandemic Information Website:
<http://www.bpr.state.fl.us/pandemic/>

Florida CIO Council, Pandemic Preparedness Committee Website:
<http://www.myflorida.com/cio/committees_pandemic.shtml>

Georgia Department of Human Resources (GDHR) Pandemic Influenza Preparedness Information Website:
<http://health.state.ga.us/pandemicflu/>

Hawaii State Department of Health, Pandemic Flu Plans Website:
<http://www.hawaii.gov/health/family-child-health/contagious-disease/pandemic-flu>

Idaho Department of Health & Welfare, Pandemic Influenza Response Plan, March 2006:
<http://www.cste.org/specialprojects/Influenzaplans/Idaho%20Influenza%20Pandemic%20Response%20-%20March%2020061.pdf>

Illinois Department of Public Health Pandemic Influenza Website:
<http://www.idph.state.il.us/pandemic_flu/index.htm>

Kansas Department of Health & Environment, Pandemic Influenza Information Website:
<http://www.kdheks.gov/flu/pandemic_influenza.htm>

Kansas Department of Health & Environment, Pandemic Influenza Preparedness and Response Plan:
<http://www.kdheks.gov/flu/download/KS_Pan_flu_10_05.pdf>

Kentucky Cabinet for Health and Family Services, Pandemic Influenza Website:
<http://www.chfs.ky.gov/dph/epi/preparedness/pandemicinfluenza.htm>

Kentucky Cabinet for Health and Family Services, Department for Public Health, Division of Epidemiology and Health Planning, Pandemic Influenza Preparedness Plan, April 2007:
<http://chfs.ky.gov/NR/rdonlyres/6CD366D2-6726-4AD0-85BB-E83CF769560E/0/KyPandemicInfluenzaPreparednessPlan.pdf>

Louisiana Office of Public Health, Statewide Draft Pandemic Influenza Plan, September 2006:
<http://www.dhh.state.la.us/offices/publications/pubs-276/Pandemic%20Influenza%20Plan_100906.pdf>

Maine.gov Pandemic Flu Planning Website:
<http://www.maineflu.gov/planning.htm>

Maine Center for Disease Control and Prevention (CDC) Pandemic Influenza Information Website:
<http://www.maine.gov/dhhs/boh/pandemic_flu_info.htm>

Maryland.gov Maryland Flu Preparedness Website:
<http://flu.maryland.gov/preparing.html>

Maryland's Department of Health & Mental Hygiene Pandemic Influenza Website:
<http://bioterrorism.dhmh.state.md.us/flu.htm>

Maryland Community Health Administration Pandemic Influenza Preparedness Plan Website:
<http://www.cha.state.md.us/edcp/html/mpipp.html>

Massachusetts Department of Public Health Pandemic Flu Information Webpage:
<http://www.mass.gov/dph/cdc/epii/flu/pandemic.htm>

Massachusetts Department of Public Health Influenza Pandemic Preparedness Plan:
<http://www.mass.gov/dph/cdc/epii/flu/pandemic_plan.htm>

Massachusetts Department of Education Pandemic Influenza Preparedness and All Hazards Planning Resources Website:
<http://www.doe.mass.edu/pandemic/resources.html>

Michigan Department of Community Health Pandemic Influenza Website:
<http://michigan.gov/mdch/0,1607,7-132-2940_2955_22779_40567-138344—,00.html>

Minnesota Department of Health Pandemic Preparedness Website:
<http://www.health.state.mn.us/divs/idepc/diseases/flu/index.html>

Mississippi – PandemicFlu.MS.Gov:
<http://www.pandemicflu.ms.gov/index.php>

Missouri State Senate Interim Committee on Pandemic Preparedness Website:
<http://www.senate.mo.gov/06info/comm/interim/pand.htm>

Missouri Department of Health and Senior Services Influenza Summit:
<http://www.dhss.mo.gov/PandemicSummit/index.html>

Missouri Department of Health and Senior Services Pandemic Influenza Plan, February 2006:
<http://www.dhss.mo.gov/PandemicInfluenza/PandemicPlan.pdf>

Montana Department of Public Health & Human Services, Pandemic Influenza Preparedness & Response Plan, May 2006:
<http://www.dphhs.mt.gov/PHSD/Communicable-disease/pandemic-flu-plan/3flu-2006-RevisedFluPlan-5-17-06.pdf>

Nebraska Department of Health and Human Services, Pandemic Flu Homepage:
<http://www.hhss.ne.gov/pandemic/>

Nebraska Health and Human Services System, Pandemic Influenza Prevention and Control Guidelines, February 2006:
<http://www.hhs.state.ne.us/puh/epi/flu/pandemic/docs/State-Plan.pdf>

Nevada State Health Division, Pandemic Flu Homepage:
<http://health.nv.gov/index.php?option=com_content&task=view&id=358&Itemid=600>

New Hampshire Department of Health & Human Services, Pandemic Planning Coordinating Committee (PPCC):
<http://www.dhhs.state.nh.us/DHHS/CDCS/ppcc.htm>

New Hampshire Influenza Pandemic Public Health Preparedness & Response Plan, February 2007:
<http://www.dhhs.state.nh.us/NR/rdonlyres/eezi3h2hnpt3ow4svczqinfz22ujnqykos67ra7fej a2vjotsrdt224l3eqxrlw7mrh2jky3xkdvcv4cuni5zo232lh/Policy-Guideline_Pandemic InfluenzaResponseandPrepardnessPlan.pdf>

New Jersey Department of Health and Senior Services Pandemic Influenza Website:
<http://www.nj.gov/health/flu/pandemic.shtml>

New Mexico Department of Health, Pandemic Influenza Webpage:
<http://www.nmbirdflu.org/>

Interim Pandemic Influenza Emergency Response, APPENDIX 2 of the Hazard Specific Appendices, New Mexico Department of Health, Emergency Operations Plan, March 2006:
<http://www.health.state.nm.us/flu/providers/Master%20Pandemic%20Influenza%20Appe ndicies%2010March2006%20FINAL1.pdf>

New York City Department of Health and Mental Hygiene Avian Flu Webpage:
<http://www.nyc.gov/html/doh/html/cd/cd-avianflu.shtml?b=12>

New York City Department of Health and Mental Hygiene Pandemic Influenza Preparedness and Response Plan, July 2006:
<http://www.nyc.gov/html/doh/downloads/pdf/cd/cd-panflu-plan.pdf>

North Carolina Division of Public Health Resources Pandemic Flu Preparedness Website:
<http://www.ncpanflu.gov/>

North Carolina Pandemic Influenza Plan, January 2007:
<http://www.epi.state.nc.us/epi/gcdc/pandemic.html>

The North Carolina Center for Public Health Preparedness, Avian & Pandemic Flu Resources Webpage:
<http://nccphp.sph.unc.edu/panflu/index.htm>

North Dakota Department of Health Pandemic Influenza Plan Summary:
<http://www.health.state.nd.us/EPR/resources/PandemicInfluenzaPlanSummary.pdf>

Ohio.gov Pandemic Flu Website:
<http://www.ohiopandemicflu.gov/>

Oklahoma State Department of Health, Pandemic Influenza Management Plan Committee, Pandemic Influenza Management Plan, July, 2005:
<http://www.health.state.ok.us/program/cdd/flu/Oklahoma%20PIM%20Plan%20Final%20WEB%20DRAFT.pdf>

Oklahoma Pandemic Influenza Management Plan, Public Health Fact Sheet, October 2006:
<http://www.health.state.ok.us/program/cdd/flu/Summary%20Fact%20Sheet%20of%20Oklahoma%20Plan.pdf>

Oregon Department of Human Services Pandemic Influenza Webpage:
<http://www.oregon.gov/DHS/ph/acd/flu/panflu.shtml>

Oregon Department of Human Services Public Health Pandemic Influenza Plan, November 2006:
<http://www.oregon.gov/DHS/ph/acd/flu/oregonfluplan.pdf>

Pennsylvania's Pandemic Preparedness Website:
<http://www.pandemicflu.state.pa.us/pandemicflu/site/default.asp>

Rhode Island Department of Health Pandemic Influenza Homepage:
<http://www.health.ri.gov/pandemicflu/index.php>

Rhode Island Department of Health Pandemic Influenza Preparedness Checklist, May 2006:
<http://www.health.state.ri.us/pandemicflu/RImedia_checklist.pdf>

South Carolina Department of Health and Environmental Control Pandemic Influenza Preparedness Webpage:
<http://www.scdhec.net/administration/ophp/pandemic_preparedness.htm>

South Dakota Department of Health Pandemic Influenza Information Webpage:
<http://doh.sd.gov/Flu/pandemic/>

Texas Department of State Health Services Pandemic Preparedness Webpage:
<http://www.dshs.state.tx.us/idcu/disease/influenza/pandemic/>

Texas Department of State Health Services Pandemic Influenza Preparedness Plan, October 2005:
<http://www.dshs.state.tx.us/idcu/disease/influenza/pandemic/Draft_PIPP_10_24_web.pdf>

Texas Department of State Health Services, Avian Flu Power Point Presentation, June 2006
<http://www.sorm.state.tx.us/Risk_Management/RMUG/3%20panfluSORM062006.ppt>

Utah.gov Pandemic influenza Website:
<http://www.pandemicflu.utah.gov/>

Utah Department of Health Pandemic Influenza Response Plan, November 2005:
<http://health.utah.gov/epi/diseases/flu/ClinicianPublicHealth/pandemic/pandemic_influenza_plan.pdf>

Virginia Department of Health Pandemic Influenza Webpage:
<http://www.vdh.virginia.gov/PandemicFlu/>

Virginia Department of Health Pandemic Influenza DVD:
<http://www.vdh.virginia.gov/PandemicFlu/PanFluDVD.asp>

Washington State Department of Health Pandemic Influenza Webpage:
<http://www.doh.wa.gov/panflu/default.htm>

West Virginia Department of Health and Human Resources Pandemic Influenza Webpage:
<http://www.wvflu.org/>

West Virginia Public Service Commission Pandemic Influenza Webpage:
<http://www.psc.state.wv.us/PanInfo/default.htm>

Wisconsin's Pandemic Influenza (Flu) Information Webpage (Included on this Webpage is information on Governor Doyle's Pandemic Readiness Summit):
<http://dhfs.wisconsin.gov/communicable/pandemic/index.htm>

Wyoming Department of Health Pandemic Influenza Webpage:
<http://wdh.state.wy.us/phsd/epiid/pandemic.html>

Wyoming Department of Health Pandemic Influenza Response Plan Version 2.0, July 2006:
<http://wdh.state.wy.us/epiid/wpirp.pdf>

Federal Government Resources

PandemicFlu.Gov, U.S. Department of Health and Human Services (DHHS):
<http://www.pandemicflu.gov/>

U.S. Department of Health and Human Services (DHHS), **National Vaccine Program Office (NVPO), Pandemic Influenza**:
<http://www.hhs.gov/nvpo/pandemics/>

Centers for Disease Control and Prevention (CDC) **Resources for Pandemic Flu:**
<http://www.cdc.gov/flu/pandemic/cdcresources.htm>

Centers for Disease Control and Prevention (CDC) **Pandemic Severity Index** (Modeled after the five levels of severity used for hurricanes and designed to help officials determine whether to take steps such as advising employers to promote tele-work)**:**
<http://www.cdc.gov/od/oc/media/pdf/MitigationSlides.pdf>

U.S. Department of Homeland Security (DHS), **National Strategy for Pandemic Flu:**
<http://www.dhs.gov/xprevprot/programs/editorial_0760.shtm>

Federal Emergency Management Agency (FEMA) **Emergency Assistance for Human Influenza Pandemic, Disaster Assistance Policy 9523.17**
<http://www.fema.gov/government/grant/pa/9523_17.shtm>

Congressional Research Service (CRS) Report for Congress, **Pandemic Influenza: An Analysis of State Preparedness and Response Plans,** September 2007:
<http://opencrs.cdt.org/document/RL34190>.

The White House, **National Strategy for Pandemic Influenza Website:**
<http://www.whitehouse.gov/homeland/pandemic-influenza.html>

The White House, **National Strategy for Pandemic Influenza: Implementation Plan,** May 2006:
<http://www.whitehouse.gov/homeland/pandemic-influenza-implementation.html>

Bureau of Justice Assistance (BJA) **Pandemic Planning Website:**
<http://www.ojp.usdoj.gov/BJA/pandemic/pandemic_main.html>

The Government Accountability Office (GAO), *Influenza Pandemic: Opportunities Exist to Address Critical Infrastructure Protection Challenges That Require Federal and Private Sector Coordination*, GAO-08-36, October 2007:
<http://www.gao.gov/cgi-bin/getrpt?GAO-08-36>

GAO Report Highlights: <http://www.gao.gov/highlights/d0836high.pdf>

National/ International Organization, Academia and Consortium Resources

National Governor's Association (NGA) publication on state-wide pandemic planning, ***"Preparing for a Pandemic Influenza: A Primer for Governors and Senior State Officials."***
<http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=8f6e0cc3a2e7c010VgnVCM1000001a01010aRCRD&vgnextchannel=4b18f074f0d9ff00VgnVCM1000001a01010aRCRD>

The National Center for Critical Incident Analysis, Report, *Pandemic Influenza – Nature's Bioterrorist Threat*:
<http://www.criticalincident.org/reports/march2005.pdf>

World Health Organization (WHO) **Epidemic and Pandemic Alert and Response (EPR) Website:**
<http://www.who.int/csr/disease/influenza/pandemic/en/>

Articles and Reports

Government Technology, ***Some IT workers may get priority on flu pandemic vaccine***, October 2007, News Report
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9044164&intsrc=hm_list>

Government Technology, ***Georgia Recipient of Pandemic Flu Preparedness Funds***, September 2007, News Report
<http://www.govtech.com/gt/articles/140023?utm_source=newsletter&utm_medium=email&utm_campaign=HHS_2007_9_13>

"***Simulation Suggests that Flu Outbreak Could Cripple the Internet***" – Government Computer News (GCN), May 2006 <http://www.gcn.com/online/vol1_no1/40631-1.html>

Influenza Pandemic Simulation, Implications for the Public and Private Sectors, a report
by Booz Allen Hamilton, 2006:
<http://www.boozallen.com/media/file/Influenza_Pandemic_Simulation.pdf>