# Department of Homeland Security Daily Open Source Infrastructure Report for 12 February 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

**Daily Highlights**

- The Associated Press reports police are on the lookout for those responsible for shooting bullet holes in the Westfield water tank causing extensive damage to the tank, which supplies water to the community of Toquerville in southern Utah. (See item 18)
- The New York Times reports New York City will soon test ways of strengthening defenses against a nuclear device or a radioactive dirty bomb attack, with an elaborate network of radiation alarms at relevant bridges, tunnels, roadways, and waterways, creating a 50−mile circle around the city. (See item 23)

**DHS Daily Open Source Infrastructure Report *Fast Jump***



## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 09, Associated Press* — **Coalmines must provide four days of air.** Underground coalmines must provide up to four days of breathable air to keep miners alive in emergencies such as an explosion or a tunnel collapse, federal regulators announced Thursday, February 8. A law enacted last year after a string of deadly accidents, including the deaths of 12 miners at the Sago Mine in January 2006, required mine operators to provide enough air to keep miners alive in an emergency but did not specify how much. On Thursday, the federal Mine Safety and Health Administration gave mine operators several options to comply with the requirement.

Among the options were providing a 96−hour supply of air in a shelter or an area of the mine designated for barricading against contaminants or drilling boreholes to provide a constant flow of fresh air to a designated area or shelter. Mine operators have 30 days to submit plans to the agency, which has been criticized by the United Mine Workers labor union and members of Congress for not implementing the law quickly enough after it took effect in June.
Source: http://www.nytimes.com/aponline/us/AP−Mine−Safety−Air.html

2. *February 08, Nuclear Regulatory Commission* — **NRC chairman addresses nuclear reactor growth issue.** Nuclear Regulatory Commission (NRC) Chairman Dale Klein said Thursday, February 8, the NRC hopes not be to an impediment to the licensing of new reactors that utilities want to build in the coming decade. “I am a regulator and I cannot promote nuclear energy,” Klein said at the third Annual Platts Nuclear Energy Conference, “but let me indulge in a bit of optimism. I do not believe the NRC to be a bottleneck in the process.” Klein, describing his vision of standard applications and a strong regulatory authority with set requirements, said in prepared remarks that the NRC will strive to provide “the regulatory stability needed in the uncertain first days of a rapidly expanding, technologically complex and capital−intensive industrial sector.” He also said he hopes to reduce the time necessary to process new reactor applications. He predicted that the “pinch points” in the licensing process are finding high quality components, hiring sufficient qualified personnel and connecting substantial numbers of new plants to the nation’s electrical grid. He added that the NRC and the Federal Energy Regulatory Commission are working closely to address issues associated with adding plants to the nation’s electrical grid to meet increasing demand for electricity.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2007/07−0 23.html

3. *February 07, San Antonio Express−News* — **Valero crude oil refineries experience five malfunctions within two weeks.** The nation's largest refiner, Valero Energy Corp. has had five refinery malfunctions in 11 days, according to information the company filed with state regulators. "Refining crude oil is like dealing with a controlled explosion," said Evan Smith, co−portfolio manager at San Antonio−based U.S. Global Investors' Global Resources Fund. "My sense is that this is a coincidence that the incidents are happening at about the same time. "Valero is a lot bigger than it used to be but they're not known as sloppy operators," Smith said. "I don't think there are any systematic operating issues or strategic capital not going to the right place."
Source: http://www.mysanantonio.com/business/stories/MYSA020807.3E.valero.130114b.html

[Return to top]

## Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

## Defense Industrial Base Sector

4.

*February 08, Federal Computer Week* — **DISA could spend close to $1 billion on security over three years.** The Defense Information Systems Agency (DISA) plans to spend $959 million on network and information systems security over the next three years, with an emphasis on protecting against insider threats and defending classified networks, according to 2008 budget documents. Funding for DISA's Information Systems Security Program (ISSP), from fiscal 2007−2009, includes $819 million in operations and maintenance and $140 million for procurements. DISA has budgeted $247 million for ISSP in 2007, with $251 million requested for 2008 and $319 million planned for 2009. The ISSP budget calls for increased defense against internal security threats. The agency plans to deploy tools to 1,500 locations worldwide to analyze, detect and respond to insider threats against information and information systems, according to the budget documents. DISA also is stepping up its defense of the Secret Internet Protocol Router Network.
Source: http://www.fcw.com/article97614−02−08−07−Web

[Return to top]

## Banking and Finance Sector

5. *February 09, USA TODAY* — **Tech experts plot to catch identity thieves.** The topic of data protection stole the show at the RSA Conference on computer security in San Francisco, CA, last week. Identity theft and corporate espionage were dominant themes among the 15,000 attendees. Identity theft was a major source of discussion. There was no shortage of hand−wringing over the consequences of consumer data ending up in the hands of thieves, and the fear was highlighted by a Federal Trade Commission report of rampant consumer complaints about identity theft. But the unreported filching of data from government agencies and private enterprises worries some. On Tuesday, February 9, Senators Patrick Leahy (D−VT) and Arlen Specter (R−PA) introduced a data−privacy bill that makes it a crime to conceal security breaches involving personal data. Since February 2005, more than 100 million records containing personal information have been subject to some sort of security breach, according to the non−profit Privacy Rights Clearinghouse. Attacks have also increased against retailers as large financial institutions have fortified their computer−security systems, forcing thieves to go elsewhere.
Source: http://news.yahoo.com/s/usatoday/20070209/tc_usatoday/techexpertsplottocatchidentitythieves

6. *February 08, Federal Trade Commission* — **FTC issues advice on preventing counterfeit check scams.** A new scam is swindling consumers: counterfeit checks that seem legitimate to both bank employees and consumers. The Federal Trade Commission (FTC) is issuing a new brochure, Giving the Bounce to Counterfeit Check Scams, which explains these scams and how to avoid them. The basics of counterfeit check schemes are the same. The consumer receives a generous check with an explanation that they've just won an award, a prize, a lottery or some other windfall. The consumer is instructed to deposit the check and wire a portion back to pay fees, taxes, or the like. The consumer deposits the check, the bank credits the funds to the consumer's account, and the consumer wires the money to the sender. Some time later, both the bank and the consumer learn the check was bogus. Unfortunately, the consumer is out of luck: the money that was wired can't be retrieved and, by law, the consumer is responsible for the deposited check. Among other guidelines, the FTC advises consumers not to rely on funds from

checks unless they know and trust the person who gave them the check or, better yet, until the bank confirms that the check has cleared.
FTC Brochure: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre40.htm
Source: http://www.ftc.gov/opa/2007/02/fyi0716.htm

[Return to top]

## Transportation and Border Security Sector

7. *February 10, Associated Press* — **British bus firm to acquire Laidlaw.** British bus and train operator FirstGroup PLC announced a $2.8 billion deal Friday, February 9, to acquire Greyhound owner Laidlaw International Inc., whose business is focused more on its fleet of 40,000 school buses. If it goes through, the transaction would pair the two largest school bus operators in the United States and Canada and give the combined company 40 percent of the school bus market. It also may leave Greyhound Lines Inc. in need of yet another new driver. FirstGroup CEO Moir Lockhead said the deal "will considerably enhance the group's existing activities in North America," namely a 13 percent stake in the North American school bus market. Analysts suggested that not only are intercity buses not FirstGroup's core area of expertise, owning Greyhound would risk a negative reaction to an iconic American operation being run by foreigners. One suggested Greyhound would be a better fit with Stagecoach's Megabus USA operations. Greyhound was founded in 1914 by a Swedish immigrant, Carl Eric Wickman, to transport Minnesota's miners for 15 cents a ride and became a coast−to−coast powerhouse as interstate highways proliferated. Its popularity peaked in the late '60s and early '70s.
Source: http://www.buffalonews.com/editorial/20070210/1047027.asp

8. *February 10, This is London (United Kingdom)* — **A tiny airline spy that spots bombers in the blink of an eye.** Tiny cameras the size of a fingernail linked to specialist computers are to be used to monitor the behavior of airline passengers as part of the war on terrorism. Cameras fitted to seat−backs will record every twitch, blink, facial expression or suspicious movement before sending the data to onboard software which will check it against individual passenger profiles. Scientists from Britain and Germany are developing a system they hope will make it virtually impossible to hijack an airliner by providing pilots and cabin crew with an early warning of a possible terrorist attack such as 9/11. They say that rapid eye movements, blinking excessively, licking lips or ways of stroking hair or ears are classic symptoms of somebody trying to conceal something. A separate microphone will hear and record even whispered remarks. Islamic suicide bombers are known to whisper texts from the Koran in the moments before they explode bombs. Airlines gave the scheme a cautious welcome, indicating it would be too expensive to fit on existing commercial aircraft and that it would probably be ten years before such systems were fitted to new planes.
Source: http://www.thisislondon.co.uk/news/article−23385096−details/
The+tiny+airline+spy+that+spots+bombers+in+the+blink+of+an+e ye/article.do

9. *February 09, Associated Press* — **Comair delays pilots' concessions, receives proposal from union.** Comair delayed its plan to implement wage cuts and other concessions on its pilots Friday after receiving a new contract proposal from the pilots' union, a spokesperson for the regional airline said. Comair was poised to impose $15.8 million in cuts on the 1,500 pilots at

11:59 p.m. Friday. Union spokesperson Paul Denke would not discuss details of the union's plan, except to say that it was presented by phone and that a financial expert helped the group repackage its proposal. Comair spokesperson Kate Marx said the cuts would be postponed at least until Monday, February 12. The Delta Air Lines Inc. subsidiary has said concessions were necessary as part of its restructuring plan to save $70 million annually. Comair, along with its Atlanta−based parent, filed for bankruptcy in September 2005. Comair operates 795 flights daily to about 100 cities in North America.
Source: http://www.usatoday.com/travel/news/2007−02−09−comair−pilots_x.htm

10. *February 08, USA TODAY* — **High−speed ferry to connect Hawaiian islands.** Hawaii is scheduled to get its first regular interisland passenger ferry service in more than 25 years this summer, but the project is raising concerns among environmentalists about whale collisions, invasive species and congestion. Hawaii Superferry launched the first of its new $90 million high−speed catamaran ferries last month in Mobile, AL, and plans to begin daily trips between Oahu and Maui and Kauai on July 1. "Hawaii is ripe for this. It's one of the last populated island chains anywhere in the world without some kind of regular ferry service," Superferry Chief Executive Officer John Garibaldi said. The ferry company has received almost $200 million in federal maritime loan guarantees to build its ships and has the backing of the state government, which is contributing about $40 million in harbor improvements. A second ferry is scheduled to be operational in 2009, when service will expand to the island of Hawaii.
Source: http://www.usatoday.com/news/nation/2007−02−08−hawaii−super− ferry_x.htm

11. *February 07, Greenwich Time (CT)* — **Grand Central−bound train derails, no injuries reported.** A New Haven Line train carrying about 600 passengers derailed Wednesday, February 7, as it approached the platform at Grand Central Terminal in New York, injuring none, but delaying many commuters for more than an hour. The first two rail cars on the 7:42 a.m. EST semi−express train out of Stamford, CT, had successfully platformed at track 19 in Grand Central just before 8:40 a.m. when the third car derailed, according to Metro−North Railroad officials. The cause of the derailment was unknown and still under investigation as of Wednesday afternoon, railroad officials said. Passengers on the first two rail cars were able to exit the train without a problem, but commuters on the remaining five cars needed the assistance of Metropolitan Transportation Authority (MTA) emergency personnel, railroad spokesperson Dan Brucker said. Third−rail power was turned off at the track, while MTA police and fire officials helped passengers off the cars, Brucker said. The derailment was the first one inside Grand Central in about five years, Brucker said.
Source: http://www.greenwichtime.com/news/local/scn−trainstory0207,0 ,1566088.story?coll=green−news−local−headlines

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

12. *February 09, Animal and Plant Health Inspection Service* — **Proposal to change the disease status of four countries in the European Union.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Friday, February 9, announced a proposal to amend its animal import regulations by changing the disease statuses of the Czech Republic, Latvia, Lithuania and Poland. The proposed changes would add these countries to the regions of the European Union (EU) considered low risk for classical swine fever (CSF) and free of swine vesicular disease (SVD). Latvia and Lithuania would also be added to the list of regions considered free of foot−and−mouth disease (FMD) and rinderpest. When the Czech Republic, Latvia, Lithuania and Poland became members of the EU, they adopted its animal health, welfare and identification legislation, including legislation specific to CSF, FMD and SVD. By adopting these laws and regulations, as well as undergoing a thorough APHIS−risk assessment. This proposed change in status means that there would be fewer restrictions on the import of animals and animal products from these countries. For example, no swine may be imported from any region affected with CSF or SVD, although some cooked and cured products from affected regions are allowed into the U.S. Countries under FMD restriction are not allowed to export ruminant animals and fresh or chilled ruminant animal product into the U.S.
Source: http://www.aphis.usda.gov/newsroom/content/2007/02/eustatus. shtml

13. *February 09, Agricultural Research Service* — **Map of Africanized honeybee spread updated.** The map of Africanized honeybees' spread in the U.S. has been updated. The map shows the spread of Africanized honeybees (AHB) by county by year. AHBs have continued their slow territorial expansion in the southern United States, and have now been confirmed in nine states. The map lists a county only when that state officially declares it to be Africanized. There are discontinuities in the spread, especially between Louisiana and Florida where AHB spread is likely a result of human−assisted transport—such as AHB swarms hitchhiking on trucks, railroad cars, ships or airplanes. Human−assisted transported AHBs are not considered a territorial spread unless the honeybees become established beyond the original swarm find.
Map: http://www.ars.usda.gov/ahbmap/
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

14. *February 08, Dow Jones* — **Foot−and−mouth seen in Brazil, near Paraguay.** Brazilian federal animal health inspectors said they discovered the virus that causes foot−and−mouth disease still present in some calves in three towns where an outbreak occurred in October 2005, the local Estado newswire reported Thursday, February 8. The state of Mato Grosso do Sul towns include Eldorado, Mundo Novo and Japora, all on the Paraguay border and all the focus of a large foot−and−mouth diseases outbreak that started on October 10, 2005. According to the newswire's report, 2.7 percent of the 11,449 blood samples of young calves showed signs of the virus in the blood stream. Mato Grosso do Sul is Brazil's No. 1 cattle state and has been banned from international beef markets since late 2005. The disease hasn't been reported outside of the original contamination zone. The state was testing new cattle on some 444 properties to see if the 2005−2006 cattle culling in the region had eliminated the virus.
Source: http://www.cattlenetwork.com/content.asp?contentid=104577

[Return to top]

# Food Sector

15. *February 09, Animal and Plant Health Inspection Service* — **Japan reopens market to U.S. chipping potatoes.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Friday, February 9, announced that Japan has reopened its market to U.S. chipping potatoes following the completion of a scientific evaluation. Japan temporarily suspended U.S. imports of all varieties of chipping potatoes in April 2006 immediately following the first U.S. detection of potato cyst nematode (PCN) in Idaho. After conducting a detailed scientific evaluation, Japanese officials concluded that the isolated detection presents no risk of introducing PCN in Japan if the U.S. takes the following actions: The potatoes may only be shipped from these designated states: Arizona, Wisconsin, Oregon, California, Colorado, Texas, New Mexico, North Dakota, Florida, Michigan, Minnesota, Maine and Washington; The potato fields must be tested and certified to be free of PCN prior to export; and The potatoes must be washed before exporting. Before Idaho is eligible to export chipping potatoes to Japan, the state must complete a comprehensive PCN survey. Currently, all U.S. chipping potatoes exported to Japan must be grown from seed potatoes produced outside of Idaho. PCN is a major pest of potato crops. If left uncontrolled, nematodes can cause up to 80 percent yield loss.
Source: http://www.aphis.usda.gov/newsroom/content/2007/02/jchippot. shtml

16. *February 09, USAgNet* — **Smoked meats recalled.** Jones Packing Inc. of Dodge City, KS, is recalling 1,331 pounds of smoked meats because they may be underprocessed the Kansas Department of Agriculture announced. The recalled meats include 903 pounds of smoked ham, 178 pounds of smoked roast beef and 250 pounds of smoked bacon. The potential underprocessing was discovered through records reviewed by Kansas Department of Agriculture food safety inspection personnel. There have been no reports of illness due to consuming these products.
Source: http://www.usagnet.com/story−national.php?Id=341&yr=2007

17. *February 06, U.S. Food and Drug Administration* — **Peanut paste recalled.** Peanut Processors, Inc. of Dublin, NC, is recalling certain bulk loads of peanut paste because the paste may contain small particles of metal. These products were sold to manufacturers of consumer food products in Virginia, Tennessee and North Carolina. Each of the food product manufacturers has been given notice of the recall and of the recall and of the specific shipments recalled. The metal particles were detected through internal quality checks by one manufacturer. No consumer complaints have been reported.
Source: http://www.fda.gov/oc/po/firmrecalls/peanut02_07.html

[Return to top]

## Water Sector

18. *February 08, Associated Press* — **Toquerville officials search for water−tank vandals.** Police are on the lookout for those responsible for putting bullet holes in a water tank in southern Utah. The incident apparently happened on Sunday, February 4. That's when deputies say they discovered water spraying out of the two bullet holes in the Westfield water tank. Witnesses claim several teenagers were shooting rifles in the area. Officers say the bullet holes caused extensive damage to the tank, which supplies water to the community of Toquerville.

Deputies say a half−million gallons of water will now need to be drained out of the tank in order to fix it.
Source: http://www.sltrib.com/news/ci_5183596

19. *February 07, Washington University* — **Seismic model of vast water reservoir revealed.** A seismologist at Washington University in St. Louis, MO, has made the first 3−D model of seismic wave damping −− diminishing −− deep in the Earth's mantle and has revealed the existence of an underground water reservoir at least the volume of the Arctic Ocean. It is the first evidence for water existing in the Earth's deep mantle. One of the most dramatic features in the global mantle shear−wave attenuation model is a very high−attenuation anomaly at the top of the lower mantle beneath eastern Asia. This anomaly is believed due to water that has been pumped into the lower mantle via the long history of the subduction of oceanic lithosphere −− crust and upper mantle −− in this region.
Source: http://news−info.wustl.edu/news/page/normal/8222.html

[Return to top]

## Public Health Sector

20. *February 11, BBC News* — **Bird flu virus kills Indonesian.** A 20−year−old woman in Indonesia who tested positive for bird flu has died, becoming the country's 64th human victim, a health official said. The woman had a history of contact with infected chickens, officials said. She died on Sunday, February 11, in West Java province, a day after being diagnosed with the H5N1 strain of the virus. Since Indonesia's first human case was discovered in 2005, 84 people have contracted the virus and 64 have died. Two of the woman's neighbors are also in hospital showing symptoms of the virus.
Source: http://news.bbc.co.uk/2/hi/asia−pacific/6351247.stm

21. *February 09, Associated Press* — **Two North Carolina hospitals warn of virus outbreak.** Two Greensboro, NC, hospitals are asking visitors, especially children, to stay away until they control an outbreak of a highly contagious stomach virus that has sickened patients and staff members. Doctors confirmed an outbreak at the hospital and believe the virus also has hit Wesley Long Hospital. The number of people affected wasn't immediately available, hospital officials said. Three suspected norovirus cases first appeared on February 1 and were not confirmed until Wednesday, February 7, Doug Allred, a spokesperson for Moses Cone Health System, said. The hospitals will admit new patients who will be sent to areas considered clear of the virus.
Source: http://www.breitbart.com/news/2007/02/09/D8N6BIMO0.html

22. *February 09, Reuters* — **Exposure to antibiotics linked to resistance.** Exposure to common antibiotics used to treat respiratory infections can increase resistance to the drugs, Belgian scientists said on Friday, February 9. In a study that looked at the impact of the drugs on individuals, Professor Herman Goossens of University Hospital in Antwerp showed a single course of a drug can lead to a build−up in resistance. "Exposure to the antibiotics was the strongest variable and this was independently associated with resistance," said Goossens. He and his team analyzed the use of macrolide antibiotics, widely used drugs in primary care to

treat ear, throat and lung infections. The scientists compared two macrolide antibiotics −− clarithromycin and azithromycin −− against a placebo on more than 200 healthy volunteers. They took several samples of bacteria from the volunteers before and up to six months after giving them antibiotics. The levels of resistant bacteria rose following the drug treatment. "We have clearly defined, at the individual level, the direct effect of antibiotic use in selecting resistant organisms," Goossens told Reuters.
Source: http://today.reuters.com/news/articlenews.aspx?type=healthNews&storyID=2007−02−09T133805Z_01_L08260078_RTRUKOC_0_US−ANTIBIOTICS−RESISTANCE.xml&WTmodLoc=HealthNewsHome_C1_%5BFeed%5D −7

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

**23.** *February 09, New York Times* — **New York to test ways to prevent nuclear terror.** New York City is about to become a laboratory to test ways of strengthening the nation's defenses against a terror attack by a nuclear device or a radioactive "dirty bomb." Starting this spring, the Bush administration will assess new detection machines at a Staten Island port terminal that are designed to screen cargo and automatically distinguish between naturally occurring radiation and critical bomb−building ingredients. And later this year, the federal government plans to begin setting up an elaborate network of radiation alarms at some bridges, tunnels, roadways and waterways into New York, creating a 50−mile circle around the city. The effort, which could be expanded to other cities if proven successful, is a major shift of focus for the Department of Homeland Security. As it finishes installing the first generation of radiation scanners at the nation's ports and land border crossings, the department is trying to find ways to stop a plot that would use a weapon built within the United States.
Source: http://www.nytimes.com/2007/02/09/nyregion/09nuke.html?hp&ex=1171083600&en=bf1c7664805cbb4b&ei=5094&partner=homepage

**24.** *February 08, Federal Emergency Management Agency* — **President declares major disaster for Florida.** Based on additional information collected by state, local, and federal disaster assessment teams, the head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) Thursday, February 8, announced that federal disaster aid has been made available for the state of Florida to help people and communities recover from the effects of severe storms, tornadoes, and flooding on December 25, 2006. FEMA Director David Paulison said the assistance was authorized under a major disaster declaration issued for the state by President Bush. The President's action makes federal funding available to affected individuals in Volusia County. "We understand these storms have strained the resources of the state government and nonprofit groups aiding in the community's response and recovery." Paulison said. "With the additional information provided by the state, we felt it was certainly appropriate to provide supplemental federal aid necessary to assist our partners in their efforts."

The assistance, to be coordinated by FEMA, can include grants to help pay for temporary housing, home repairs and other serious disaster−related expenses. Low−interest loans from the U.S. Small Business Administration also will be available to cover residential and business losses not fully compensated by insurance.
Source: http://www.fema.gov/news/newsrelease.fema?id=34006

25. *February 08, Government Technology* — **Florida conducts annual Homeland Security exercise.** Governor Charlie Crist joined Florida's Cabinet officers, state agency heads, and officials in law enforcement and emergency management to conduct the fifth annual homeland security "tabletop" exercise at the State Emergency Operations Center. The exercise is an annual drill where the Governor and top state officials respond to mock terrorism and homeland security threats. The scenario of the 2007 training exercise was a terrorist event involving a radiological threat. The primary objective of the exercise is to give the state's top executives and staff an opportunity to engage in policy−level discussions with federal and local officials. The exercise provides the opportunity to evaluate information−sharing and to enhance coordination of their response plans and recovery roles with partner agencies. Representatives from the Federal Bureau of Investigation, U.S. Coast Guard, Florida National Guard, and the Federal Emergency Management Agency also participated in the half−day drill.
Source: http://www.govtech.net/news/news.php?id=103837

26. *February 08, Federal Computer Week* — **DHS to test communications strategy in exercise.** As part of an exercise involving a simulated terrorism attack, the Department of Homeland Security (DHS) wants to gauge the extent to which the public would trust information DHS releases electronically. Like its predecessors, the fourth Top Officials (TopOff) exercise is intended to test the nation's readiness to deal with a large−scale terrorist attacks. This time, the exercise will test the department's public communications strategy. The idea is to give the public information that is as complete and timely as possible about the events surrounding the attacks and what actions they should take to protect themselves. DHS will provide that information in two formats: a live video feed and a Website. The live feed will resemble a newscast, according to DHS, featuring interviews with public officials and other experts, while the Website will function more like a newspaper.
Source: http://www.fcw.com/article97613−02−08−07−Web

[Return to top]

## Information Technology and Telecommunications Sector

27. *February 09, eWeek* — **Cyber−security czar calls on IT industry for help.** Addressing a crowded room of attendees at the ongoing RSA Security Conference on Thursday, February 8, Greg Garcia, assistant secretary for cyber−security and telecommunications at the Department of Homeland Security, said that he and his team are already hard at work creating policies that aim to better protect critical infrastructure. Over the first four months on the job, Garcia said, he has focused primarily on establishing a game plan for his office's future projects and working to establish inroads with members of the IT and communications industries to encourage private companies' contribution to those efforts. While the federal government is aggressively looking for ways to create stronger protections for the nation's IP backbone, the process will not be able to move forward quickly unless businesses and academic institutions that control the nation's

largest networks are willing to pitch in, he said. The cyber−security chief said that his initial priorities revolve around work to breed cooperation between federal agencies to develop common security policies for defending networks and to help the private sector strengthen national preparedness and incident−response plans.
Source: http://www.eweek.com/article2/0,1895,2093175,00.asp

**28.** *February 09, eWeek* — **Next wave in security: Protecting smart phones, PDAs.** With the number of employees using smart phones and other mobile devices, corporations must start to focus their security on more than just their network perimeter, according to security analysts and specialists attending the RSA Conference. Research done by the Business Forum Management Program in 2006 found that roughly 49 percent of the 680 executives surveyed are "mobile" or "very mobile," and about 80 percent plan to increase the number of mobile devices used in the next few years. And even though a quarter of the respondents reported having critical data stored on mobile devices, 40 percent said they have no security and compliance measures in place to protect data on those devices. The next wave in security will deal with protecting items such as smart phones, said Curtis Cresta, vice president and general manager of North American Operations for F−Secure. Smart phones, he said, are easier to maintain and cost less than laptops. In other regions, such as Asia and Europe, the widespread use of business applications on mobile phones has already begun, noted Gartner analyst John Pescatore. With the increased presence of applications on cell phones, the threat of Web−based attacks becomes less theoretical, he said.
Source: http://www.eweek.com/article2/0,1895,2093092,00.asp

**29.** *February 09, Register (UK)* — **Anatomy sheds new light on Storm Worm.** A deluge of Trojan−laced spam that slyly tricked recipients by promising information about winter storms ravaging Northern Europe last month was even craftier than originally thought. Among the new revelations: The Storm Worm malware launched DDoS attacks on a host of Websites related to spam, antispam and just about anything else that may have piqued the perpetrators' ire, according to Joe Stewart, senior security researcher for SecureWorks. It also appears to be a close descendant of worms that spread in November and December, a connection that few if any have made until now. Stewart says Storm Worm is a variant of the Win32/Nuwar worm that spread as early as November. Unbeknownst to most at the time, Storm Worm also installed a DDoS attack tool that wreaked havoc on various Websites. Among them was spamnation.info, which is dedicated to countering the menace of spam. Other sites that were also targeted by Storm Worm included stockpatrol.com and several sites Stewart guesses were run by rival spammer gangs.
Anatomy of a worm report: http://www.secureworks.com/research/threats/view.html?threat=storm−worm
Source: http://www.theregister.co.uk/2007/02/09/storm_worm_anatomy/

**30.** *February 08, eWeek* — **Highly−critical flaw discovered in Trend Micro products.** A dangerous buffer−overflow flaw in Trend Micro anti−virus software products was reported by Trend Micro and confirmed by security researchers at iDefense Labs. Researchers at Secunia have also posted an advisory on this vulnerability and have deemed this to be highly critical. This flaw can be exploited in both Windows and Linux systems, and could be used to gain access to machines, cause denial−of−service activity and allow attackers total control of affected systems. Trend Micro responded to the vulnerability by pushing out a patch that a

company spokesperson says fixes the issue. The vulnerability targets all scan engine and pattern file technology in Trend Micro products due to an error within UPX compressed executables.
Secunia Advisory: http://secunia.com/advisories/24087/
Source: http://www.eweek.com/article2/0,1895,2092841,00.asp

31. *February 08, IDG News Service* — **Big set of Microsoft security patches coming Tuesday.** Microsoft plans to release 12 sets of security patches Tuesday, February 13, fixing critical vulnerabilities in a number of its products, including the company's new security software. The bulk of the patches will fix flaws in the Windows operating system and Office, Microsoft said. Five of the updates will be for Windows, and two of them will be for Office. Microsoft also plans to release one less−critical update that addresses flaws in both Windows and Office.
Source: http://www.infoworld.com/article/07/02/08/HNmssecuritypatche s_1.html

32. *February 08, CNET News* — **Spyware, data privacy bills reappear in House.** In October 2004, all but one member of the U.S. House of Representatives voted for a bill that was supposed to curtail the threat of malicious PC−disrupting spyware. But the Senate ignored it. So the House once again approved spyware regulations in May 2005, which yielded precisely the same lack of a result. Hoping that the third time proves the charm, House leaders on Thursday, February 8, introduced a bill that would once again try to impose 31 pages of regulations on the software industry in an effort to define what types of activities are permissible and which ones aren't.
Source: http://news.com.com/Spyware%2C+data+privacy+bills+reappear+in+House/2100−1028_3−6157826.html?tag=nefd.top

**Internet Alert Dashboard**

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

# Commercial Facilities/Real Estate, Monument &Icons Sector

33. *February 09, Enid News and Eagle (OK)* — **Suspicious object draws bomb squad attention.** Enid, OK, police had a “suspicious device” to investigate Thursday morning, February 8. Authorities ended up calling Oklahoma Highway Patrol’s bomb squad from Oklahoma City to a residence in the 2900 block of North Adams. “It was definitely constructed by someone to look like an explosive device,” said Enid Police Department Capt. Dean Grassino. The metal cylindrical object, covered with duct tape and with protruding white electrical wires, was found in the front yard of the residence. The bomb squad’s robot, outfitted with a camera and mechanical arm examined the object, Grassino said, which was hollow. “It was able to examine the device and determine it was not an explosive device,” he said. Police did not know if the device was placed at the home purposely, but do know it was constructed to look like an explosive device.

Source: http://www.enidnews.com/localnews/local_story_040014536.html

[Return to top]

# General Sector

Nothing to report.
[Return to top]