Daily Open Source Infrastructure Report
12 April 2012

Top Stories

- Cybercrooks forged a Zeus-based trojan that enables them to siphon funds from businesses using cloud-based payroll service providers. – *The Register* (See item **9**)
- A federal court suspended operations of two debt-collecting businesses a man reportedly used to swindle $5 million from hundreds of thousands of U.S. consumers. – *U.S. Federal Trade Commission* (See item **11**)
- An audit revealed the Department of Veterans Affairs failure to fully comply with federal information security laws resulted in more than 15,000 outstanding risks. – *Federal Computer Week* (See item **33**)
- Microsoft released security bulletins April 10 that addressed many bugs that could be exploited by attackers to remotely inject and execute malicious code. – *H Security* (See item **38**)
- Firefighters battled wildfires that consumed thousands of acres in 9 states on the East Coast April 10. – *CBS News* (See item **50**)

Fast Jump Menu

Energy Sector

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

1. *April 10, KFYR 5 Bismarck* – (North Dakota) **OSHA cites oil well for violations.** A Wyoming-based oil company is facing over $65,000 in fines from the U.S Department of Labor's Occupational Safety and Health Administration (OSHA) for safety violations in an oil field near Ray, North Dakota, KFYR 5 Bismarck reported April 10. According to an OSHA release, Cyclone Drilling, based out of Gillette, Wyoming, was cited with two repeat, five serious, and one other than serious violation of safety and health standards for exposing workers on an oil drilling rig to electrical, fire, and fall hazards, among others.
Source: http://www.kfyrtv.com/News_Stories.asp?news=56364

2. *April 10, Associated Press* – (Louisiana) **Coast Guard: Tanker spills fuel oil on Miss. River.** A tanker discharged fuel oil into the Mississippi River a few miles from New Orleans, the U.S. Coast Guard (USCG) said April 10, but authorities reported no signs of the shoreline, wildlife, or a nearby drinking water system being affected. The USCG listed Overseas Shipholding Group Inc. as the responsible party. The firm issued a statement saying the initial estimate was that only about 50 gallons had been discharged. The USCG could not confirm the amount. A petty officer said a light, spotty sheen stretched 29 miles downriver from the initial cleanup site, which was about 10 miles downriver from New Orleans. The discharge from a ballast pipe on the 800-foot tanker Overseas Beryl was discovered April 9 and plugged 9 hours later, the USCG said. Both the Coast Guard and the Louisiana Department of Environmental Quality said there were no signs of oil affecting the shoreline or wildlife.
Source: http://www.businessweek.com/ap/2012-04/D9U28PB80.htm

3. *April 10, New Orleans Times-Picayne* – (Louisiana) **Valero refinery in St. Bernard Parish shuts down today after power failure.** Valero's St. Bernard Parish refinery in Meraux, Louisiana, lost power and had to shut down its production units April 10, a week after it was hit by lightning causing a power surge, subsequent electrical shortage, and sulfur dioxide and hydrogen sulfide releases. A Louisiana Department of Environmental Quality (DEQ) spokesman said sulfur dioxide, hydrogen sulfide, and volatile organic compounds were released into the flares, but that no exact amounts of such releases were immediately available. When the hydrocracker unit shut down, all releases were sent to the refinery's flares that burned off most of the chemicals, meaning the off-site release was reportedly minimal, at about 12 parts per billion of sulfur dioxide. A DEQ emergency response manager said such a release would not involve health issues, only "quality of life" factors, such as a bad smell that could possibly cause headaches.
Source:
http://www.nola.com/environment/index.ssf/2012/04/valero_refinery_in_st_bernard.html

[Return to top]

Chemical Industry Sector

4. *April 10, WTRF 7 Wheeling* – (Ohio) **The cause of the tanker truck accident has been determined.** A huge tanker truck hauling sodium hydroxide was speeding before it overturned April 9, closing Route 7 to I-470 westbound ramp in Belmont County, Ohio, for about 16 hours. The Ohio State Highway Patrol (OSHP) said April 10 the driver of the truck hauling 44,000 pounds of caustic soda was charged with unsafe speed for conditions. The chemical did not leak, but if it had, it could have resulted in a disaster, state police officials said. An OSHP sergeant said the truck was going much too fast around a tight curve, resulting in the accident.
   Source: http://www.wtrf.com/story/17377913/the-cause-of-the-tanker-truck-accident-has-been-determined

5. *April 10, WLOS 13 Asheville* – (North Carolina) **Driver charged in fiery crash.** The man behind the wheel of a tanker-truck hauling sulfuric acid that crashed on I-26 in Henderson County, North Carolina, the week of April 2 was cited for exceeding safe speed, WLOS 13 Asheville reported April 10. The accident on the Peter Guice Memorial Bridge damaged the bridge, shutting it down for more than 2 days. The driver cited in the wreck is due in court June 20.
   Source:
   http://www.wlos.com/shared/newsroom/top_stories/videos/wlos_vid_7151.shtml

For another story, see item **27**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *April 11, Today's Zaman* – (International) **Gendarmes seize smuggled radioactive substance in Ankara.** Teams from a Turkish anti-smuggling unit seized two glass tubes containing 500 grams of Cesium-137, a radioactive isotope of cesium, which they suspected was smuggled to Turkey from Russia through Georgia, Today's Zaman reported April 11. The teams acted after a tip-off that radioactive substances had been brought into Turkey from Georgia by means of a car with a German license plate. Upon searching the car, they found the Cesium-137 as well as an unlicensed gun and 18 coins thought to have historical value. Three people in the car, all Turkish nationals living in Germany, were detained. Sources said they all had prior charges related to smuggling on their criminal records. Cesium-137, the most common radioactive form of the metal cesium, is commonly used for the treatment of cancer and in a variety of gauges in the construction and drilling industries, but it can be used in nuclear weapon production as well. The half-life of cesium-137 is 30 years.
   Source: http://www.todayszaman.com/news-277106-gendarmes-seize-smuggled-radioactive-substance-in-ankara.html

For another story, see item **50**

[Return to top]

Critical Manufacturing Sector

7. *April 11, Detroit News* – (Michigan) **Prototype battery blamed in explosion at GM's Tech Center.** One person was transported to a hospital and four others were being evaluated April 11 after a prototype battery exploded at a battery research lab at the General Motors Technical Center in Warren, Michigan. The building housing the research lab received considerable damage. A GM official said the prototype lithium-ion battery that exploded during testing was being put through intensive tests designed to make it fail. Firefighters searched for other fires that might have been caused by the explosion. A HAZMAT team also was called to the scene. Some of the 80 workers were dismissed for the day, though most remained at the facility.
Source: http://www.detroitnews.com/article/20120411/AUTO0103/204110389/Battery-explosion-GM-s-Tech-Center-injures-1-2-people?odyssey=tab|topnews|text|FRONTPAGE

8. *April 10, WBAY 2 Green Bay* – (Wisconsin) **Small explosion evacuates Mercury Marine plant.** A small explosion and fire evacuated part of the Mercury Marine plant in Fond du Lac, Wisconsin, April 10. Firefighters said an explosion caused molten aluminum to shoot 25 feet to the ceiling, igniting dust particles, which wound up getting sucked into the exhaust system. Part of Mercury Marine plant 17 had to be evacuated while firefighters and plant employees put out the fire. The plant was expected to reopen after the exhaust system was checked out.
Source: http://www.wbay.com/story/17376018/2012/04/10/small-explosion-evacuates-mercury-marine-plant

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

9. *April 11, The Register* – (International) **New Zeus-based trojan leeches cash from cloud-based payrolls.** Cybercrooks have forged a Zeus-based trojan that targets cloud-based payroll service providers. A new attack, detected by transaction security firm Trusteer, shows crooks are going up the food chain. Researchers captured a Zeus configuration that targets Ceridian, a Canadian human resources and payroll services provider. The trojan works by capturing a screenshot of the payroll services Web page when a malware-infected PC visits the site. This data is uploaded, allowing crooks to obtain user ID, password, company number, and the icon selected by the user for the image-based authentication system – enough information to siphon funds from

compromised accounts into those controlled by money mules. Trusteer thinks crooks are targeting the small cloud service provider to get around the tougher problem of how to bypass industrial strength security controls typically maintained by larger businesses. Cloud services can be accessed using unmanaged devices that are typically less secure and more vulnerable to infection by Zeus-style financial malware.
Source: http://www.theregister.co.uk/2012/04/11/zeus_based_trojan_targets_payrolls/

10. *April 11, Santa Fe New Mexican* – (New Mexico) **FBI: Bank robbery suspect arrested.** The FBI April 10 arrested a Santa Fe, New Mexico man they say is connected to the April 2 robbery of U.S. Bank. The FBI said the suspect in the April 2 robbery is believed to be the man responsible for three other robberies in Santa Fe in the past year. Santa Fe olice and FBI investigators worked together on the case and arrest, according to an FBI spokesman. Video surveillance of the bank robbery showed a man displaying a hand gun and robbing the bank of an undisclosed amount. The same description matched video of a man who robbed other banks in Santa Fe in recent months.
Source: http://www.santafenewmexican.com/Local News/bank-robbery-arrest

11. *April 11, U.S. Federal Trade Commission* – (California; International) **Court halts alleged fake debt collector calls from India, grants FTC request to stop defendants who posed as law enforcers.** In response to charges from the U.S. Federal Trade Commission (FTC), a federal court halted an operation the agency alleges collected phantom payday loan debts that consumers either did not owe to the defendants or did not owe at all, the FTC announced April 11. The scheme involved more than 2.7 million calls to at least 600,000 different phone numbers nationwide, the FTC said. In less than 2 years, they fraudulently collected more than $5.2 million from consumers, many of whom were strapped for cash and thought the money they were paying would be applied to loans they owed, according to FTC documents filed with the court. The agency charged an individual, a California-based man, and two companies he controls with violating the FTC Act and the Fair Debt Collection Practices Act. Often pretending to be American law enforcement agents or representatives of fake government agencies, callers from India who were working with the defendants would harass consumers with back-to-back calls, the FTC said. The defendants typically demanded hundreds of dollars and, in violation of federal law, routinely used obscene language and threatened to sue or have consumers arrested, the FTC's complaint alleged. They also threatened to tell the victims' employers, relatives, and neighbors about the bogus debt, and sometimes followed through on these threats. Once victims were pressured into paying, the callers instructed them to use a pre-paid debit card such as a WalMart MoneyCard, another debit card, a credit card, or Western Union so the money could be deposited into one of the defendants' merchant processing accounts, the FTC charged.
Source: http://www.marketwatch.com/story/court-halts-alleged-fake-debt-collector-calls-from-india-grants-ftc-request-to-stop-defendants-who-posed-as-law-enforcers-2012-04-11

12. *April 11, Reuters* – (National; International) **U.S. SEC sues AutoChina for securities fraud.** U.S. securities regulators sued AutoChina International Ltd, its executives, and

others for securities fraud April 11. The U.S. Securities and Exchange Commission (SEC) said the company's employees, board members, and other Chinese citizens unlawfully bought and sold AutoChina stock to boost its trading volume as the company sought loans. AutoChina, which is based in China and owns and operates a commercial vehicle leasing business there, traded its shares on the NASDAQ stock market until October 2011. Its listing was suspended for failing to file required documents with the SEC. The defendants opened brokerage accounts beginning in October 2010, deposited some $60 million in the accounts, and bought and sold millions of shares of AutoChina stock, the SEC said. The lawsuit comes as the SEC steps up its inquiries into Chinese companies whose shares trade in the United States for accounting violations and other misconduct. The SEC lawsuit, filed in federal court in Massachusetts, is seeking civil penalties and other sanctions.
Source: http://www.reuters.com/article/2012/04/11/sec-autochina-idUSL2E8FB75S20120411

13. *April 10, St. Louis Post-Dispatch* – (Missouri) **US Fidelis co-founder admits federal tax evasion, fraud.** Four days after pleading guilty to state fraud charges, the co-founder of US Fidelis appeared April 9 in a U.S. district court in St. Louis, Missour to admit he also broke federal laws in cheating customers and failing to declare or pay taxes on $13 million received from the company in just 1 year. He pleaded guilty of conspiracy to commit mail and wire fraud and filing a false tax return. In his plea, he admitted he failed to declare $13 million in "distributions" from Fidelis on his 2006 federal tax return. That year, in fact, he reported a negative income, an assistant U.S. attorney said. He also acknowledged tricking consumers into believing auto service contracts Fidelis peddled by phone and mail were actually extended warranties from the vehicles' manufacturers. When customers canceled and asked for a refund, as up to 60 percent did, he admitted telling Fidelis staffers to withhold up to 40 percent of the amount due. He also admitted he and his brother used the latter's credit card to make payments for customers who they thought were likely to cancel or refuse to pay. The payments triggered full payment for Fidelis' share of the contract from a financing company, his plea says. Some of the admissions were similar to what was contained in his guilty plea April 5 to state charges of insurance fraud, stealing and unlawful merchandising practices. Prosecutors allege that the man and his brother funneled millions of dollars of profits into lavish homes, luxury goods, and payments on behalf of relatives. Fidelis, once one of the nation's largest sellers of auto service contracts, collapsed in 2009.
Source: http://www.loansafe.org/us-fidelis-co-founder-admits-federal-tax-evasion-fraud

[Return to top]

Transportation Sector

14. *April 11, Associated Press* – (National; International) **Korean Airlines jetliner diverted to Canadian military base after bomb threat.** A Korean Airlines Boeing 777 en route from Vancouver, Canada, to Seoul, South Korea, was diverted to a nearby Canadian military base after the airline's U.S. call center received a bomb threat.

Authorities continued to search the aircraft early April 11 and the Royal Canadian Mounted Police (RCMP) said nothing suspicious had yet been found. Korean Airlines said in a statement the call center received the threat April 10 about 25 minutes after take-off from Vancouver International Airport. Airline officials said the aircraft with 149 passengers then turned around. A Canadian spokeswoman for The North American Aerospace Defense Command, said two U.S. F-15 fighter jets from Portland, Oregon, escorted the plane to Canada's Comox air base on Vancouver Island, 113 miles outside Vancouver. The passengers and crew stayed overnight in the area while officials did a detailed search of the plane's luggage April 10, a RCMP inspector said. The inspector said the same Korean Airlines flight out of Vancouver faced a similar threat April 9, and the all-clear was given after a 2-hour search.
Source: http://www.startribune.com/nation/146959355.html

15. *April 10, PR Newswire* – (National; International) **Analysis of 15 failed terrorist plots against surface transportation provides insight into tactics, weapons, and more.** The Mineta Transportation Institute, April 10, released a research report, Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface Transportation, which examines several factors in 13 plots that authorities uncovered and foiled before attacks could be carried out. It also presents an additional two cases in which terrorists attempted to carry out attacks that failed. The reports analyzed plots from 1997-2012, primarily in the United States and the United Kingdom because they have been frequent targets. The report describes each plot in terms of the terrorists' plan, motivation, objective, target selection, tactics and weapons, reconnaissance, timing, security measures in place at the target, and how the plot was disrupted. A principal investigator noted that four of the plots involved chemical or biological substances. "It seems highly likely that the plotters in these cases had in mind the 1995 sarin attack in Tokyo," he said. "By mid-decade the poison fad was over." He said train and bus bombings in Madrid and London that killed many people led terrorists by the end of the decade to shift to multiple bombs as the attack prototype. The free report is available for download from transweb.sjsu.edu/project/2979.html.
Source: http://www.marketwatch.com/story/analysis-of-15-failed-terrorist-plots-against-surface-transportation-provides-insight-into-tactics-weapons-and-more-2012-04-10

For more stories, see items **4** and **5**

[Return to top]

Postal and Shipping Sector

16. *April 11, WFOR 4 Miami* – (Florida) **Woman injured after acid bomb explodes in mailbox.** A Davie, Florida woman was injured April 11 after some sort of explosive went off in her mailbox. She told police she was home the night of April 10 when she heard a loud "boom". She said she did not think anything about it. It was when she left her home April 11 that she noticed the door to her mailbox was hanging from the opening. When she reached inside, she told police her hand touched a plastic bottle and she experienced a burning sensation. She called police to report it and was treated for

minor injuries by Davie Fire Rescue. Police suspect the material inside the bottle and the mailbox was some sort of acid. A police captain said since the incident involved a mailbox they are looking into possible federal charges of deploying a destructive device.
Source: http://miami.cbslocal.com/2012/04/11/woman-injured-after-acid-bomb-explodes-in-mail-box/

17. *April 10, KPTV 12 Portland* – (Oregon) **Police looking for vandals behind mailbox bombs.** Police in Oregon City, Oregon are looking for whoever is responsible for blowing up four mailboxes over the weekend of April 7. Officers first received a 911 call the night of April 8 after two of the mailboxes were destroyed. They later discovered two more bombs had been set off. Remnants of the bomb were seized as evidence and sent to the Oregon State Police Crime Lab for fingerprint and other analysis. Police said the explosives were made by putting a cleaning solution — possibly toilet bowl cleaner — into a plastic bottle and adding tin foil. The tin foil causes a chemical reaction that builds pressure after the lid is closed, officers said. Eventually, the bottle explodes. The crimes committed fall under first-degree criminal mischief and carry a maximum penalty of up to $125,000 in fines and 5 years in prison.
Source: http://www.kptv.com/story/17375528/oregon-city-police-looking-for-mailbox-bombers

[Return to top]

Agriculture and Food Sector

18. *April 11, Food Safety News* – (International) **Two food poisoning incidents in India sicken hundreds.** Two food poisoning incidents in separate areas of India are getting attention for the large numbers of people sickened, Food Safety News reported April 11. The exact source of the illnesses remain unknown. Local residents in Jewar said as many as 300 suffered from food poisoning after eating at a ceremony at the nearby Chiroli village April 9. District officials are investigating and so far suspect food served for lunch was contaminated. Another large food poisoning incident occurred over the weekend of April 7 in the educational center of Pune, in western India. A total of 132 students were admitted to local hospitals April 7 when illnesses followed a mid-day meal. The students suffered from vomiting and nausea. All but 12 were discharged from hospitals April 8. All were discharged April 9. In neither food poisoning incident did Indian officials disclose the exact type of food-borne illness involved.
Source: http://www.foodsafetynews.com/2012/04/two-food-poisoning-incidents-in-india-sicken-hundreds/

19. *April 11, Minneapolis Star-Tribune* – (Minnesota; Midwest; International) **Botulism worries spur recall of fish, not yet gutted, sold in Twin Cities.** Minnesota state authorities are warning consumers about a threat to their health involving many hundreds of pounds of fish that have yet to be gutted being sold at ethnic grocery outlets in the Twin Cities, as well as elsewhere in the Upper Midwest. The Minnesota Department of Agriculture said April 10, more than 1,500 pounds of dried, uneviscerated fish are being recalled because of a “high risk” the food is contaminated

with a botulism-producing bacteria. While no illnesses were reported in connection with the recall, consumers were advised to throw away any dried, uneviscerated fish they may have bought. Import Foods Wholesale Inc., of St. Paul, was cooperating with the recall of smoked croaker, barracuda, big eye, and red snapper that originated from Guyana in South America. Seng Ong Wholesale Inc., also of St. Paul, was cooperating as well and recalling dried mackerel and round scad. State agriculture officials were working with the U.S. Food and Drug Administration to determine additional product origins and distribution channels. Import Foods sold its fish in 10-pound boxes in Minnesota, North Dakota, South Dakota, and Iowa.
Source: http://www.startribune.com/local/146966635.html

20. *April 11, Portland Press Herald* – (Maine) **Portland Shellfish Co. shut for violations.** For the second time in a little more than a year, federal regulators shut down Portland Shellfish Co. in Portland, Maine, citing "numerous violations" of federal laws and health regulations and its agreement to fix food safety problems identified in early 2011, the Portland Press Herald reported April 11. The Food and Drug Administration (FDA) also ordered Portland Shellfish, which processes lobster and shrimp at its plant, to recall and destroy seafood the company's president said is worth about $25,000. According to a letter to the company from FDA officials, Portland Shellfish will not be allowed to reopen until it updates its plans and procedures for making sure the seafood it processes is safe. The FDA's letter, obtained by the Portland Press Herald, said a conveyor belt used in shrimp processing tested positive in February for listeria. The FDA said the company processed lobster in the same room during the period just before the positive test and said that lobster must be recalled and destroyed. The company cooks raw shrimp and lobster, then freezes it, selling it to wholesalers along the East Coast, its president said. The FDA shut down the firm for several weeks in January 2011, citing unsanitary conditions including listeria contamination. Portland Shellfish has had to recall contaminated lobster meat four times since 2008, and the FDA said it has recorded food safety violations by the firm for more than a decade.
Source: http://www.pressherald.com/news/portland-shellfish-shut-for-violations_2012-04-11.html

21. *April 10, Food Safety News* – (National; International) **Berry cookies recalled for undeclared milk.** Biscomerica Corp. is recalling four types of berry cookies because they may contain milk that is not listed as an ingredient, Food Safety News reported April 10. The California-based company is voluntarily recalling cartons of its Knott's Berry Farm brand Boysenberry Cookies, Blueberry Cookies, Raspberry Cookies, and Strawberry Cookies, citing a risk the products may contain undeclared milk. The cookies were distributed nationwide between August 1, 2011 and April 5 and were sold in retail stores and through mail orders. They were distributed to California, Colorado, Florida, Hawaii, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, Texas, Washington, and Wisconsin. They were also distributed to parts of Canada and the Bahamas. The recall was initiated after an investigation found Biscomerica had listed whey, a milk product, as an ingredient but had not identified it as "milk," an allergen that must be declared on packaging. Production of the berry cookies has been suspended until the problem is corrected.

Source: http://www.foodsafetynews.com/2012/04/berry-cookies-recalled-for-undeclared-milk/

22. *April 10, Food Safety News* – (New York) **Vegetable Biryani recalled for undeclared allergen.** A New York-based company is voluntarily recalling packages of frozen Vegetable Biryani because they contain an undeclared nut allergen, Food Safety News reported April 10. Rajbhong Food of Flushing, New York, issued a recall of packages of frozen, ready-to-eat Vegetable Biryani because they contain cashews — a potential allergen — that are not listed as an ingredient. An investigation determined the problem arose from a breakdown in the finished product review process. Labels now being printed have been corrected to accurately reflect all ingredients in packaging.
Source: http://www.foodsafetynews.com/2012/04/vegetable-biryani-recalled-for-undeclared-allergen/

23. *April 10, KATU 2 Portland* – (Oregon) **Fire breaks out inside grain silo in North Portland.** A smoldering fire in a grain silo kept firefighters busy April 10 in Portland, Oregon. The fire broke out at Columbia Grain. An employee reported smelling smoke in 1 of the 125-foot tall silos on the site, and everyone was immediately evacuated. Firefighters were able to get hoses up to the top of the silo and spray water inside. The silo was about a quarter full. "Firefighters are always concerned about grain elevator fires because grain dust can be explosive in the right conditions," the Portland Fire battalion chief said in a news release. "We shut down all power to the facility and then checked each silo for hot spots."
Source: http://www.katu.com/news/local/Fire-breaks-out-inside-grain-silo-in-North-Portland-146905905.html

[Return to top]

Water Sector

24. *April 10, WOI-DT 5 Des Moines* – (Iowa) **Temporary water shortage in Mount Ayr.** A power and pumping issue in Mount Ayr, Iowa, caused a water shortage for the town in Ringgold County April 10. Temporary portable toilets were set up. Water service was restored. However, there was little water pressure and the town's water tower is empty. Residents were asked to boil water until April 12.
Source: http://www.woi-tv.com/story/17376262/water-shut-off-in-mount-ayr

25. *April 10, Jackson Newspapers* – (West Virginia) **Flow meter to be installed in Ripley city dam.** The dam behind the water plant in Ripley, West Virginia, will have a notch cut in it to allow the installation of a flow meter. According to Jackson Newspapers April 10, the move will cost the city about $20,000 but may save millions. The meter should settle the ongoing debate between the city and the West Virginia Department of Environmental Protection (DEP) concerning the sufficiency of the stream flow to handle the output of the sewage facility in west Ripley. DEP says more flow is necessary. The agency wants Ripley to build a sewage disposal plant and, if needed, pipe the outflow to the Ohio River, a project that could cost more than $30 million. Ripley has been out of compliance with DEP orders for years concerning the outflow

and is under order to pay a large fine. If the flow meter shows a sufficiency of flow, the fine can be adjusted downward. Formal notification of dates and times of testing will be given to the public as the time for that work approaches.
Source: http://www.jacksonnewspapers.com/news/x1170665867/Flow-meter-to-be-installed-in-Ripley-city-dam

26. *April 9, Elmira Star-Gazette* – (New York) **Major upgrade underway at CV State Park.** In a major upgrade, work is underway to replace the aging drinking water supply system in Chenango Valley State Park in Broome County, New York, the Elmira Star-Gazette reported April 9. The $1.2 million project involves an upgrade of the park's pumping station, installation of a new control system, and replacement of the system that provides drinking water to cabins, pavilions, camping sites, offices, restrooms, and water fountains in the 1,200-acre site in the Town of Fenton. Funding is coming from NY Works, a $1.2 billion statewide infrastructure program detailed recently by the governor of New York and legislative leaders. The state park's water system evolved from a collection of systems, some dating from the 1920s. Officials hope the replacement work will be finished by the weekend of May 26.
Source: http://www.stargazette.com/article/20120409/NEWS01/120409006/Major-upgrade-underway-CV-State-Park

For another story, see item **2**

[Return to top]

Public Health and Healthcare Sector

27. *April 10, U.S. Environmental Protection Agency* – (U.S. Virgin Islands) **EPA fines U.S. Virgin Islands Health Department for long term mismanagement of chemicals and pesticides.** The U.S. Environmental Protection Agency (EPA) found the U.S. Virgin Islands Department of Health violated federal law governing the handling and storage of hazardous waste at two of its facilities and fined the agency $68,000 for the violations, the agency said in a April 10 press release. EPA inspections at the facilities, the Old Municipal Facility in Charlotte Amalie, St. Thomas and 3500 Estate Richmond, Christiansted in St. Croix, found unlabeled and decaying containers of chemicals and pesticides on the properties. Many of the containers spilled and the health department failed to properly identify what types of wastes were being stored. In some instances, the hazardous chemicals were kept on-site for more than 10 years in a state of neglect and decay. Among the hundreds of hazardous chemicals on-site were pyrethrin (a neurotoxin), chlorpyrifos (an insecticide), and calcium hypochlorite (a bleach) — all of which are toxic. Federal environmental law requires hazardous chemicals to be stored, handled, and disposed of properly to safeguard public health and the environment.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/bead4d5adead891b852579dc0056a39e!OpenDocument

[Return to top]

Government Facilities Sector

28. *April 11, Associated Press; CBS* – (Oklahoma) **Tornadoes, giant hail slam northwest Oklahoma.** At least two tornadoes touched down, and hail the size of softballs pounded northwestern Oklahoma April 9, injuring two people and damaging a county jail and numerous vehicles, the Associated Press reported April 11. The National Weather Service said one tornado was spotted about 3 miles south-southwest of Woodward. Another tornado was spotted east of Sharon. KWTV 9 Oklahoma City reported the storm caused more than $250,000 in damage so far. In Woodward, hail up to 4.25 inches broke vehicle windows and damaged roofs. A sheriff said hail broke every skylight in the jail, and one hail stone cut an inmate on the back. He said hail damage caused the roof to leak.
Source: http://www.cbsnews.com/8301-201_162-57411614/tornadoes-giant-hail-slam-northwest-oklahoma/

29. *April 11, Middletown Times Herald-Record* – (New York) **Chlorine leak prompts evacuation of NFA.** A leak in a 150-gallon chlorine tank at Newburgh Free Academy in Newburgh, New York, prompted the evacuation of the school's employees April 11. High school students were on spring break. A hazmat team from the Newburgh City Fire Department responded. The cause or extent of the leak was not yet known. The chlorine is used for the school's swimming pool.
Source:
http://www.recordonline.com/apps/pbcs.dll/article?AID=/20120411/NEWS/120419958

30. *April 10, Nextgov* – (National) **FCC move to disable stolen smartphones won't stop government data thieves.** A new nationwide system for shutting off stolen smartphones announced April 10 might stop scammers from reselling government devices, but it would not necessarily protect the sensitive data inside, some information security experts said. The wireless industry agreed to, within 6 months, block service on portable electronics when users report them to police as stolen, a Federal Communications Commission (FCC) chairman and law enforcement officials said April 10. The companies also are working to create, within 18 months, a single database containing the identification numbers of stolen devices worldwide so that thieves cannot swap carriers to avoid detection. The Veterans Affairs Department, the largest federal agency, reported that only 55 percent of its portable electronics inventory — including smartphones, tablets, and laptops — was protected with a standard encryption format called Federal Information Processing Standards 140-2; NASA ranked at the bottom with a 41 percent protection rate; and DHS, reported 75 percent of its devices were encrypted. Most agencies reported encrypting at least 80 percent of their mobile devices, including 100 percent fully encrypted inventories at the State and Treasury departments, and the General Services Administration and Social Security Administration. AT&T, T-Mobile, Verizon, and Sprint, the carriers that cover 90 percent of U.S. subscribers, have committed to participate in the phone-disabling database, FCC officials said.
Source: http://www.nextgov.com/nextgov/ng_20120410_5674.php

31. *April 10, Los Angeles Times* – (National; International) **European court OKs extradition to U.S. of five terrorism suspects.** A man who celebrated the September 11th attacks in sermons and allegedly tried to set up a terrorist training camp in Oregon can be extradited to the United States from Britain, the European Court of Human Rights ruled April 10. The court said the man and four other terrorism suspects, including two accused of involvement in the 1998 bombings of U.S. embassies in Kenya and Tanzania that killed hundreds and wounded thousands, could be sent to face trial in the United States without fear that they would face "inhuman and degrading" conditions in a maximum-security prison if convicted. The men had argued that they could be subject to solitary confinement for the rest of their lives in a "supermax" prison in Colorado where many terrorism convicts are serving time. The suspects have 3 months to appeal the decision to the European court's grand chamber, but such appeals are rarely taken up. U.S. authorities want the man extradited to face allegations he tried to set up a training camp in Bly, Oregon, for would-be insurgents in Afghanistan, and that he was involved in the kidnapping of a group of Western tourists in Yemen in 1998. The other suspects covered by the European court ruling included one of the man's alleged conspirators in trying to establish the Oregon terrorist training camp.
Source: http://latimesblogs.latimes.com/world_now/2012/04/european-court-rules-on-extradition-of-cleric.html

32. *April 10, Fort Worth Star-Telegram* – (Texas) **Arlington mayor was target of alleged murder-for-hire plot.** An Arlington, Texas mayor and a city attorney were the targets in an alleged murder-for-hire plot that led to the arrest of a business-owner, the city said April 10. FBI agents arrested the man April 9 at his home. The Drug Enforcement Administration was also involved in the investigation. The suspect was being held by U.S. marshals April 10, and was scheduled to appear for a detention hearing April 13 before a U.S. magistrate.
Source: http://www.star-telegram.com/2012/04/10/3874403/arlington-mayor-was-target-of.html#storylink=omni_popular

33. *April 6, Federal Computer Week* – (National) **IG report finds flaws in VA's information security program.** An inspector general audit revealed that the Department of Veterans Affairs (VA) failure to fully comply with the Federal Information Security Management Act (FISMA) resulted in more than 15,000 outstanding security risks, Federal Computer Week reported April 6. The fiscal year 2011 performance audit examined the extent to which VA's information security program complied with FISMA requirements and National Institute for Standards and Technology guidelines. Substantial inadequacies were discovered in areas related to access controls, configuration management controls, continuous monitoring, and services continuity practices. Also, VA has not effectively implemented procedures to identify and correct system security flaws on network devices, database and server platforms, and Web applications. Deficiencies were also found in reporting, managing, and closing plans of action and milestones. The report accentuated a larger compliance issue government-wide. A March 7 review by the Office of Management and Budget showed that only 7 out of 24 agencies are more than 90 percent compliant with FISMA

directives.
Source: http://fcw.com/articles/2012/04/06/fisma-compliance-va-failure.aspx

For another story, see item **50**

[Return to top]

Emergency Services Sector

34. *April 11, WWAY 3 Wilmington* – (North Carolina) **Brunswick County 911 service restored.** Technicians restored partial service to North Carolina's Brunswick County Central Communications (9-1-1) Center after an equipment failure caused a temporary loss of 9-1-1 service April 11. 9-1-1 operators were notified of the failure shortly after 3 a.m. and immediately began routing calls to the New Hanover County 9-1-1 Center, which serves as a backup for Brunswick County. Phone company technicians worked for 4 hours to restore partial service. As of April 11, Brunswick County was answering 9-1-1 calls, but had only about half of the 9-1-1 lines that are usually available. The cause of the equipment failure is under investigation.
Source: http://www.wwaytv3.com/2012/04/11/brunswick-county-911-service-restored

35. *April 10, Santa Rosa Press Democrat* – (California) **Turkey into electrical wires knocks out power to Sonoma County's 911 system.** A wild turkey that flew into power lines knocked out the high-tech emergency 9-1-1 dispatch system in Sonoma County, California, April 8, and crippled operations at the courthouse and county jail April 9. The power blackout was compounded when the county's massive and expensive emergency backup power system failed. The blackout affected almost 2,000 homes and businesses, including the county's computer aided dispatch system used by nearly all public safety departments in the county. Without it, police and fire dispatchers were forced to take calls with paper and pencil for an hour. With the blackout, the dispatchers' computers and every computer connected to the county system went out. At that point, the county's uninterrupted power supply, or UPS, should have kicked in. April 9, computer crews were checking why the 10-year-old backup system failed. Without electricity, dispatchers lost access to computerized maps that help them quickly pinpoint locations for firefighters, police, and ambulance crews. Instead, everyone had to use paper map books and communicate using radios and phones. No significant delays or problems in responding to calls were reported during the blackout, officials said.
Source:
http://www.pressdemocrat.com/article/20120409/ARTICLES/120409571/1033/news?Title=Turkey-into-electrical-wires-knocks-out-power-to-county-911-system

For more stories, see items **28**, **30**, **50**, and **51**

[Return to top]

Information Technology Sector

36. *April 11, Computerworld* – (International) **Apple promises Flashback malware killer.** April 10, Apple for the first time publicly acknowledged a malware campaign that has infected an estimated 600,000 Macs, and said it would release a free tool to disinfect users' machines. Although Flashback has circulated since September 2011, it was only in March that the newest variant began infecting Macs using an exploit of a Java bug Oracle patched in mid-February. Apple maintains its own version of Java for Mac OS X, and is responsible for producing security updates. It issued a Java update April 3 that quashed the bug Flashback has been using to infect Macs. In the 7 weeks between Oracle's and Apple's updates, hackers responsible for Flashback managed to insert their software — designed for, among other things, password theft — onto an estimated 2 percent of all Macs. Apple said it was working with Internet service providers to "disable [the Flashback] command and control network," referring to the practice of asking hosting firms to pull hacker-operated command-and-control servers off the Internet so infected computers cannot receive further orders. The company promised to issue a special tool to "detect and remove the Flashback malware." Apple did not set a timetable for its release.
    Source:
    http://www.computerworld.com/s/article/9226084/Apple_promises_Flashback_malware_killer?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Reader

37. *April 11, The H* – (International) **Samba fixes critical remote code execution vulnerability.** The Samba developers patched a critical security vulnerability that effects all versions of the open source, cross-platform file sharing solution from Samba 3.0.x up to version 3.6.3 that was released in January, The H reported April 11. The hole allows an attacker to gain complete access to a Samba server from an unauthenticated connection. The GPLv3 licensed Samba is used by many Unix and Linux systems with the ability to share files with Windows systems by implementing the SMB, SMB2, and CIFS protocols. The vulnerability was discovered by two security researchers working for the Zero Day Initiative. The flaw, which is located in the code generator for Samba's remote procedure call interface, makes it possible for clients on the network to force the server to execute arbitrary code. This attack can be performed over an unauthenticated connection, granting the attacker root user privileges and thus complete access to the Samba server. The fact the problem was located in the Perl-based DCE/RPC compiler Samba uses to generate code for handling remote requests has, presumably, made it very hard to detect with automated code auditing methods and caused it to stay hidden for such a long time.
    Source: http://www.h-online.com/security/news/item/Samba-fixes-critical-remote-code-execution-vulnerability-1518580.html

38. *April 11, H Security* – (International) **Patch Tuesday closes critical Windows, Office and IE holes.** April 10, Microsoft released 6 security bulletins that addressed 11 vulnerabilities in its products, 8 of which are considered to be critical. Four of the bulletins address critical holes in all supported versions of Windows, Internet Explorer

(IE), the .NET Framework, Office and SQL Server, as well as Microsoft Server and Developer tools. All of these bugs could be exploited by attackers to remotely inject and execute malicious code on a victim's system via a specially crafted file. One critical bulletin, MS12-024 notes a privately reported vulnerability that could allow attackers to modify existing signed executable files. Another, MS12-027, is an issue in Microsoft's common controls, used in numerous Microsoft applications, which can be exploited when a user visits a malicious site or opens an e-mail attachment to allow remote code execution. An Internet Explorer bulletin, MS12-023, affects all supported versions of IE, closes five holes, one when printing a specially crafted HTML page and four when IE accesses deleted objects in various situations. The rating for these holes is either critical or moderate depending on the combination of operating system and IE version. Finally, MS12-025 closes a vulnerability in the .NET framework that allows attackers to "take complete control of an affected system."
Source: http://www.h-online.com/security/news/item/Patch-Tuesday-closes-critical-Windows-Office-and-IE-holes-1518553.html

39. *April 11, H Security* – (International) **Adobe fixes critical vulnerabilities in Reader and Acrobat.** Adobe released versions 10.1.3 and 9.5.1 of its Acrobat and Reader products to address high priority security vulnerabilities that could be used by an attacker to cause the application to crash and potentially take control of an affected system. These include memory corruption in the JavaScript API and JavaScript handling, an integer overflow in the True Type Font handling, and a security bypass via the Adobe Reader installer, all of which could lead to arbitrary code execution. Adobe Acrobat and Reader 10.1.2 and earlier 10.x versions, as well as 9.5 and earlier 9.x versions for Windows and Mac OS X are affected — on Linux, Reader 9.4.6 and earlier 9.x versions are vulnerable.
Source: http://www.h-online.com/security/news/item/Adobe-fixes-critical-vulnerabilities-in-Reader-and-Acrobat-1518711.html

40. *April 11, The Register* – (International) **Malware-infected flash cards shipped out with HP switches.** HP sent out a warning to customers after the vendor found it inadvertently shipped virus-laden compact flash cards with its networking kit. The unnamed malware appeared on flash cards that came bundled with HP ProCurve 5400zl switches. The flash card would not have any effect on the switch itself but "reuse of an infected compact flash card in a personal computer could result in a compromise of that system's integrity," HP warned in a bulletin issued April 10. It is unclear how the unknown malware got onto the Flash cards that come bundled with the 10 Gbps-capable line of LAN switches, but an infected computer somewhere in the manufacturing process — possible in a factory run by a third-party supplier — is the most obvious suspect.
Source:
http://www.theregister.co.uk/2012/04/11/hp_ships_malware_cards_with_switches_oops/

41. *April 10, Threatpost* – (International) **No permissions Android application can harvest, export device data.** April 9, a researcher was able to demonstrate Android applications without permissions can still access files used by other applications,

including which applications are installed and a list of any readable files used by those applications. That capability could be used to identify applications that have weak permissions vulnerabilities and exploit those, he warned. He unveiled a proof of concept Android application, dubbed "NoPermissions" that works with Android phones running version 4.0.3 and 2.3.5 of the operating system. Among the data he found on his own Android phone were certificates from his mobile Open VPN application. Not only could an attacker take advantage of the lack of strict permissions to collect data, he wrote, they could also export it from the phone without permissions. The URI ACTION-VIEW Intent network access call is supported without permissions, which will open a browser on the Android device. An attacker could then pass data to the browser in the form of a URI with GET parameters to pass it to an Internet accessible server or device using successive browser calls.
Source: http://threatpost.com/en_us/blogs/no-permissions-android-application-can-harvest-export-device-data-041012

For more stories, see items **9**, **30**, and **33**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

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

[Return to top]

Communications Sector

42. *April 11, Dayton Beach News-Journal* – (Florida) **Bright House phone outage irks customers.** Bright House Networks phone service disconnected for nearly 4 hours April 9, leaving as many as 49,000 central Florida customers without service. Cable and Internet service was not affected, a spokesman said. The phone customers who were impacted were on one switch that failed, and not all of the 49,000 customers on that switch were affected, he said. Most of those on the switch were residential customers and because of the timing of the disruption — 12:37 p.m. to 4:20 p.m. — most would not have been impacted, he said. Customers had lost and delayed dial tones, he said.
Source: http://www.news-journalonline.com/business/local-business/2012/04/11/bright-house-phone-outage-irks-customers.html

43. *April 10, Boston Globe* – (Massachusetts) **Downed Boston TV stations back on the air.** Three Boston television (TV) stations that were knocked off the air April 8 by a technical glitch returned to service April 10. Over-the-air broadcasts from CBS Corp. stations WBZ-TV 4 and WSBK-TV 38, ABC network affiliate WCVB-TV 5, and PBS station WGBX-TV 44 shut down at about 8 p.m. All four stations share the same antenna, located atop a 1,200-foot tower in Needham, Massachusetts. WCVB-TV quickly resumed broadcasting through a backup antenna but the other three stations

stayed off the air. The outage had no effect on most viewers, because the stations continue to feed their signals to cable and satellite TV providers, who serve about 98 percent of viewers in the Boston area. At 1 p.m. April 10, engineers at the affected stations briefly shut down WGBH, then moved its signal to the backup antenna being used by WCVB. Then WCVB, WSBK, WBZ, and WGBX all began broadcasting from the WGBH antenna. The director of broadcast operations and engineering for WBZ and WSBK, said the outage was due to a breakdown in a "five-way power divider," an electronic component that separates the signals from multiple stations before feeding them to the antenna. Fixing the problem will require a complete shutdown of the antenna. To accomplish this, each station will install a temporary antenna on the tower. After that, the WGBH antenna will be completely shut down. The power divider can then be repaired.
Source: http://www.boston.com/Boston/businessupdates/2012/04/downed-boston-stations-back-the-air/7zbd3Z288EU6pmBpwgaHxM/index.html

For more stories, see items **30** and **41**

[Return to top]

Commercial Facilities Sector

44. *April 11, Chicago Sun-Times Media Wire* – (Illinois) **30 displaced in blaze at Rogers Park apartment building.** About 30 people were homeless after an extra-alarm fire burned a Chicago apartment building April 10. Crews called an extra alarm for the blaze shortly after they arrived. All residents of the 19-unit apartment building had to be evacuated and 30 were displaced from their homes. The fourth floor and back porches of the building were heavily damaged, while other units had water damage or broken windows.
Source: http://www.suntimes.com/news/metro/11836960-418/30-displaced-in-blaze-at-rogers-park-apartment-building.html

45. *April 11, KJTV 34 Lubbock* – (Texas) **Apartment complex gutted by natural gas-fueled fire.** Lubbock, Texas fire investigators said leaking natural gas appeared to have sparked a massive explosion and fire that ripped through an apartment complex April 10. The deputy fire marshal reported natural gas was the main fuel source, but investigators were still looking for the ignition source. Witnesses said they heard a single blast that shook nearby buildings, followed by an inferno and dense smoke. Seven residents were injured in the explosion and fire. A total of 38 people were left homeless, and the damage was so severe that the complex had been deemed unsafe and was demolished.
Source: http://www.myfoxlubbock.com/mostpopular/story/fire-explosion-lubbock-apartments-smoke/IDg_V4IMpEOcaJ-gaB_2Iw.cspx

46. *April 10, ClarksvilleNow.com* – (Tennessee) **Many animals lose lives in suspicious pet store blaze.** Clarksville, Tennessee fire rescue officials were investigating what they called a suspicious fire April 10 that killed a number of animals at D&R Pet Store. The fire marshal said there was a great deal of damage to the store and many animals

were killed by the fire and smoke. “The fire was suspicious in nature due to the fact that there were multiple points of origin as we call it. There were two different fires that didn’t connect so that’s what makes it suspicious in nature,” the fire marshal said.
Source: http://www.clarksvillenow.com/pages/12798558.php

47. *April 10, Associated Press* – (Nevada) **NTSB releases recommendations for air races.** Air race pilots should take their modified aircraft on a dry run before participating in certain types of competitions and should possibly wear flight suits to help them withstand high gravitational forces, the National Transportation Safety Board (NTSB) said April 10. The recommendations were among seven the board offered during a news conference in Reno, Nevada, nearly 6 months after a crash at the Reno National Championship Air Races that killed 11 people and seriously injured more than 70 spectators. The NTSB also called on the Federal Aviation Administration (FAA) to correct what it said were numerous errors and discrepancies in its guidance for race course designs, including the distance that spectators should be from the edge of the course. The FAA said it was already acting on the NTSB recommendation.
Source: http://www.businessweek.com/ap/2012-04/D9U28GT80.htm

48. *April 10, Associated Press* – (Arkansas) **Pipe bomb left at Mormon church in northern Ark.** The Boone County Sheriff’s office was investigating an apparent pipe bomb found after Easter services in the parking lot of a Mormon church near Harrison, Arkansas. The sheriff said a caller reported finding the device April 8 at the Church of Jesus Christ of Latter-day Saints. He said the device contained a flammable powder. The FBI was helping in the investigation.
Source: http://www.mysanantonio.com/news/article/Pipe-bomb-left-at-Mormon-church-in-northern-Ark-3472531.php

For more stories, see items **9**, **35**, and **50**

[Return to top]

National Monuments and Icons Sector

49. *April 11, Newark Star-Ledger; Associated Press* – (New Jersey) **New brush fires flare up across N.J., despite rise in humidity.** Despite cooler temperatures and a slight increase in humidity, new brush fires sprouted April 10 as a pair of older conflagrations continued to burn in southern New Jersey. Although weather conditions were expected to improve, fire experts said the risk for fire would remain high until New Jersey gets significant amounts of rain. Among the new fires reported April 10 was a large fire near Barnegat, which burned about 20 acres, but was contained, according to the acting chief of the forest fire service. In Middlesex County, crews from several state and local agencies were called to a fire near Woodland Elementary School in Monroe Township and a second fire to the north, in Sayreville. Residents of the Atlantic Heights development in Barnegat were greeted by the sounds of fire trucks and helicopters April 10 as a brush fire blazed across the road. Within just a few hours, firefighters were able to contain the blaze and keep it within a few hundred feet of the community.

Source: http://www.nj.com/news/index.ssf/2012/04/new_brush_fires_flare_up_acros.html

50. *April 10, CBS News* – (National) **Dry, windy conditions fuel wildfires in East.** Along the Eastern Seaboard, firefighters are battling a string of wildfires after weeks of unusually warm and dry weather, CBS News reported April 10. Fires burned in nine states, from New Hampshire to Florida. Wildfires broke out up and down the East Coast, April 9, fueled by whipping winds and dry conditions. On New York's Long Island, hundreds of firefighters raced to keep flames from closing in on Brookhaven National Lab, a nuclear physics facility. The fire swallowed up 1,000 acres, destroyed at least two homes, and sent three firefighters to the hospital. Officials said the fire was 50 percent contained, but they warned homes were still in jeopardy. Firefighters said they had no idea when they would have the fire under control. In New Jersey, another fire — which officials were calling suspicious — was on track to burn through 1,000 acres. The dry, windy weather also helped feed flames in Pennsylvania and Connecticut where a brush fire lined a railroad track. Nearby homes and businesses were evacuated. In Virginia, helicopters dumped water to try to douse flames. The wildfire outbreak stretched all the way down to Miami where a fast-moving fire caught residents by surprise.
Source: http://www.cbsnews.com/8301-505263_162-57411672/dry-windy-conditions-fuel-wildfires-in-east/

[Return to top]

Dams Sector

51. *April 10, KBOI 2 Boise* – (Idaho) **Idaho first responders stage statewide disaster drill.** Local, state, and federal responders in Idaho conducted a 2-day statewide disaster test at Gowen Field's Emergency Operations Center, KBOI 2 Boise reported April 10. In the test, emergency workers simulated a 7.0 magnitude earthquake in eastern Idaho with its epicenter in Idaho Falls, affecting six Idaho counties and causing the Palisades Dam to collapse. "We have faults that are known throughout the state," said the director of the state's bureau of homeland security. "There was the Challis (earthquake), and an event in Elko not too long ago. We are very seismically active." The response to the simulated scenario will be evaluated by experts from several states.
Source: http://www.kboi2.com/news/local/disaster-drill-146898825.html?tab=video&c=y

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer